THÈSE EN COTUTELLE
POUR L'OBTENTION DU GRADE DE DOCTEUR
DE L'UNIVERSITÉ DE BORDEAUX
ET DE L'UNIVERSITÉ ALEXANDRU IOAN CUZA DE IAȘI

École doctorale Droit Bordeaux
École doctorale de Droit – Université Al. I. Cuza de Iași

Discipline : Droit
Spécialité : Droit privé et sciences criminelles

Présentée par
Cătălin Boacnă

La vie privée à l'ère numérique, un défi en droit pénal.
Étude comparative France – Roumanie

Sous la direction de
Pr. Jean-Christophe Saint-Pau et Pr. Tudorel Toader
Soutenue publiquement le 19 décembre 2025 à Bordeaux

DEVANT UN JURY COMPOSE DE:

Monsieur Guillaume BEAUSSONIE, Professeur à l'Université Toulouse Capitole, *Président du jury*

Monsieur Jean-Christophe SAINT-PAU, Professeur à l'Université de Bordeaux, *Directeur de thèse*

Monsieur Tudorel TOADER, Professeur à l'Université Alexandru Ioan Cuza de Iași, *Directeur de thèse*

Madame Marie-Christine SORDINO, Professeure à l'Université de Montpellier, *Rapporteure*

Madame Charlotte CLAVERIE-ROUSSET, Professeure à l'Université de Bordeaux, *Examinatrice*

Madame Ruxandra RĂDUCANU, Professeure à l'Université de Craiova, *Rapporteure*

SOMMAIRE

Une table des matières détaillée figure à la fin de l'ouvrage

Sommaire **2**

Remerciements **2**

Abréviations **8**

Introduction générale **14**

Première partie

La protection de la vie privée à l'ère numérique

Titre I. Le fondement juridique de la protection de la vie privée 98

Chapitre 1. L'effet des évolutions technologiques sur la vie privée 99

Chapitre 2 .Les ingérences dans le droit à la vie privée dans le contexte de l'évolution numérique 162

Titre II. Les infractions classiques destinées à assurer la protection de la vie privée en Roumanie et en France 258

Chapitre 1. Les réglementations traditionnelles relatives au domicile et à la correspondance 258

Chapitre 2. L'analyse de l'infraction d'atteinte à la vie privée 292

Seconde partie

Le droit pénal face à l'évolution technologique: intrusion, défis, adaptation

Titre I. Le droit pénal face aux algorithmes: une nouvelle réalité juridique 412

Chapitre 1. Le droit pénal face à l'intelligence artificielle, l'apprentissage automatique et le profilage de masse 412

Chapitre 2. Effets juridiques de la cryptographie dans les conversations numériques 520

Titre II. Intrusion de l'état dans la vie privée. Synchronisation du droit pénal avec l'évolution technologique 545

Chapitre 1. Intrusion gouvernementale: du mandat de perquisition à l'interception des conversations 547

Chapitre 2. Surveillance électronique 616

Chapitre 3. Vie privée versus médecine moderne 646

Conclusions générales et propositions de lege ferenda **693**

Bibliographie **698**

Annexes **817**

Index alphabétiques **840**

Tables des matières **844**

Remerciements

Je tiens à exprimer la forme de gratitude la plus vive et profonde aux Messieurs les Professeurs Tudorel Toader et Jean Christophe Saint-Pau, sans les conseils avisés et le soutien constant desquels je n'aurais pas pu aboutir à ce travail de recherche aujourd'hui. Le fait qu'ils aient accepté de m`offrir tout le soutien dont j'avais besoin n'est pas seulement un honneur pour moi, mais c'est une forme de responsabilité qui m'a fait comprendre et admirer les véritables repères du droit roumain et français.

Messieurs les Professeurs Tudorel Toader et Jean Christophe Saint-Pau m'ont accordé leur confiance et leur attention professionnelle tout au long d`un parcours assez difficile, ponctué de nombreux défis pour une telle mission. L`exigence intellectuelle a été doublée d`une disponibilité humaine dans ce parcours de recherche doctorale – ma première rencontre que j'ai eue avec Monsieur le Professeur Tudorel Toader peu après avoir quitté le poste de juge à la Cour constitutionnelle pour devenir recteur de la plus ancienne université en Roumanie et celle avec Monsieur le Professeur Jean Christophe Saint-Pau dans son bureau à l'Institut de sciences criminelles et de la justice (ISCJ) de Bordeaux, où j'ai découvert le droit français, m`ont laissé une impression très positive.

L`achèvement de cette cotutelle n'aurait pas été possible sans le soutien des membres de l'école doctorale de l`Université Al. I. Cuza et de l'Université de Bordeaux, que je remercie pour le temps qu`ils m`ont consacré et pour leur implication dans le soutien du projet. Je tiens tout particulièrement exprimer toute ma considération à Madame la Professeure Tamara Ungureanu, directrice de l'école doctorale à Iasi.

Dans ce contexte, je tiens à exprimer ma gratitude au personnel administratif pour qui, j`en suis convaincu, les choses n'ont pas été du tout faciles. L'expérience de recherche vécue à la bibliothèque de l'ISCJ a été particulièrement enrichissante, grâce au soutien constant et aux conseils avisés des bibliothécaires et de l`ensemble du personnel de l'institution.

Sur le plan personnel, je tiens à remercier ma famille, mes collègues du cabinet d'avocats et mes collègues doctorants qui m'ont accueilli chaleureusement à Bordeaux et m'ont apporté le soutien et les conseils utiles pour mieux comprendre les mécanismes de l'enseignement universitaire français.

Enfin et surtout, je voudrais mentionner que cette expérience de cotutelle n'aurait pas été possible sans la bourse du gouvernement français France Excellence Roumanie, accordée par l'ambassade de France.

Je dédie cette thèse à la personne qui voulait le plus que je la termine avec succès, mon père, décédé au CHU Pellegrin de Bordeaux en 2019.

À la mémoire de mon père,

Gheorghe Boacna

Titre : La vie privée à l'ère numérique, un défi en droit pénal. Étude comparative France – Roumanie

RÉSUMÉ

De concept philosophique traçant la frontière entre sphère intime et sphère publique, la vie privée est devenue, à l'époque moderne, un droit fondamental. À l'ère des mutations technologiques, sa portée est reconfigurée par les réseaux sociaux, la collecte massive de données, l'intelligence artificielle, les algorithmes et une surveillance omniprésente, qu'elle émane des grandes plateformes ou d'acteurs étatiques. Dans une perspective comparée, cette recherche doctorale examine les mécanismes par lesquels le droit pénal est appelé à recalibrer ses fonctions préventive et répressive sans renoncer aux principes de légalité, de nécessité, de proportionnalité et de subsidiarité.

Elle met en lumière les défis imminents : profilage de masse, suivi continu, biométrie, prédiction comportementale — bref, la tendance à réduire l'identité humaine à un nombre. La vie privée tend ainsi à devenir un dispositif binaire d'identification : un nombre menacé par d'autres nombres et, simultanément, protégé par eux. L'ouvrage, du point de vue du droit pénal matériel et procédural, la manière dont les ordres juridiques français et roumain réagissent à l'extension des moyens techniques de surveillance et de traitement des données. Dans un cadre comparatif sont analysées conjointement les infractions classiques relatives à la vie privée, au domicile, à la correspondance et au secret professionnel ainsi que les nouvelles incriminations liées à l'environnement numérique, afin de mettre en évidence les continuités, les ruptures et les zones d'incohérence normative. La thèse intègre la jurisprudence de la CEDH et de la CJUE relative à la surveillance secrète, aux interceptions à large échelle et au profilage, en montrant comment ces références européennes dessinent les limites acceptables de l'ingérence et, dans le même temps, laissent un espace significatif à l'extension du contrôle sur la personne. Sont également pris en compte les points de vue des principaux systèmes juridiques européens en matière de surveillance de masse, afin de souligner l'absence de véritable frontière de l'ingérence lorsque les infrastructures et les échanges de données dépassent le cadre national.

Dans une ligne d'évolution qui part symboliquement de l'arrêt Semayne's Case (1604) et conduit aux régimes modernes du renseignement et aux législations inspirées de la « loi Big Brother », le travail montre comment l'intrusion de l'État tend à être justifiée par des formules de plus en plus générales, au risque de s'éloigner de la finalité de protection de l'individu. Un exemple significatif de divergence entre les deux systèmes réside dans la possibilité, en droit français, d'imposer des formes d'« assignation à résidence » ou des restrictions sévères de liberté en dehors de toute procédure pénale en cours ou de toute condamnation, mécanisme qui

ne trouve pas d'équivalent direct en droit roumain et qui pose de manière aiguë la question des garanties effectives de la vie privée et de la liberté individuelle.

La thèse propose des repères concrets afin que l'intervention pénale demeure un instrument effectif de protection de la vie privée, en évitant que le discours juridique ne soit absorbé par un pouvoir numérique engagé dans un processus accéléré d'autolégitimation et de reconfiguration.

Title: Privacy in the Digital Age: A Challenge for Criminal Law. A Comparative Study of France and Romania

ABSTRACT

From a philosophical concept that once marked the boundary between the intimate and the public spheres, private life has evolved in the modern era into a fundamental right. In the context of technological developments, the notion of private life has been reshaped by social networks, massive data collection, artificial intelligence, algorithms, and the ubiquitous surveillance conducted by IT giants and state actors alike. From a comparative perspective, this doctoral thesis aims to present the mechanisms through which criminal law is called upon to recalibrate its preventive and repressive functions without renouncing the principles of legality, necessity, proportionality, and subsidiarity. It also highlights the imminent challenges for criminal law, such as mass profiling, permanent monitoring, biometrics, and predictive behaviour, and, more broadly, the transformation of human identity into a number.

Private life has become a binary mechanism of identification, a number threatened by other numbers and, at the same time, a number protected by other numbers. The thesis examines, from the perspective of substantive and procedural criminal law, how the French and Romanian legal systems react to the expansion of technical means of surveillance and data processing. Within a comparative framework, it analyses together the classic offences relating to privacy, the home, correspondence, and professional secrecy, and the new offences linked to the digital environment, in order to highlight continuities, ruptures, and areas of normative inconsistency.

The thesis integrates the case law of the ECtHR and the CJEU relating to secret surveillance, large-scale interceptions, and profiling, showing how these European benchmarks shape the acceptable limits of intrusion and, at the same time, leave significant scope for the extension of control over the individual. The perspectives of the main European legal systems on mass surveillance are also taken into account, precisely to underline the absence of a real boundary to interference when infrastructures and data exchanges go beyond the national

framework. In an evolutionary line that starts symbolically with Semayne's Case (1604) and reaches modern intelligence regimes and legislation inspired by the "Big Brother law", the study shows how state intrusion tends to be justified by increasingly general formulas, at the risk of moving away from the aim of protecting the individual. A significant example of divergence between the two systems lies in the possibility, under French law, of imposing forms of "house arrest" or severe restrictions on liberty outside any pending criminal proceedings or conviction, a mechanism which has no direct equivalent in Romanian law and acutely raises the issue of effective guarantees of private life and individual liberty.

The thesis proposes concrete benchmarks to ensure that criminal intervention remains an effective instrument for the protection of private life, preventing legal discourse from being absorbed by a digital power engaged in an accelerated process of self-legitimation and reconfiguration.

ABRÉVIATIONS

AFP	Agence France Presse
AI/IA	Intelligence Artificielle
AJ pénal	Actualité juridique pénal, Dalloz
AJDA	Actualité juridique – droit administratif, Dalloz
AML	Anti-money Laudering
ANSSI	Agence nationale de la sécurité des systèmes d'information
art.	article
Ass. plén.	arrêt de l'Assemblée plénière de la Cour de cassation
BIPA	Biometric Information Privacy Act
Bull. civ.	Bulletin des arrêts des chambres civiles de la Cour de cassation
C. civ.	Code civil
C. pén.	Code pénal
C. proc. civ.	Code de procédure civile
C. proc. pén.	Code de procédure pénal
C.	Code
CA	arrêt d'une cour d'appel
Cah.just.	Les Cahiers de la justice
Cass.	Cour de cassation
CCR Roumanie)	Curtea Constituțională a României (Cour Constitutionnelle de
CE	Conseil d'État
CEDH fondamentales	Convention européene des droits de l'Homme et des libertés
Cf.	*confer*
Ch.	chambre

chron.	Chronique
Civ.	arrêt d'une chambre civile de la Cour de cassation
CJCE	Cour de justice des Communautés européennes
CJU	Cour de justice de l'Union européene
CM	Comité des Ministres
CNA de l'audiovisuel, Roumanie)	Consiliul Național al Audiovizualului, România (Conseil national
CNCDH	*Commission nationale consultative des droits de l'Homme*
CNCTR *renseignement*	*Commission nationale de contrôle des techniques de*
CNIL	Commission nationale de l'informatique et des libertés
coll.	collection
Com. cassation	arrêt de la chambre commerciale et financière de a Cour de
cons.	considérant
Const. 58	Constitution du 4 octobre 1958
Const. const.	décision du Conseil constitutionnel
Crim.	arrêt de la chambre criminelle de la Cour de casssation
D.	Recueil, Dalloz
DDSE	Détention à domicile sous surveillance électronique
dir.	sous la direction de
DNS	Domain Name System
doctr.	Doctrine
Dr. fam.	Droit de la famille, LexisNexis
Dr. pénal	Droit pénal, LexisNexis
éd.	Édition
EDPB	Comité européen de la protection des données
et al.	et alii auctores (et autres auteurs)

EUR-Lex	législation et jurisprudence de l'Union européenne
Eurojust	Agence de l'Union européenne pour la coopération judiciaire en matière pénale
Europol	Office européen de police
ex.	exemple
fasc.	Fascicule
FBI	Federal Bureau of Investigation
FNAEG	Fichier national automatisé des empreintes génétiques
FTC	Commission fédérale du commerce (États-Unis)
Gaz. Pal.	La Gazzette du Palais, Lextenso
GDPR/RGPD	General Data Protection Regulation/Règlement général sur la protection des données.
GINA	Genetic Information Nondiscrimination Act
GREVIO	Groupe d'experts sur la lutte contre la violence à l'égard des femmes et la violence domestique (Conseil de l'Europe)
HMSO	Her Majesty's Stationary Office
ibid.	*ibidem*
ICCJ	Înalta Curte de Casație și Justiție (Haute Cour de cassation et de justice, Roumanie)
IEEE	Institute of Electrical and Electronics Engineers
IMSI	Identité Internationale d'Abonné Mobile
Inf.Soc	The informational society
infra	ci-dessous
Interpol	Organizația Internațională a Poliției Judiciare
IoT	Internet of Things
IP	internet protocol
IPA	Investigatory Powers Act
ISP	Internet Service Provider

IVT	Invalid Traffic
JCl	Jurisclasseur, LexisNexis
JCl Pén.	Juriclasseur Pénal code, LexisNexis
JCP	La semaine juridique, LexisNexis
JO	Journal officiel de la République Française
Juris.	Jurisprudence
L.	loi
n°	numéro(s)
NIS	Network and Information Systems Directive
NIST	National Institute of Standards and Technology
not.	notamment
obs.	observations
op.cit.	*opere citato*, ouvrage précité
OUP	Oxford University Press
p.	page
PUF	Presses universitaires de France
PwC	PricewaterhouseCoopers
QPC	Questions prioritaires de constitutionnalité
R.	règlement
Rec.	recommandation
Rép. civ.	Répertoire de droit civil, Dalloz
Rép. droit international	Répertoire de droit international, Dalloz
Rép. pén	Répertoire de droit pénal et de procédure pénale, Dalloz
SE	surveillance électronique
sec.	section
spé.	specifiquement

t.	tome
TFUE	Traité sur le fonctionnement de l'Union européenne
Trib.	Tribunal
UE	Union Européenne
UNODC	United Nations Office on drugs and crime
vol.	Volume

INTRODUCTION GÉNÉRALE

„*Toutes les choses sont des nombres*"

Pythagore

1. Questions d'actualité. Assistons-nous aujourd'hui à l'enterrement de l'intimité et du droit à la vie privée dans une république numérique où les algorithmes[1] rédigent leur propre Constitution ? La sauvegarde du droit à la vie privée face à l'éloquence des algorithmes peut-elle encore recourir aux mécanismes dilatoires classiques qui permettent généralement de résoudre la plupart des phénomènes menaçant la société ? Sommes-nous de simples ressortissants d'un territoire numérique où les règles sont déjà préétablies ou avons-nous encore la faculté de déterminer une conduite protectrice ? Le légicentrisme[2] est-il la solution du droit positif pour assurer la cohabitation pacifique entre le concept de vie privée et les réalités de ce territoire que nous explorons avec peur et tension ? Ces interrogations s'inscrivent dans le cadre de l'analyse d'une réalité à la fois sociale et juridique dans laquelle le concept de vie privée fait l'objet d'un processus continu de fluidification et de redéfinition conceptuelle.

2. Mathématiques vs. vie privée. Même Samuel D. Warren, le père visionnaire du droit à la vie privée, n'aurait pu prédire en 1890[3] que certains des calculs mathématiques les plus audacieux d'Alan Turing[4] pourraient avoir un lien direct avec la vie privée ou que ces véhicules qui démarraient en tournant la manivelle extérieure se transformeraient en véhicules surveillant les réactions comportementales de l'utilisateur afin de l'avertir qu'il est trop fatigué ou qu'il doit faire une pause-café. Il aurait semblé tout à fait exagéré à l'époque de penser que les mathématiques pouvaient avoir un lien aussi étroit avec la vie privée.

3. Le droit pénal appelé à la rescousse. Concrètement, le droit pénal est aujourd'hui invité à participer à la transformation du concept de vie privée, non seulement en tant que simple

[1] Le terme « algorithme » vient du mathématicien persan Abu Abdullah Muhammad bin Musa al-Khwarizmi (vers 780 - 850 après J.-C.), considéré comme le père de l'algèbre. Ses recherches ont influencé des domaines tels que l'arithmétique, l'algèbre, l'astronomie et la géographie, et il a été le pionnier de l'introduction du système numérique hindou dans le monde arabe et en Europe. Dans son ouvrage traduit en latin sous le titre *Algoritmi de numero Indorum*, il utilise le concept numérique du zéro. Dans l'Antiquité, ni les Grecs ni les Romains ne reconnaissaient l'existence du chiffre zéro, estimant qu'il était impossible de trouver un symbole pour « rien ». L'existence du chiffre zéro est considérée comme importante en Inde, et ce zéro numérique ou indien est considéré par les spécialistes comme l'une des innovations les plus importantes de l'humanité et le point de départ des mathématiques et de la physique modernes.

[2] Terme utilisé dans la doctrine française pour souligner la puissance de la loi face à tout défi rencontré. La toute-puissance de la loi devrait apporter des solutions rapides à toute situation qui dépasse le simple phénomène social pour entrer dans le domaine juridique.

[3] S. Warren, I. Brandeis, *The Right to Privacy,* Harvard Law Review, Vol. IV, December 15, 1890, N° 5, p.193 – 220.

[4] Alan Mathison Turing (23 juin 1912 – 7 juin 1954), mathématicien et informaticien, est considéré comme l'un des plus grands scientifiques du XXe siècle et l'un des fondateurs de l'informatique et de l'intelligence artificielle.

greffier chargé de rédiger le contrat synallagmatique conclu entre l'homme et l'algorithme[5], mais aussi en tant que notaire investi de pleins pouvoirs. La diligence du droit pénal dans le but de défendre la vie privée doit être efficace, adaptée à des situations où seul l'équilibre entre les mécanismes de réglementation juridique et l'évolution technologique est en mesure d'offrir la meilleure forme de protection. Je ne promeus en aucun cas l'idée d'une hypertrophie normative, mais je n'encourage pas non plus la passivité néfaste du législateur qui permet que le profilage de masse ou l'intrusion injustifiée des géants de l'informatique dans la vie privée ne soient qu'une source de monétisation. Je ne rejette pas non plus l'idée d'une litispendance entre la protection offerte dans l'environnement numérique et celle offerte dans la vie réelle. Les deux domaines ont pour point central la vie privée et le même droit pénal qui devrait offrir une protection.

Section 1
OBJET D'ÉTUDE: LA VIE PRIVÉE DANS LE CONTEXTE DE L'ÉVOLUTION NUMÉRIQUE

4. Tout a commencé par la question suivante : «Les machines peuvent-elles penser?»[6]. Cette question, qui en 1950 était totalement incomprise par la société, a évolué d'un simple test opérationnel[7] basé sur le jeu de l'imitation[8] à un défi d'une actualité brûlante pour la protection juridique de la vie privée[9]. Peu à peu, cette question est devenue importante non seulement pour les mathématiques et l'informatique[10], domaines qui faisaient preuve d'optimisme quant à la résolution cognitive de tout problème[11], mais aussi pour la

[5] P. Beauvais, D. Chilstein, E. Dreyer(dir.), *Le droit pénal de l'avenir*, Paris, Dalloz, 2024. p.19: « Ainsi, d'un point de vue sémantique, le terme d'algorithme est très régulièrement employé comme synonyme de l'IA. En effet, que l'on se réfère à la machine - le robot, le drone - ou à l'interface numérique - le logiciel - la technologie d'IA est une construction algorithmique qui, par le traitement de données multiples, a vocation à atteindre un objectif prédéterminé ».

[6] A. Turing, *Computing Machinery and Intelligence*, Mind, vol. LIX, n° 236, Oxford University Press, 1950, p.433-460.

[7] Pour éviter le débat philosophique et les discussions métaphysiques, Turing utilise des outils pragmatiques pour montrer si la machine peut imiter ou non le comportement humain, sans s'intéresser à ce qu'est la pensée. « Je propose de considérer la question suivante : « Les machines peuvent-elles faire ce que nous faisons (jouer au jeu de l'imitation) ? ». Cette formulation remplacera la question initiale, qui est trop dénuée de sens pour être discutée », présente Turing dans son hypothèse de travail. À l'heure actuelle, les algorithmes semblent avoir dépassé le stade du jeu d'imitation et le droit ne peut se contenter d'être un simple spectateur de cette évolution.

[8] R. M. French, *Subcognition and the Limits of the Turing Test* », Mind, vol. 99, n° 393, Oxford University Press, 1990, p.53-65.

[9] B. Rey, *La vie privée à l'ère du numérique*, Paris, Lavoisier, 2012, p.2.

[10] Le texte fondateur du concept d'Intelligence Artificielle a été adopté en 1956 lors de la conférence « The Dartmouth Summer Research Project on Artificial Intelligence » organisée par John McCarthy, Marvin Minsky, Claude Shannon et Nathaniel Rochester. Le terme « Intelligence Artificielle » a été proposé par le mathématicien John McCarthy et inséré dans le document signé par les trois autres organisateurs.

[11] A. Newell, H. A. Simon, *Human Problem Solving*, Englewood Cliffs (NJ), Prentice-Hall, 1972, p.8-15.

philosophie[12][13], et a reçu une réponse pragmatique en 1997 avec la victoire de l'ordinateur contre Kasparov[14]. Après ce moment historique, la question a été présente pendant la période du deep-learning[15][16] et est devenue omniprésente entre 2020 et 2025 avec le lancement à grande échelle des grands modèles linguistiques (large language model - LLM)[17], à l'occasion duquel Chat-GBT3 a passé le test de Turing[18] et est redevenu d'actualité. Dans ce contexte assez tumultueux, le droit a dû trouver les outils nécessaires pour réglementer cette nouvelle situation.

§1. NOTIONS ESSENTIELLES

5. Première définition juridique officielle (2024). La définition juridique du système d'intelligence artificielle[19] est apparue dans un document législatif officiel en 2024[20], 68 ans après la création du concept : «„système d'IA", un système automatisé qui est conçu pour fonctionner à différents niveaux d'autonomie et peut faire preuve d'une capacité d'adaptation après son déploiement, et qui, pour des objectifs explicites ou implicites, déduit, à partir des entrées qu'il reçoit, la manière de générer des sorties telles que des prédictions, du contenu, des recommandations ou des décisions qui peuvent influencer les environnements physiques ou virtuels».

---

[12] H. Dreyfus, *What Computers Can't Do. The Limits of Artificial Intelligence*, Cambridge (Mass.), MIT Press, 1972 (2e éd. 1992). Dans le contexte où Dreyfus a identifié quatre types d'intelligence (*Associationistic* – apprentissage mécanique, comportements simples ; *Simple Formal* – algorithmes exacts, jeux avec des règles fixes ; *Complex Formal* – jeux de type échecs, adaptation à une croissance exponentielle des combinaisons ; *Nonformal* – comportement humain quotidien, sans règles fixes, utilisation de l'intuition et résolution d'énigmes) générée par un système informatique (p.204, *op. cit.*), en essayant de prédire l'avenir de l'Intelligence Artificielle, il a évité de donner une réponse catégorique (p.203) : "But these difficulties give us no idea of the future of artificial intelligence. Even if the attempt to program isolated intelligent activities always ultimately requires the programming of the whole mature human form of life, and even if an Athene-like digital computer is impossible in principle that is, even if mature human intelligence is organized in terms of a field which is reciprocally determined by the objects in it and capable of radical revision the question still remains to what extent".

[13] R. Searle, „*Minds, brains, and programs*," Behavioral and Brain Sciences, vol. 3, no 3, 1980, p. 417–424: "Could a machine think? And that is why strong AI has little to tell us about thinking, since it is not about machines but about programs, and no program by itself is sufficient for thinking". Dans cet ouvrage, Searle soutient que seul le cerveau humain est capable de penser et qu'aucun programme créé à partir d'algorithmes ne peut remplacer cette réalité.

[14] M. Campbell, A. J. Hoane Jr., Feng-hsiung Hsu, « *Deep Blue* », Artificial Intelligence, vol. 134, Elsevier, 2002, p.57-83.

[15] Y. Lecun, Y. Bengio, G. Hinton, "*Deep learning*", Nature, 2015, 521 (7553), p.436-444.

[16] D. Silver, A. Huang, C. Maddison, *et al.*, "*Mastering the game of Go with deep neural networks and tree search"*,Nature, vol.529, 2016, p. 484–489.

[17] T. B. Brown *et al.*, "*Language Models are Few-Shot Learners*," ArXiv abs/2005.14165, 2020.

[18] C. Biever, "*ChatGPT broke the Turing test - the race is on for new ways to assess AI*", Nature, 2023.

[19] Dans *Lexique des termes juridiques 2025-2026*, sous la dir. de S. Guinchard et T. Debard, 33e éd., Paris, Dalloz, 2025, la définition de l'expression « système d'intelligence artificielle » est la suivante : « Système informatique capable d'effectuer un choix autonome, distinct de celui de la personne qui l'a conçue ou qui en a l'usage ».

[20] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle et modifiant les règlements (CE) n° 300/2008, (UE) n° 167/2013, (UE) n° 168/2013, (UE) 2018/858, (UE) 2018/1139 et (UE) 2019/2144 et les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (règlement sur l'intelligence artificielle), JOUE L, 12 juillet 2024, n° 1689 (AI Act).

6. La première loi sur la protection des données a vu le jour dans le droit allemand (1970). Le droit allemand a manifesté sa volonté d'être un précurseur[21] en matière de protection des données à caractère personnel dans le contexte de l'évolution technologique, dès 1970, avec l'adoption de la *Hessisches Datenschutzgesetz*[22] et, par la suite, avec l'adoption de la *Bundesdatenschutzgesetz* (BDSG) en 1978[23], deux actes normatifs qui ont ensuite inspiré des textes similaires dans le droit français et européen[24].

7. La première loi nationale sur la protection des données a vu le jour en Suède (1973). Il convient également de noter l'implication active du droit suédois dans l'élaboration de la première législation nationale (1973)[25] visant à protéger la vie privée dans le cadre du traitement des données par ordinateur et à créer un organisme de surveillance institutionnel[26]. Toutefois, lorsqu'ils expriment leur admiration pour cet acte normatif du droit scandinave, certains auteurs rappellent que la protection des données trouve son origine dans la Loi suédoise sur la Liberté de la Presse, adoptée en 1776[27]. Il s'agit de la première loi garantissant l'accès des citoyens aux documents publics et reconnaissant la liberté de la presse[28]. L'UNESCO[29] et le Conseil de l'Europe[30] considèrent qu'il s'agit du prototype des législations modernes en matière d'accès à l'information, qui a jeté les bases d'une culture de la transparence administrative.

---

[21] S. Simitis, *Reviewing Privacy in an Information Society*, University of Pennsylvania Law Review, vol. 135, nr. 3, 1987, p.707-746.

[22] La loi du Land de Hesse est considérée comme le premier acte normatif au monde à définir les données à caractère personnel dans le contexte du développement numérique, en énonçant des principes tels que la limitation de la finalité de leur collecte et de leur utilisation (un tel principe est ensuite utilisé pour le profilage incontrôlé), l'obligation de sécurité (anticipation du risque de failles de sécurité) ou la désignation d'une autorité indépendante chargée de leur protection. La loi peut être consultée dans sa version initiale ici: https://www.worldlii.org/int/other/NDPrivLegis/1970/1.html.

[23] *Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG*), Federal Law Gazette, BGBl, I, 2017. https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.html#p0032

[24] B. Van Alsenoy, "*National Data Protection Laws before 1980*." Chapter, in *Data Protection Law in the EU: Roles, Responsibilities and Liability*, 163–206. KU Leuven Centre for IT & IP Law Series. Intersentia, 2019.

[25] S. Öman, "*Implementing Data Protection in Law*", in Scandinavian Studies in Law, vol. 47, 2004, p.389-406.

[26] S. Öman, *op. cit.*, p.390: „The first national legislation aimed at protecting the informational privacy of individuals when their personal data are processed in computers saw the light of day in Sweden in 1973. The Swedish 1973 Data Act only covered processing of personal data in traditional, computerised registers. The act did not contain many material provisions on when and how the data should be processed, or general data protection principles. Instead, the act required for each computerised personal data register a prior permit from a new data protection authority – the Data Inspection Board".

[27] R. Wong, *The Shape of Things to Come: Swedish Developments on the Protection of Privacy.* Script-Ed, Vol. 2, No. 2, 2005. p.107-124. Available at SSRN: https://ssrn.com/abstract=924634

[28] B. Wennberg, K. Örtenhed, *Press Freedom 250 Years: Freedom of the Press and Public Access to Official Documents in Sweden and Finland – a living heritage from 1766*, Stockholm: The Riksdag of Sweden, 2018.

[29] "*The Swedish Freedom of the Press Ordinance of 1766: The world's first legislation guaranteeing free communication of information*", Unesco. https://www.unesco.org/en/memory-world/swedish-freedom-press-ordinance-1766-worlds-first-legislation-guaranteeing-free-communication?

[30] Olsson A.R., *Access to Official Documents — Issue Discussion Paper, CommDH(2012)7*, Discussion Paper du Commissaire aux Droits de l'Homme, Conseil de l'Europe, Strasbourg, 2012. https://rm.coe.int/16806da686

8. Le droit français est revenu dans la course (1978). Bien que le départ ait déjà été pris avec l'adoption de la loi innovante sur la protection des données dans le Land de Hesse (1970)[31], avec l'entrée en vigueur de la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le droit français a fait preuve d'une véritable vision en matière de collecte de données à caractère personnel en vue du profilage d'une personne par des moyens automatisés.

Ainsi, l'article 2 de la Loi Informatique, en vigueur du 23 juillet 1978 au 7 août 2004, interdit de prendre une décision sur la base d'une évaluation automatisée : « aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé ». Le même article interdit la collecte automatisée de certaines informations personnelles dans le but de rendre une décision judiciaire fondée sur l'appréciation d'un comportement humain.

9. Réaction tardive du droit roumain (2001). Contrairement à cette avancée occidentale, la Roumanie n'a pas développé de législation similaire pendant la période communiste, car le régime politique était axé sur une surveillance massive de la population, un contrôle total et illimité des données privées[32], la protection des libertés individuelles étant reléguée au second plan[33]. La mise en place d'un cadre réglementaire concernant les données à caractère personnel est apparue tardivement, seulement après le changement de régime en 1989 et dans le contexte de l'intégration européenne. La première réglementation complète se trouve dans la loi n° 677/2001 relative à la protection des personnes à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[34], adoptée pour transposer la Directive 95/46/CE. Bien qu'elle ait représenté une avancée assez tardive pour la défense du droit à la vie privée, la loi n° 677/2001 a prouvé son utilité et a introduit des obligations claires pour les opérateurs de données privées. Parallèlement, la loi n° 102/2005 a été adoptée, instituant l'Autorité nationale de surveillance du traitement des données à caractère personnel (ANSPDCP), dotée de compétences de contrôle et de sanction. De même, la loi n° 506/2004 a réglementé la protection des données dans le secteur des communications électroniques, en

[31] Des commentaires supplémentaires sur l'importance de cet acte normatif sont formulés par le professeur Alexander Roßnagel, spécialiste en droit numérique, l'un des experts les plus reconnus en Allemagne en matière de protection des données privées, sont disponibles ici : https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2023-06/HDSIG_digital.pdf

[32] M. Oprea, *Banalitatea răului. O istorie a Securității în documente (1949–1989)*, Iași/București, Polirom, 2002.

[33] D. Deletant, *Ceaușescu and the Securitate : Coercion and Dissent in Romania, 1965-1989*, Armonk (N.Y.), M. E. Sharpe, 1995.

[34] L'objectif de cette loi, énoncé dans son premier article, était le suivant : « La présente loi a pour objet de garantir et de protéger les droits et libertés fondamentaux des personnes physiques, en particulier le droit à la vie intime, familiale et privée, en ce qui concerne le traitement des données à caractère personnel. »

application de la Directive ePrivacy. L'alignement total sur la norme européenne en vigueur et, implicitement, le rattrapage du retard par rapport à l'Occident ont été réalisés grâce à l'entrée en vigueur du Règlement général sur la protection des données (RGPD) le 25 mai 2018, qui a remplacé la directive 95/46/CE.

10. Contexte social de l'apparition de la législation sur les données. Les quatre lois françaises, allemandes et suédoises sont apparues dans un contexte social assez similaire : les gouvernements cherchaient à informatiser l'administration publique en utilisant des algorithmes de traitement automatique des informations personnelles, qui devaient être utilisées principalement à des fins statistiques[35].

11. La loi de 1978, réponse à un article de presse. La situation de la France est particulière car la loi de 1978 est apparue en réaction à un article publié dans le quotidien Le Monde, le 21 mars 1974, sous le titre : « Une division de l'informatique est créée à la Chancellerie : SAFARI ou la chasse aux Français »[36]. Il présentait un projet gouvernemental connu sous le nom de SAFARI (Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus) par lequel les ministères tentaient de créer et d'interconnecter une base de données regroupant les 52 millions de Français et d'attribuer à chaque personne un numéro d'identification unique et numérique[37].

Sans prévoir que ces données deviendraient au fil des ans une véritable mine d'or pour les géants de l'informatique[38], l'auteur de l'article identifie en fait le pouvoir conféré à leur détenteur : « en effet, une telle banque de données, soubassement opérationnel de toute autre collecte de renseignements, donnera à qui la possédera, une puissance sans égale ».

§2. TRANSFORMATION DE L'IDENTITÉ EN UN CODE NUMÉRIQUE

12. Le statisticien René Carmille, inventeur du code numérique. L'histoire de cet « identifiant » est assez mouvementée, car elle est étroitement liée au nom de René Carmille[39],

---

[35] T. Naef, *The Global Reach of the Right to Data Protection. In: Data Protection without Data Protectionism*, European Yearbook of International Economic Law, vol 28. Springer, 2023.

[36] P. Boucher, *Une division de l'informatique est créée à la chancellerie "Safari" ou la chasse aux Français,* Le Monde, 1974. https://www.lemonde.fr/archives/article/1974/03/21/une-division-de-l-informatique-est-creee-a-la-chancellerie-safari-ou-la-chasse-aux-francais_3086610_1819218.html

[37] « pas un hasard non plus si le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) destiné à définir chaque Français par un "identifiant", qui ne définisse que lui, maintenant terminé, est l'objet de convoitises ardentes ».

[38] A. Rouvroy *et al.*, « *Gouvernementalité algorithmique et perspectives d'émancipation : Le disparate comme condition d'individuation par la relation?* », Réseaux, n° 177, 2013. p.163-19.

[39] René Carmille (8 janvier 1886 – 25 janvier 1945), considéré comme le père des statistiques en France, est un pionnier dans l'utilisation des cartes perforées et des lecteurs de cartes électromagnétiques. En 1930, dans le but de gérer plus efficacement le recrutement des soldats dans l'armée, il attribua à chacun un numéro d'identification à 12 chiffres, basé sur la date et le lieu de naissance. Pour atteindre cet objectif, il a repris des échantillons d'une

qui a participé à la transformation de l'identité d'une personne, composée du nom, du prénom, du lieu et de la date de naissance, en un code numérique. Concrètement, afin de construire une relation plus sûre et plus simplifiée entre l'individu et l'État, dans le but de rendre les informations statistiques plus efficaces, il a inventé[40] en 1934 le Code Numérique d'Identité destiné à l'enregistrement des futurs soldats enrôlés dans l'armée, et à partir de 1941, il l'a largement utilisé en tant que directeur du Service National de Statistique, le prédécesseur de l'INSE[41]. Il est considéré comme l'inventeur[42] du numéro d'identification connu aujourd'hui sous le nom de « Numéro de Sécurité sociale » (NIR)[43].

13. Le premier hacker éthique[44]. Les auteurs américains[45] mentionnent René Carmille comme ayant joué un rôle important dans la protection des données et de la vie privée[46], étant le premier hacker éthique à avoir manipulé les données personnelles de la population, traitées dans un système automatisé[47].

14. Manipulation des données privées. Pendant l'occupation nazie, le nouveau gouvernement de Vichy a demandé à l'officier statisticien de fournir un registre numérique sur le nombre de Juifs et d'étrangers[48], et celui-ci a falsifié les données du recensement afin que la religion ne figure pas dans ces colonnes des cartes perforées[49]. Ainsi, en évitant d'inscrire

---

carte perforée à 80 colonnes réalisée par une filiale allemande d'IBM, afin qu'elle soit fabriquée par la société française Bull. Il s'agissait d'une tentative primitive d'utiliser une machine pour gérer des quantités de données qui, jusqu'alors, étaient conservées dans des registres classiques.

[40] G. Lang, « *Éléments pour une histoire du Numéro de sécurité sociale* », Statistique et société, n° 6, 2018. En mémoire d'Alain Desrosières, 2018. p.37-45.

[41] L'Institut National de la Statistique et des Études Économiques a été créé un an après la mort de René Carmille, sur les bases qu'il avait posées.

[42] M.-L. Lévy, « *Le numéro d'identité* », in Population et Sociétés, n° 232, Paris, INED, 1989. p.1-4.

[43] INSEE, *The National Register for the Identification of Individuals (RNIPP) at the core of French administrative life* − Courrier des statistiques n° 8, 2023. https://www.insee.fr/en/information/6692672?sommaire=6692684

[44] M., Wills, *WWII and the First Ethical Hacker*, JSTOR Daily, 2017. https://daily.jstor.org/wwii-and-the-first-ethical-hacker/. Étant donné que l'utilisation du terme « hacker » peut être considérée comme inappropriée dans le contenu de l'article, il est mentionné que : "While Carmille didn't re-write code or introduce a bug in the system, his "hacking" was akin to sabotage, throwing a bureaucratic wrench into the machine".

[45] E. Black, *IBM et l'Holocauste. L'alliance stratégique entre l'Allemagne nazie et la plus puissante multinationale américaine*, trad. de l'anglais par Odile Demange, Paris, Robert Laffont, 2001, 595 p. Ce travail du journaliste d'investigation américain a fait connaître René Carmille dans le monde entier et lui a attribué des qualités de héros, en raison de la manière dont il a géré les données privées de la population.

[46] D. Harshbarger, *A Quiet Hero. A Novel of Resistance in WWII France*, Herndon (VA), Mascot Books, 2019, 376 p. Il s'agit d'un roman historique qui transforme en fiction le livre d'Edwin Black et donne une personnalité légendaire à René Carmille en le présentant comme le sauveur de dizaines de milliers de Juifs, grâce à la dissimulation des données personnelles de ceux qui devaient être arrêtés.

[47] A. Davis, *A History of Hacking*, The Institut, 2015.

[48] L. Heide, *Monitoring People: Dynamics and Hazards of Record Management in France*, *1935-1944,* Technology and Culture, 45(1), 2004.p. 80–101.

[49] A. Davis, *op. cit.* : "After the invasion, the pro-Nazi Vichy government ordered a nationwide census. Carmille requested the assignment of compiling data from the census forms onto tabulator cards for analysis. His group transferred the data, including information from Column 11—where citizens were asked to indicate their religion—onto tabulator cards. They were instructed by the Nazis to sort the cards and print a list of all Jews living in France so that they could be located and sent to concentration camps. Over the course of two years, Carmille and his group purposely delayed the process by mishandling the punch cards".

certaines données personnelles dans les registres (lieu de naissance, nationalité, religion), de nombreux Juifs ont été sauvés de la mort.

15. Mécanographie. Dans le même temps, sur la base des informations centralisées sur ces cartes perforées, des soldats ont été identifiés et recrutés pour faire partie de la Résistance française. Le nom de René Carmille est associé aux mécanismes d'utilisation de quantités massives de données privées[50], précurseur du Big Data actuel. Il a réussi à dissimuler la véritable identité des Juifs en utilisant la mécanographie[51].

16. Controverses. D'autre part, les historiens français[52] manifestent leur réticence[53] à l'égard de l'activité de René Carmille en ce qui concerne l'utilisation de la technologie inventée par IMB (cartes perforées) pour identifier les futures victimes de l'antisémitisme[54]. Selon un rapport réalisé en 1998 à la demande du directeur de l'INSEE[55], la collecte de données par le SNS pendant l'occupation nazie a représenté un facteur de risque pour l'exercice des libertés fondamentales[56] et a été considérée dans certains cas comme un instrument de répression de la population, de type para-policier[57].

17. Le point zéro pour l'apparition de l'*homo numericus*. Nous avons considéré que l'activité de René Carmille était importante, car c'est à ce moment-là que le nombre est devenu un substitut de la personne.

---

[50] A. Dignat, « *René Carmille (1886-1945) – La Résistance au bureau des statistiques* », Herodote.net, 2021: « *sous l'Occupation, le polytechnicien René Carmille fut le précurseur de l'usage massif des données en France. Il mit en place le Service national de statistiques (SNS) qui deviendra plus tard l'INSEE. Il inventa aussi le numéro de sécurité sociale* ».

[51] Elle est considérée l'ancêtre de l'informatique telle qu'on la connaît aujourd'hui. Le Dictionnaire de l'Académie Française définit le terme ainsi : « *utilisation de machines et de procédés mécaniques dans les opérations de dépouillement et de tri de documents administratifs, comptables, etc*. ».

[52] Annette Wieviorka, spécialiste de l'histoire de l'Holocauste, commente la présentation faite par les auteurs américains, affirmant que les travaux de Carmille sont controversés : « *Alors que l'homme est controversé (résistant incontestable, il est déporté à Dachau où il meurt, mais son rôle dans les affaires juives reste douteux), Black en fait un personnage jouant double jeu*. » (https://www.lemonde.fr/archives/article/2001/02/13/un-beau-sujet-gache_4182313_1819218.html)

[53] La gestion des fichiers individuels par la statistique publique : des précédents et des controverses (3/3), Statistique publique – Histoire, CGT-Insee-Genes, 21 mai 2021, accessible à l'adresse : https://www.cgtinsee.org/statistique-publique/histoire-118/article/la-gestion-des-fichiers-individuels-par-la-statistique-publique-des-precedents-426#nb6

[54] Dans une étude publiée dans *Cercle de généalogie juive*, bulletin n° 23, 1990, sur Serge (journaliste d'origine allemande) et Beate Klarsfeld (historienne d'origine roumaine), deux « chasseurs de nazis » qui ont contribué à prouver certains crimes de guerre, le statisticien Michel-Louis Lévy a décrit René Carmille comme un « *héros imprudent et quelque peu mégalomane* ».

[55] J.-P. Azéma, R. Lévy-Bruhl, B. Touchelay. *Mission d'analyse historique sur le système statistique français*, [Rapport de recherche] INSEE. 1998.

[56] J.-P. Azéma, *op. cit.* p.60: « *Mais de nombreuses voix s'étaient élevées dans le jeune INSEE pour protester contre la «mise en fiches»* de la population jugée dangereuse pour l'exercice des libertés individuelles. »

[57] *Ibidem*, « *SNS franchit la ligne jaune et fonctionne, au moins indirectement, de manière para-policière*" (p.56), „*élaboré des instruments qui auraient pu être utilisés à des fins directement répressives* » (p.57).

La figure de René Carmille est pertinente en tant que tournant où le nombre commence à se substituer à la personne, préfigurant le monde de l'*homo numericus*[58]. Son histoire fonctionne comme une étude de cas sur la manière dont la comptabilisation et la classification numérique ont produit un nouveau régime d'identité et la possibilité de l'existence d'un nouveau sujet de droit. En ce sens, l'épisode Carmille devient le point de départ de la transition vers l'identité numérisée. Et, à mesure que la configuration sociale a ainsi changé, le droit pénal a été appelé, à chaque fois, à recalibrer sa fonction protectrice et ses limites d'intervention, afin de répondre aux nouveaux risques et vulnérabilités générés par cette mutation.

18. Identification numérique en Roumanie (1978). En Roumanie, la transformation de l'identité en un numéro a eu lieu en 1978, par un décret émis par le Conseil d'État[59]. L'attribution du Code Numérique Personnel (CNP) à l'ensemble de la population s'est faite par l'enregistrement d'un numéro à 13 chiffres dans « les documents d'identité, d'état civil et autres documents personnels ». L'organisation de cette numérotation de la population a été assurée par le Ministère de l'Intérieur, le Comité pour les problèmes des conseils populaires et la Direction centrale des statistiques. L'attribution du CNP visait à éviter les confusions causées par des noms similaires, à intégrer les citoyens dans un système informatisé d'enregistrement, à permettre une surveillance plus efficace de la population et, dans le même temps, à aligner la Roumanie sur les tendances internationales.

§3. LE DROIT PÉNAL FACE À L'*HOMO NUMERICUS*

19. Le droit numérique - des principes similaires au droit canonique médiéval ? Bien que la comparaison puisse sembler quelque peu exagérée, le droit du développement technologique contemporain fonctionne de plus en plus comme un droit parallèle, avec ses propres sources, objectifs et sanctions, à l'instar de l'autonomie historique du droit canonique[60] par rapport au droit laïc[61].

[58] Cette appellation apparaît pour la première fois dans un document officiel de l'État, dans un projet de loi datant de 2009. « Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique, Rapport n° 330 (2009-2010) ». Nous retrouvons cette appellation dans la littérature juridique antérieure à cette période. P. Josephe, *La société immédiate : Paris, Calmann-Lévy, 2008*, *Questions de communication*, n° 14, 2008. Étonnamment, ce nouveau type de personnalité avait déjà été anticipé dès 1997 – N. Negroponte, *L'Homme numérique*, Paris, Éd. Pocket, 1997.

[59] Décret n° 59 du 2 mars 1978 modifiant la loi n° 5/1971 relative aux documents d'identité et au régime du changement de domicile, Journal officiel n° 15 du 4 mars 1978.

[60] A. Winroth, J. C. Wei (dir.), *The Cambridge History of Medieval Canon Law*, Cambridge–New York, Cambridge University Press, 2022.

[61] C. Lovisi, *Introduction historique au droit*, 6e éd., Paris, Dalloz, coll. « Cours », 2022, p.166.

Au cours de la sombre période du Moyen Âge, il existait même un droit pénal canonique qui fonctionnait selon ses propres règles[62], avec des styles d'argumentation, « métaphoriques ou allégoriques », différents du droit séculier.

Le droit pénal actuel doit reconnaître l'existence de l'*homo numericus*, tant du point de vue de la « personne lésée » que de celui de l'« agresseur », dans un monde où la « lex informatica »[63] connaît une dynamique accélérée. En fait, l'étape de la reconnaissance est déjà dépassée, le nouveau paradigme n'étant pas seulement celui qui consiste à trouver les mécanismes de défense de l'*homo sapiens* contre l'*homo numericus*, mais aussi celui qui consiste à défendre l'*homo numericus* contre son propre « moi ».

20. La délinquance se transfère-t-elle de l'être humain à sa « création » ? Lorsque nous discutons de la « dangerosité » de l'*homo numericus*, les règles qui sous-tendent le développement du droit pénal[64] s'appliquent exactement, la prédisposition à la délinquance étant un attribut de l'être humain[65], mais aussi de sa « création ».

21. « Les symptômes de l'état de dangerosité »[66]. Avant d'interdire un acte répréhensible et de transformer cette interdiction en infraction, il faut impérativement que le filtre de l'état de dangerosité de chaque individu ou des masses[67] fonctionne, le droit pénal étant *ultima ratio*[68], conformément au principe de subsidiarité[69]. Si nous reprenons l'argumentation d'André Decocq[70] et analysons les « symptômes de l'état de dangerosité » qui sont visibles dans la société

---

[62] C. Lovisi, *op. cit.*, p. 167 : *« Pour autant, les deux droits ne se confondent pas. Le droit pénal en donne un bon exemple. L'Église a son propre droit pénal, applicable à certaines personnes et à certaines infractions. Alors que le droit laïque privilégiait la répression, le droit pénal ecclésiastique vise d'abord à l'amendement du coupable car il faut sauver son âme. Les peines canoniques doivent éviter au délinquant de retomber dans le mal et lui permettre de se repentir* ».

[63] J. R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology* , 76 Tex. L. Rev. 553, 1997-1998.

[64] A. Decocq, *Droit pénal général*, 1re éd., Paris, Dalloz, coll. « Bibliothèque Dalloz », 19 juin 2025., préface de Y. Mayaud, p.18-19.

[65] D. Sznycer, C. Patrick, "*The origins of criminal law*", Nat Hum Behav, vol. 4, 2020, p.506–516.

[66] « *Mais, en tant que forte prédisposition à la délinquance, c'est-à-dire à la perpétration d'infractions, l'état dangereux provoque la crainte d'actes réprouvés, projette dans l'avenir la réprobation. Il serait faux, à cet égard, de voir en lui, à la différence de l'infraction, une conception purement scientifique du phénomène criminel : l'analyse des causes et les symptômes de l'état dangereux est certes scientifique, mais la notion de danger, liée à celle d'infraction, a, tout comme elle, des racines émotives. C'est ce qui explique le caractère de coercition sur la personne qui s'attache à la mesure de sûreté : elle est la rançon de la crainte*. », A. Decocq, *op. cit.*, p.19.

[67] « *De plus, pour être passible de sanctions pénales, l'acte illicite en question doit constituer une violation d'une règle d'importance fondamentale pour la coexistence des personnes dans une société civilisée et démocratique. Par conséquent, lorsque nous pensons au droit pénal, nous avons généralement à l'esprit des comportements qui portent gravement atteinte à l'autonomie personnelle.* », W. Wohlers, "*Criminal Law as a Regulatory Tool*", in M. Dyson, B. Vogel (Eds.), *The Limits of Criminal Law: Anglo-German Concepts and Principles,* Oxford, Hart Publishing, 2020. p.235–262.

[68] E. Dreyer, « *La subsidiarité du droit pénal* », Mélanges J. H. Robert, LexisNexis, 2012, p.247.

[69] S. Van Drooghenbroeck, M. van de Kerchove, *Subsidiarité et droit pénal: aspects nouveaux d'une question ancienne,* in F. Delpérée, *Le principe de subsidiarité. Actes des journées juridiques. J. Dabin* organisées en novembre 2000 par le département de droit publique de l'Université Catholique de Louvain, Bruylant, Bruxelles 2002, p.153-159.

[70] « *Mais, en tant que forte prédisposition à la délinquance, c'est-à-dire à la perpétration d'infractions, l'état dangereux provoque la crainte d'actes réprouvés, projette dans l'avenir la réprobation. Il serait faux, à cet égard,*

actuelle, nous pouvons comprendre que le droit pénal est le seul à pouvoir offrir le meilleur traitement prophylactique mais aussi réparateur.

On trouve une explication tout aussi valable de ce type d'argumentation juridique chez Emmanuel Dreyer : « la sanction pénale, par sa force symbolique et réelle, doit être réservée aux hypothèses les plus graves dans lesquelles la société entend marquer sa réprobation compte tenu du trouble à l'ordre public résultant ou pouvant résulter de l'acte à punir »[71].

22. La République numérique vs. moralité. Même si on vit dans une République numérique[72] que le droit français essaie de réguler[73], le droit pénal doit continuer à agir sous l'autorité du principe de moralité[74], même si l'*homo numericus* semble être une espèce guidée par l'exploitation et la monétisation des données.

J'estime que dans le contexte actuel, le droit pénal ne peut être guidé exclusivement par « le principe du miroir » – les normes ont un correspondant direct dans la morale – mais doit accepter une gouvernance basée sur le principe instrumental : « l'existence de ses normes contribue à prévenir ou à atténuer le fait moralement répréhensible »[75].

23. Le droit pénal et le miroir de la moralité. Le droit pénal à l'ère numérique ne peut être un simple miroir de la moralité, mais doit incriminer uniquement les actes de type « public wrongs »[76] qui causent un dommage, un préjudice[77] et affectent les valeurs communes de l'ordre

---

de voir en lui, à la différence de l'infraction, une conception purement scientifique du phénomène criminel : l'analyse des causes et les symptômes de l'état dangereux est certes scientifique, mais la notion de danger, liée à celle d'infraction, a, tout comme elle, des racines émotives. C'est ce qui explique le caractère de coercition sur la personne qui s'attache à la mesure de sûreté : elle est la rançon de la crainte. », A. Decocq, *op. cit.*

[71] E. Dreyer, *op. cit.*

[72] Vie publique, *Loi République numérique du 7 octobre 2016 (Loi Lemaire) : quels changements,* 2016. https://www.vie-publique.fr/eclairage/20301-loi-republique-numerique-7-octobre-2016-loi-lemaire-quels-changements

[73] LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique, a les principes directeurs suivants : circulation des données et des connaissances, protection des droits dans la société numérique et accès de tous au numérique.

[74] L. Fuller, "*The Morality of Law"*, (rev edn,) Yale University Press 1969.

[75] J. Edwards et al., "*The Internal Morality of Criminal Law*", in Oxford Journal of Legal Studies, 43, 2023. p 475 – 496.

[76] « Une faute publique est une faute qui porte atteinte à l'ordre civil de la communauté politique : c'est une faute qui préoccupe légitimement le public, c'est-à-dire les membres de la communauté en tant que citoyens, car elle attaque ou sape les valeurs ou les institutions qui contribuent à la constitution de cet ordre. » (p. 7) - R. A. Duff, "*Legal Moralism and Public Wrongs*", dans K.K. Ferzan et S.J. Morse (dir.), *Legal, Moral, and Metaphysical Truths: The Philosophy of Michael S. Moore*, Oxford, Oxford University Press, 2015, p.3-20

[77] Développant son argumentation juridique sur la base des travaux de H. Donnedieu de Vabres, *Traité élémentaire de droit criminel et de législation pénale comparée,* préc n° 89 et de M. Lacaze, *Réflexions sur le concept de bien juridique protégé par le droit pénal*, LGDJ Fondation Varenne Collection des Thèses n° 39 2010, préf A. D'hauteville, n° 23, G. Rabut-Bonaldi soutient que le rôle du préjudice dans la théorie de l'infraction doit être analysé tant du point de vue de l'auteur que du législateur. Ainsi, dans l'ouvrage *Le préjudice en droit pénal*, Paris, Dalloz, coll. « Nouvelle Bibliothèque de Thèses », n° 159, 1ère éd., 13 avr. 2016, (préface de J.-C. Saint-Pau), l'auteur soutient : « La notion d'infraction renvoie ainsi à deux réalités. Il s`agit d`abord du texte pris par le législateur donnant à tel ou tel comportement une qualification pénale et le sanctionnant d`une peine c`est l`infraction du législateur. Il s`agit ensuite du comportement lui même violant la norme pénale et portant atteinte à son objet de protection c`est l`infraction du délinquant. » (p.31)

public[78]. Tout acte antisocial n'engendre pas en soi une responsabilité pénale, sans être « textualisé » par le droit pénal - « aucune attitude, aussi perturbatrice soit-elle pour l'ordre social, ne peut donner lieu à une réaction pénale si cela n'a pas été prévu par un texte de droit »[79].

Section 2
CONCEPTUALISATION: LE NOUVEAU RAPPORT ENTRE ORDRE PUBLIC ET VIE PRIVÉE

24. Redéfinir la notion d'ordre public[80]. La recherche et surtout la redéfinition de l'ordre public dans la société numérique et algorithmique impliquent une réflexion sur la manière dont le bien commun peut être protégé face aux nouveaux risques générés par la collecte massive de données et l'intelligence artificielle, ce qui implique de trouver un équilibre entre les libertés individuelles et les impératifs de la sécurité numérique.

Dans cette redéfinition de la notion, nous devrions également accepter le danger comme le nouveau type de justice, ultra-personnalisée et de plus en plus présente, juger les individus en fonction du risque de dangerosité établi par des algorithmes, en reléguant au second plan l'acte présumé antisocial et en ignorant la présomption d'innocence[81].

§1. L'ORDRE PUBLIC, UNE NOTION AMBIGUË ET IMPRÉVISIBLE

25. L'intérêt général. L'ordre public découle de l'intérêt général de la société et peut être considéré comme une sous-catégorie de celui-ci[82], les deux concepts ne devant pas être

[78] A.P. Simester, A. von Hirsch, *Crimes, Harms, and Wrongs: On the Principles of Criminalisation*, Oxford, Hart Publishing, 2011. L'idée centrale de cet ouvrage est qu'en l'absence d'un préjudice public, tout acte immoral ne doit pas nécessairement relever du droit pénal et que le but de la peine n'est pas de purifier moralement un individu, mais de rétablir les valeurs fondamentales qui ont été affectées. Les auteurs proposent quatre conditions pour incriminer un acte : le comportement doit être répréhensible ; il doit causer un préjudice ; le préjudice résultant du comportement répréhensible doit être attribué à l'auteur ; l'incrimination est le meilleur instrument juridique pour obtenir réparation.

[79] M.-L. Rassat, *Le droit pénal*, 2e éd., coll. « Connaissance du droit », Dalloz, Paris, 2025, p.21.

[80] *Lexique des termes juridiques 2025-2026*, sous la dir. de S. Guinchard et T. Debard, 33e éd., Paris, Dalloz, 2025, p 793: « Vaste conception d'ensemble de la vie en commun sur le plan politique et juridique. Son contenu varie selon les régimes politiques. À l'ordre public s'opposent, d'un point de vue dialectique, les libertés individuelles dites publiques ou fondamentales et spécialement la liberté de se déplacer, l'inviolabilité du domicile, les libertés de pensée et d'exprimer sa pensée. L'un des points les plus délicats est celui de l'affrontement de l'ordre public et de la morale. »

[81] A. Garapon, J.-L. Lassègue, *Justice numérique : révolution graphique et rupture anthropologique*, Paris, Presses universitaires de France (PUF), 2018.

[82] E. Barbin, *La protection directe de l'intérêt général par l'administration : la mise en œuvre de la police administrative préventive*, mémoire de Master 2 Droit public, Université Jean-Moulin Lyon 3, n° 23, 2016, p.64.

confondus[83]. Même si les défis d'aujourd'hui sont différents de ceux qui existaient au moment de l'adoption de la Déclaration des droits de l'Homme et du Citoyen de 1789, l'article 4 de cet acte juridique reste tout aussi pertinent pour définir la notion d'ordre public, en particulier lorsqu'il est enfreint : « la liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui : ainsi, l'exercice des droits naturels de chaque homme n'a de bornes que celles qui assurent aux autres Membres de la Société la jouissance de ces mêmes droits. Ces bornes ne peuvent être déterminées que par la Loi »[84].

26. Notion imprévisible pour la vie privée. Il est évident que l'ordre public est une notion essentiellement fonctionnelle[85], par laquelle l'État doit garantir le respect des droits et libertés de chaque individu[86], et le droit a l'obligation de trouver l'équilibre qui crée cet « état dans lequel les libertés s'exercent le mieux »[87]. Lorsque nous discutons de l'ordre public dans le contexte de la protection de la vie privée ou de la liberté d'expression, cette notion devient particulièrement imprévisible[88].

27. Trouble à l'ordre public, interface entre la société et la procédure pénale. Étonnamment, dans le droit pénal procédural français, l'ordre public n'est pas seulement utilisé pour justifier des mesures préventives, pour fonder l'intérêt de la poursuite pénale ou pour limiter certaines libertés, mais il est également utilisé comme interface entre la société et la

---

[83] J. Heron, « *Rapport français* », in *L'ordre public*, Association Henri Capitant, Journées libanaises, LGDJ, 2001, p.944.

[84] L'esprit révolutionnaire français a consacré l'idée que chaque être humain doit vivre et agir librement, en exerçant pleinement ses droits, ce qui constitue le fondement de la notion moderne d'ordre public. Les limites de cette liberté ont ensuite été fixées par l'Assemblée Constituante, qui a compris que cette liberté ne pouvait être tout à fait absolue, car elle risquerait de menacer la liberté d'autrui et l'équilibre social (voir J. Petit, « La police administrative », in P. Gonod, F. Melleray, et P. Yolka (dir), *Traité de droit administratif*, T. 2, Dalloz, 2011, p.6.). De cette tension entre l'idéal de liberté et la nécessité de protéger la communauté est née la conception juridique de l'ordre public, attribuée à l'État comme mission d'assurer une coexistence qui garantisse à la fois les libertés et les droits de tous.

[85] P. Malaurie, cité par M. Gautier dans « L'ordre public », in J-B Auby (dir), *L'influence du droit européen sur les catégories du droit public*, Dalloz, 2010, p.325.

[86] À titre d'exemple, nous estimons pertinente une intervention du Conseil d'État du 9 janvier 2024, affaire n° 374508, qui a interdit le spectacle de stand-up comedy que le comédien Dieudonné M'Bala M'Bala devait donner à Saint-Herblain. Initialement, le spectacle avait été interdit par le préfet, mais sa disposition avait été contestée devant le Tribunal Administratif de Nantes. La juridiction avait suspendu l'acte administratif et estimé que le spectacle pouvait avoir lieu, car sinon la liberté d'expression serait portée atteinte. C'est dans ce contexte qu'est intervenu le Conseil d'État, qui a présenté comme principal motif d'interdiction du spectacle la gravité des risques de troubles à l'ordre public : « Le juge des référés du Conseil d'État a considéré qu'en se fondant sur les risques que le spectacle projeté représentait pour l'ordre public et sur la méconnaissance des principes au respect desquels il incombe aux autorités de l'État de veiller, le préfet de la Loire-Atlantique n'avait pas commis, dans l'exercice de ses pouvoirs de police administrative, d'illégalité grave et manifeste ». En substance, le problème principal était que le spectacle comportait de nombreuses attaques racistes, antisémites, discriminatoires et contre la dignité humaine.

[87] B. Seiller, « *La notion de police administrative* », in RFDA, 2015, p.877.

[88] C. Bigot, « *Pratique du droit de la presse 2023-2024* », 4e éd., collection Hors collection Pratique du droit de la presse, Paris, Dalloz, 2023.p.113.

procédure pénale[89]. Ce rôle d'interface se manifeste dans le Code de procédure pénale par l'expression « trouble à l'ordre public ».

Cette notion a été introduite à l'article 11, paragraphe 3, du Code de procédure pénale afin de justifier la communication au public par le parquet de certains éléments du dossier. En introduisant une dérogation au principe du secret de l'instruction établi au paragraphe 1 du même article, le parquet bénéficie d'une grande liberté d'appréciation, sans pouvoir être véritablement blâmé pour son refus ou, au contraire, pour la divulgation de certaines informations à l'opinion publique[90].

28. Vérification administrative de l'identité. L'ordre public est également invoqué, en vertu de l'article 78-2 du Code de procédure pénale, y compris lorsque l'identité d'une personne est vérifiée, par exemple, simplement parce qu'elle a été arrêtée dans la rue par des agents de police. Cette vérification d'identité peut avoir un caractère judiciaire, répressif, lorsqu'il existe déjà une enquête pénale visant à prouver une infraction, et un caractère préventif ou administratif lorsqu'il s'agit de lutter contre une infraction potentielle.

Certains auteurs soulignent que sous le prétexte d'un contrôle administratif motivé par la protection de l'ordre public, l'identité de toute personne peut être vérifiée sans qu'il y ait d'élément suspect : « en présence de circonstances particulières qui doivent être justifiées par les autorités et qui établissent ce risque d'atteinte à l'ordre public, peut ainsi être contrôlée l'identité de toute personne, quel que soit son comportement »[91].

29. Impossibilité de définition. D'autre part, la doctrine française critique assez largement l'utilisation de la notion d'ordre public par le droit pénal, notamment en raison de l'impossibilité de la définir avec précision : « nul n'a jamais pu en définir le sens, chacun en vante l'obscurité et tout le monde s'en sert »[92]. Bien qu'elle soit contestée précisément en raison de son caractère « vague »[93], la notion d'ordre public est invoquée comme argument suprême tant pour légitimer les nouveaux mécanismes basés sur des algorithmes, utilisés dans la lutte contre la criminalité, que pour élaborer des normes juridiques pénales adaptées à la société numérique.

---

[89] J. Bossan, *L'intérêt général dans le procès pénal*, thèse de doctorat (Droit privé et sciences criminelles), Université de Poitiers, soutenue en juin 2007 sous la direction de M. Michel Danti-Juan.

[90] B. Bouloc, *Procédure pénale*, 29e éd., collection « Précis » (Droit privé), Dalloz, Paris, publié le 30 novembre 2023, p.749 : « pour éviter la propagation d'informations inexactes ou mettre fin à un trouble à l'ordre public, ou pour tout autre impératif d'ordre public, le procureur peut d'office ou à la demande du juge d'instruction ou des parties, rendre publics des éléments objectifs tirés de la procédure ne comportant pas d'appréciation sur le bien fondé des charges retenues contre les personnes mises en cause ».

[91] P. Conte, S. Detraz, J. Larguier, *Procédure pénale*, 26e éd., collection « Mémentos », Dalloz, Paris, publié le 21 septembre 2023. p.140.

[92] P. Malaurie cité par M. Gautier dans « *L'ordre public* », in J-B Auby (dir), *L'influence du droit européen sur les catégories du droit public*, Dalloz, 2010. p.317.

[93] J. Dumont, « *Fasc. 20 : Contrôle judiciaire et détention provisoire, Art. 137 à 150* », J.-Cl. proc. pén., 2001. p.43.

§2. CONTROVERSES. UNE NOTION ÉLASTIQUE ET DÉROUTANTE

30. Contestation véhémente. Le point le plus contesté est l'invocation « passe-partout »[94] de la perturbation de l'ordre public dans le contexte de la nécessité d'émettre des mandats de placement ou de maintien en détention provisoire ou pour fixer les peines, considérée comme un moyen répressif dicté par « l'émotion »[95]. Les auteurs français soulignent également que l'ordre public ne peut être rationalisé ni « ni même conceptualisé » et qu'il reflète un état subjectif, une image instantanée de l'opinion publique, qui peut être influencée par les moyens de communication médiatiques[96].

31. L'ingérence de l'État au nom de l'ordre public. D'autre part, il ne faut pas oublier que c'est précisément au nom de l'intérêt public, « qui commande de préserver l'ordre public et d'assurer le bon fonctionnement de la justice »[97], que l'ingérence des acteurs étatiques est légitimée. Lorsque l'ingérence de l'État était arbitraire et non réglementée par des normes claires, la CEDH est intervenue tant dans le cas de la France[98] que dans celui de la Roumanie[99].

---

[94] W. Jeandidier, « *Détention provisoire, Convention européenne des droits de l'homme et Code de procédure pénale, ou valse-hésitation de la Chambre criminelle* », RS crim. 1986. p.718.

[95] J. Pradel, *« La réforme de la détention provisoire (commentaire de la loi no. 70-643 du 17 juillet 1970)* », Gaz. Pal. 1972, I, doc., p.10.

[96] A. Dorsner-Dolivet, *« Les dispositions de la loi du 15 juin 2000 renforçant les garanties judiciaires en matière de détention provisoire* », Dr. pén. 2000. chro. 39 p.8.

[97] C. André, *Droit pénal spécial*, 7e éd., Paris, Dalloz, 2024, p.253.

[98] Dans les années 1980, en l'absence d'une réglementation claire, les autorités judiciaires et administratives françaises ont fréquemment recouru aux écoutes téléphoniques, alors considérées comme de simples actes de police judiciaire, autorisés par le Parquet ou le Ministère de l'Intérieur. Cette pratique était critiquée pour son manque de transparence et le risque d'ingérence arbitraire dans la vie privée, car il n'existait aucune garantie procédurale quant à la durée, aux limites et au contrôle de ces mesures. La situation a été portée devant la Cour européenne des droits de l'homme dans les affaires Kruslin c. France et Huvig c. France (24 avril 1990), où il a été constaté que la législation française n'offrait pas « de garanties suffisantes contre les abus », violant ainsi l'article 8 de la Convention européenne des droits de l'homme. En réaction directe à ces condamnations, le législateur pénal français a adopté la loi du 10 juillet 1991 relative au secret des communications par télécommunications, qui a instauré pour la première fois un cadre réglementaire détaillé. Cette loi a réglementé les conditions, la durée, l'autorité compétente et le contrôle judiciaire des interceptions, transformant une pratique jusqu'alors arbitraire en une ingérence admissible et justifiée, lorsqu'elle était exercée dans les limites de la loi.

[99] Avant 1989, la surveillance de la population roumaine était un sujet qui aurait pu remplir des bibliothèques entières. Dans un régime dictatorial, les interceptions des conversations, la lecture des lettres, les filatures et d'autres moyens d'intrusion constituaient les meilleures armes pour contrôler la population. Après cette période, les modifications apportées aux règles de procédure pénale ont été assez insuffisantes, et les interceptions dans les affaires pénales portant sur des infractions graves étaient en grande partie effectuées par le Service roumain de renseignement en vertu de la loi n° 51/1991 sur la sécurité nationale. La procédure manquait de transparence et le contrôle judiciaire était minimal, ce qui a suscité des soupçons d'ingérence arbitraire dans la vie privée. Cette situation a été sanctionnée par la Cour européenne des droits de l'homme dans l'affaire Dumitru Popescu c. Roumanie (n° 2) (26 avril 2007), où il a été constaté que la législation nationale n'offrait pas de garanties suffisantes contre les abus, en violation de l'article 8 de la CEDH. Ces critiques ont été reprises dans l'arrêt Bucur et Toma c. Roumanie (8 janvier 2013), dans lequel la Cour a dénoncé l'absence de contrôle démocratique sur les interceptions et le rôle excessif des services de renseignement, mais aussi la sanction d'un lanceur d'alerte qui avait révélé des abus. À la suite de ces condamnations, la Roumanie a été contrainte de modifier sa législation. Le code de procédure pénale adopté en 2014 a introduit un mécanisme plus rigoureux d'autorisation des écoutes par le juge

32. Cas justificatif. Avec l'adoption de la loi du 10 juillet 1991[100], l'enregistrement judiciaire ou administratif des conversations téléphoniques, même s'il constitue une intrusion dans la vie privée, est autorisé par la loi et devient ainsi un cas justificatif[101]. La présente étude a accordé une attention particulière à l'intrusion de l'État dans la vie privée sous toutes ses formes[102], en présentant notamment une évolution diachronique depuis les perquisitions domiciliaires[103] abusives jusqu'à la surveillance réalisée par des algorithmes**.**

33. Conclusion - l'ordre public à l'ère numérique : « mystérieuse et d'une déroutante élasticité ». Comme on peut le comprendre à partir de l'argumentation ci-dessus, le champ de bataille pour ce type de débat se trouve dans les salles d'audience, devant les tribunaux. C'est essentiellement là que s'opère la distinction entre ce qui constitue une véritable violation de l'ordre public et de l'intérêt général et ce qui, au contraire, ne peut être qualifié comme tel. Le présent travail analyse un nombre important de décisions judiciaires et, compte tenu des contradictions constatées, des annulations des cours de contrôle judiciaire, des revirements jurisprudentiels, mais aussi des différences d'interprétation de la notion d'« ordre public » dans le droit pénal français et roumain, cette caractéristique du concept se confirme : « mystérieuse et d'une élasticité déconcertante »[104].

---

des libertés, et la décision n° 51/2016 de la Cour constitutionnelle roumaine (CCR) a retiré au SRI les instruments juridiques lui permettant d'effectuer une surveillance technique, car il ne s'agissait pas d'un organe judiciaire et il ne pouvait pas mener d'actes de poursuite pénale. Le débat public s'est encore intensifié lorsque le Ministère de la Justice a découvert que, même après cette décision de la CCR, les agents du SRI continuaient à administrer des preuves dans les dossiers pénaux, affectant ainsi l'indépendance des procureurs, sur la base de protocoles secrets et illégaux.

[100] Loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, Journal officiel de la République française, n° 162 du 13 juillet 1991.

[101] C. André, *op. cit.*, p.253.

[102] Voir le chapitre « *L'ingérence de l'État dans la vie privée. L'adaptation du droit pénal à l'évolution technologique* ».

[103] *Et domus sua cuique est tutissimum refugium* (« *La maison de chacun est son refuge le plus sûr* ») est une expression encore couramment utilisée aujourd'hui, qui trouve son origine dans un discours prononcé en 1628 par Sir Edward Coke, avocat et homme politique anglais. Il évoquait l'affaire Semayne de 1604, dans laquelle un citoyen anglais avait contesté la perquisition de son domicile par un agent de l'État. C'est la première fois qu'un tribunal établit qu'une perquisition doit être effectuée avec une autorisation préalable et ne doit pas être arbitraire. Cet événement a contribué à l'introduction de règles claires concernant les perquisitions dans le quatrième amendement de la Constitution des États-Unis d'Amérique.

[104] W. Jeandidier & J. Belot, *Les grandes décisions de la jurisprudence: procédure pénale*, coll. Thémis, Presses universitaires de France (PUF), 1986, p. 151.

Section 3

DÉFINITION ET ÉVOLUTION DES ALGORITHMES. DÉTERMINATION DU RÔLE PAR RAPPORT À LA VIE PRIVÉE

Les algorithmes, appelés à défendre l'ordre public français. L'entrée en vigueur de la loi n° 2023-380 du 19 mai 2023[105] marque un moment historique pour la France, mais aussi pour l'UE, en ce qui concerne l'utilisation des algorithmes à des fins de maintien de l'ordre public spécifique au droit pénal. Elle marque un tournant dans l'utilisation des algorithmes par le droit pénal.

L'utilisation du terme « algorithme »[106] dans le texte même de la loi semble viser à faciliter l'acceptation par la société d'une norme qui, en réalité, permet une intrusion brutale de l'État dans la vie privée.

§1. LA PREMIÈRE EXPÉRIENCE EUROPÉENNE

34. Expérience de laboratoire pour l'acceptation des algorithmes. L'organisation des Jeux Olympiques de 2024 semble avoir représenté pour la France une expérience de laboratoire[107] pour l'intégration des algorithmes dans le droit pénal[108]. Bien que l'article 10 justifie l'utilisation des algorithmes – « à titre expérimental et jusqu'au 31 mars 2025, à la seule fin d'assurer la sécurité des manifestations sportives, récréatives ou culturelles qui, par l'ampleur de leur fréquentation ou par leurs circonstances, sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes », - ces événements sportifs sont désormais terminés, mais la surveillance algorithmique est toujours en vigueur[109] et a été prolongée jusqu'en décembre 2027.

[105] Loi n° 2023-380 du 19 mai 2023 relative aux Jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, publiée au Journal officiel (J.O.) n° 116 du 20 mai 2023.
[106] La définition qu'on retrouve dans *Lexique des termes juridiques 2025-2026*, sous la dir. de S. Guinchard et T. Debard, *op. cit.*, p.62, est la suivante : « traitements automatisés destinés, notamment, à détecter des connexions susceptibles de révéler une menace terroriste ».
[107] A. Courrèges, « *Un an après* », Revue Droit administrati*f*, n° 8-9, LexisNexis, 2025. p.8.
[108] A. Lassale, « *De Big Brother à Big Data : l'avenir de la police administrative à l'ère de la vidéosurveillance intelligente* », in RFDA, 202. p.955.
[109] H. Adda, « *IA et vidéoprotection : quelles solutions pour les collectivités ?* », in AJ Collectivités Territoriales (AJCT), 2025, p.152.

35. « Police augmentée ». L'idée d'une « police augmentée » en France est apparue dès 2018, lorsque des quantités impressionnantes de données issues des dossiers de police ont été collectées et traitées de manière automatisée[110].

Par la suite, en 2020, le Ministère de l'Intérieur a apporté des précisions sur l'utilisation de l'intelligence artificielle dans le Livre blanc de la sécurité intérieure : « l'intelligence artificielle permet aux agents de se dégager d'un grand nombre de tâches répétitives, en automatisant ces tâches ».

36. Conseil d'État : la surveillance algorithmique met en danger la vie privée. Le recours officiel aux algorithmes dans le but de défendre l'ordre public[111] et de mettre en place une police du futur[112] a été rendu possible par l'entrée en vigueur de la loi n° 2023-380 du 19 mai 2023 relative à l'organisation des Jeux Olympiques, anticipant en partie ce qui va se passer avec la mise en œuvre de l'AI Act[113] d'ici août 2026. Le projet de loi a fait l'objet d'un examen par le Conseil d'État et d'un avis de la CNIL, les deux institutions précisant que la mise en œuvre de ce type de surveillance intelligente met en danger la protection de la vie privée, mais comprend en même temps une série de mécanismes de contrôle qui maintiennent les dispositions dans les limites constitutionnelles[114].

37. Rôle clé de la France dans la lutte pour la souveraineté numérique. Bien que le débat sur le droit et les algorithmes soit quelque peu étranger à la culture juridique française et plutôt spécifique à la culture américaine[115], la mise en place de caméras de surveillance augmentées peut être interprétée comme un exemple de la volonté de la France de jouer un rôle clé « sous l'effet d'une réflexion globale visant à introduire des instruments de contre -pouvoirs dans les usages de la technologie »[116].

Dans le même ordre d'idées, il ne faut pas négliger ni le moment de l'adoption de la loi Lemaire de 2016[117] sur la République Numérique, ni les ambitions de développer des

[110] X. Latour, « *Sécurité intérieure : un droit "augmenté" ?* », in Actualité juridique – Droit administratif (AJDA), 2018. p.431.
[111] C. Lequesne, « *L'intelligence artificielle et l'ordre public* », in *RFDA* 2025. p.39.
[112] A. Lassale, « *De Big Brother à Big Data : l'avenir de la police administrative à l'ère de la vidéosurveillance intelligente* », in Revue française de droit administratif (RFDA), 2024. p.955.
[113] Règlement (UE) 2024/1689 du Parlement européen et du Conseil du 13 juin 2024 relatif aux règles harmonisées en matière d'intelligence artificielle (« AI Act »), Journal officiel de l'Union européenne L, 12 juillet 2024.
[114] CNIL, *Caméras dites « intelligentes » ou « augmentées » dans les espaces publics – Position sur les conditions de déploiement*, 2022.
[115] J. Kroll, J. Huey, S. Barocas, E. Felten, J. Reidenberg, D. Robinson et H. Yu, « *Accountable Algorithms* », in University of Pennsylvania Law Review, vol. 165, 2017.
[116] C. Lequesne, *op. cit.*
[117] Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique.

technologies quantiques[118] qui garantissent le rôle stratégique de la France dans l'architecture numérique européenne et dans la compétition mondiale pour la souveraineté technologique[119].

38. Journaux attestant le motif de l'accès aux bases de données. Compte tenu du risque majeur d'intrusion non autorisée dans la vie privée, sur le plan technique, la loi n° 2023-380 du 19 mai 2023 relative à l'organisation des Jeux Olympiques prévoit la création de journaux individuels des opérations de consultation des bases de données et du motif pour lequel les agents de police les ont consultées. Il existe également un risque d'atteinte à l'autonomie décisionnelle similaire à celui des entreprises privées[120], voire des policiers impliqués dans le processus de prévention et de lutte contre les actes antisociaux, car les algorithmes dicteront ce qui semble pertinent ou non.

A. Problème d'actualité: l'identification biométrique de la population

39. La reconnaissance faciale est interdite par la loi, mais déjà utilisée dans la pratique. L'article 10 fait également référence à un aspect pertinent, à savoir que le traitement des données « n'utilise aucun système d'identification biométrique, ne traite aucune donnée biométrique et ne met en œuvre aucune technique de reconnaissance faciale ». Même si cette garantie légale est une ligne rouge à ne pas franchir[121], elle est assez contestable, car dans le cadre de la surveillance des villes sûres[122], il existe déjà des cas notoires où les autorités publiques ont acheté des logiciels de reconnaissance faciale et biométrique[123].

40. Tribunal de Grenoble (2025) : le logiciel BriefCam porte atteinte à la vie privée des habitants. La décision du tribunal de Grenoble du 24 janvier 2025 est un exemple concret de l'utilisation par les autorités publiques de logiciels basés sur des algorithmes et la reconnaissance biométrique. Le préfet du département de l'Isère a autorisé la mise en place d'un

---

[118] « *Stratégie nationale sur les technologies quantiques* », communiqué de presse, Présidence de la République, 21 janvier 2021, France 2030.

[119] *France Quantum 2025: le quantique comme enjeu de puissance pour la France* , in Portail de l'IE, 2025.

[120] P. Lokiec, « *L'intelligence artificielle est porteuse d'une profonde transformation de l'exercice du pouvoir dans l'entreprise, Gestion du personne*l », in ActuELRH, 2024.

[121] V. C. Lequesne (dir.) et J. Keller, « *Surveiller les foules. Pour un encadrement des IA "physiognomoniques*" », Rapport pour l'Observatoire de l'éthique publique, 2023.

[122] R. Challier, M. Picaud, F. Castagnino, « *De la "safe city" aux dispositifs numériques de sécurité urbaine* », in Réseaux, n° 251/3, 2025. p.11-43.

[123] La société américaine Clearview AI avait développé une base de données mondiale contenant des milliards de photos, collectées automatiquement sur les réseaux sociaux et les sites publics, afin de fournir aux forces de police et à d'autres autorités un outil de reconnaissance faciale instantanée. Toute image téléchargée pouvait être comparée à cette base de données, permettant ainsi l'identification rapide d'une personne. La CNIL a estimé que cette pratique enfreignait gravement le RGPD : il n'y avait pas de consentement, les finalités n'étaient pas déterminées et les personnes concernées n'étaient pas informées. En 2022, Clearview a été sanctionnée de 20 millions d'euros par la CNIL et contrainte de supprimer les données relatives aux citoyens français.

système de vidéosurveillance le 10 avril 2017, utilisant un traitement algorithmique des images collectées. À cette fin, le logiciel BriefCam, dont les fonctionnalités ont été testées par d'autres institutions publiques[124], a été acheté. Il permet « d'identifie[r] les hommes, les femmes, les enfants et les véhicules d'intérêt avec rapidité et précision, en utilisant la reconnaissance faciale, la similitude d'apparence »[125].

Une association de défense des droits civiques a contesté cette décision d'autorisation, mais dans un premier temps, l'action a été rejetée comme irrecevable[126] sur la base de questions relevant exclusivement de la procédure de contestation de l'acte administratif. Par la suite, un nouveau procès a été ouvert et la décision du tribunal de Grenoble est catégorique en ce sens qu'elle interdit l'utilisation du programme de reconnaissance algorithmique : « la mise en œuvre du logiciel Briefcam sur le territoire de la commune de Moirans n'a été accompagnée de la détermination d'aucune finalité déterminée et explicite et d'aucune garantie de nature à sauvegarder le droit au respect de la vie privée des administrés ».

41. Risque d'identifier les conducteurs dans la circulation. D'autre part, la CNIL a envoyé des notifications officielles, notamment au Ministère de l'Intérieur, soupçonné d'utiliser BriefCam pour identifier les conducteurs dans la circulation[127], mais aussi à d'autres mairies. Il ne faut pas non plus ignorer le risque que ces systèmes de surveillance évaluent une prédisposition à commettre un acte criminel uniquement sur la base de la détection des émotions transmises par une personne suivie de près[128].

B. La réponse de la société à la surveillance de l'État

42. Sousveillance. Ce terme désigne la pratique consistant pour les citoyens à enregistrer et à surveiller les activités des autorités ou des institutions au pouvoir à l'aide de technologies portables ou mobiles. Il est évident que ce terme vient du français et se veut l'opposé de surveillance, qui signifie « regarder d'en haut ». Sousveillance se traduit par « regarder d'en bas ». Si surveillance est le terme qui désigne la surveillance des citoyens par ceux qui sont au pouvoir, par l'État, sousveillance exprime la situation inverse dans laquelle les citoyens

[124] G. Livolsi, M. Destal, C. Le Foll, « *La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale* », in Disclose, 2023.
[125] Présentation reprise du site officiel de promotion du programme (www.briefcam.com/).
[126] G. Eveillard, « *Rejet par ordonnance – La possibilité de rejeter par ordonnance le recours contre un acte non encore né* », in Droit administratif, n° 4, avril 2024. comm. 12.
[127] S. Gérardin, « *Plusieurs mises en demeure pour l'utilisation du logiciel Briefcam* », in Dalloz actualité, 13 déc. 2024.
[128] H. Lami, « *1984, une dystopie devenue réalité ? De l'écran à l'algorithme : une brève analyse juridique* », in Revue française de droit administratif (RFDA), 2025, p. 182.

surveillent ceux qui sont au pouvoir. Il s'agit d'une forme d'autodéfense numérique, par laquelle les individus contestent les actions des acteurs étatiques, qu'il s'agisse de fonctionnaires, de politiciens, d'employés d'institutions de contrôle, etc. La définition d'un auteur est la suivante : « la sous-surveillance vise à renforcer la capacité des individus à accéder et à collecter des données sur leur surveillance et à neutraliser cette surveillance. (...) Une manière de contester et de remettre en question à la fois la surveillance et son acceptation »[129]. Parmi les pratiques les plus courantes, on trouve le fait de filmer les policiers ou d'autres fonctionnaires à l'aide d'un smartphone ou de caméras corporelles.

43. Qui surveille les surveillants ? Concrètement, grâce aux mécanismes de sous-surveillance, les individus surveillent leurs surveillants, selon le même principe que la question « Quis custodiet ipsos custodes ? ». La question semble avoir été posée pour la première fois par Juvénal, dans la Satire XV, v 331[130], dans un contexte moral et satirique : le poète dénonçait l'infidélité des épouses et ironisait sur l'inutilité des gardes, qui pouvaient eux-mêmes se révéler corrompus. À partir de cette scène domestique, l'expression a toutefois dépassé le cadre privé et est devenue, au fil du temps, un principe central de la réflexion politique et souvent même un sujet de débat juridique[131]. Elle exprime le dilemme fondamental de tout ordre social : qui garantit l'intégrité de ceux qui exercent le pouvoir ? Dans la pensée moderne, la question a été reprise dans les analyses sur la surveillance étatique, mais aussi en rapport avec la surveillance algorithmique. Foucault[132], décrivant le panoptique de Bentham[133], montre comment le pouvoir moderne voit sans être vu, générant une asymétrie qui rend la question de Juvénal encore plus actuelle. À l'ère numérique, marquée par la surveillance algorithmique et l'émergence de la sous-surveillance, cette question redevient cruciale pour comprendre le rapport entre liberté, contrôle et responsabilité démocratique.

---

[129] S. Mann, J. Nolan, B. Wellman, « *Sousveillance : Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments* », Surveillance & Society, vol. 1, n° 3, 2003. p.331–355.

[130] Juvenal (Decimus Iunius Iuvenalis) était un poète satirique romain (Ier-IIe siècle après J.-C.), auteur des 16 Satires, textes célèbres pour leur ton moralisateur et critique à l'égard de la corruption, de la décadence et de l'immoralité de la Rome impériale. Son style, souvent virulent, dénonce les excès de l'élite, les abus de pouvoir et la dégradation des mœurs.

[131] Voir le commentaire de A. Maron, « *Quis custodiet ipsos custodes* ? », Droit pénal, LexisNexis, n° 5, mai 2023; M.-H. Gozzi, « *Sed quis custodiet ipsos custodes ? – À propos de la loi du 24 juillet 2015 relative au renseignement* », *La Semaine Juridique – Édition Générale*, n° 38, 14 septembre 2015; Doussot. J.-P., « *Quis custodiet ipsos custodes ? ou de la nécessité d'évaluer l'évaluateur* », in La Semaine Juridique – Administrations et Collectivités territoriales, LexisNexis, n° 20, 16 mai 2005; É. A. Caprioli, « *Surveillance des communications électroniques à des fins de sécurité – La CEDH invalide partiellement l'ancien système britannique de surveillance électronique* », in Communication – Commerce électronique, LexisNexis, n° 1, janvier 2019; J. Laughland, *Le Tribunal pénal international : gardien de l'ordre mondial*, Paris, François-Xavier de Guibert, 2003. p.11-13.

[132] M. Foucault, *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, coll. « Bibliothèque des histoires », 1975.

[133] J. Bentham, *Panopticon; or the Inspection-House* (1791), in J. Bowring (éd.), *The Works of Jeremy Bentham*, t. IV, Édimbourg, William Tait, 1843.

C. Les algorithmes, à droite du juge

44. Les tribunaux bloquent-ils la surveillance généralisée ? À l'heure actuelle, il semble que les tribunaux jouent le rôle de contrepoids institutionnel capable de limiter l'expansion des algorithmes vers des formes de surveillance généralisée de la population[134]. Tous ces débats nous montrent que ce type de surveillance n'en est qu'à ses débuts – « le régime algorithmique policier demeure embryonnaire et soulève de nombreuses interrogations comme en atteste l'affaire relative à la vidéoprotection du pont de Saint-Nazaire »[135].

45. La neutralité des algorithmes dans le processus pénal est contestable. Le danger d'une justice dans laquelle les algorithmes font partie du processus pénal et se tiennent à la droite du juge, voire lui volent sa place, est très bien exprimé par la doctrine française en se référant à l'expérience américaine : « on frémit déjà en songeant au fait que les Américains n'ont pas hésité à promouvoir un logiciel d'évaluation des risques de récidive des condamnés aux États-Unis (COMPAS) qui vient guider la décision du juge »[136].

Les données statistiques relatives au COMPAS suscitent de sérieux doutes quant à sa neutralité[137] dans un contexte où les citoyens afro-américains se sont vu attribuer automatiquement un risque de récidive deux fois plus élevé que ceux d'autres origines[138].

46. Question difficile pour les algorithmes : punissons-nous l'homme ou l'acte ? La question classique de la criminologie – en cas de commission d'une infraction, punissons-nous l'homme ou l'acte matériel en soi ? – fait l'objet d'une importante redéfinition conceptuelle : « l'essor des algorithmes, de l'intelligence artificielle et d'une justice prédictive qui serait fondée sur les caractéristiques de chacun, pourrait bien venir renouveler l'analyse des risques de passages à l'acte et surtout des risques de récidive »[139]. Nous savons déjà que la punition de l'acte antisocial en soi ne peut avoir lieu sans analyser l'auteur, sinon nous pourrions punir un acte commis par une personne sans discernement. Dans le même temps, un comportement

---

[134] H. Adda, « *IA et vidéoprotection : quelles solutions pour les collectivités* ? », in AJ Collectivités Territoriales (AJCT), 2025, p.152: « Le risque de surveillance généralisée - traditionnellement identifié en matière de vidéoprotection se trouve ici accentué par l'analyse algorithmique et automatisée des individus filmés ».

[135] C. Lequesne, « *L'intelligence artificielle et l'ordre public* », in *RFDA* 2025, p.39. L'auteur fait référence à la saisine en novembre 2024 du département de la Loire-Atlantique auprès du tribunal administratif de Nantes afin d'utiliser la fonction de détection automatique du système de vidéosurveillance urbaine, et le tribunal a estimé qu'une telle demande n'avait aucun fondement juridique.

[136] F. Terré & N. Molfessis, *Introduction générale au droit*, 17e éd., Paris, Dalloz, 2025, p.260.

[137] M. Tonry, *« Prediction and Incapacitation* », in Doing Justice, Preventing Crime, Oxford Academic, 20 août 2020.

[138] E. Filiol, « Les risques concernant l'utilisation des algorithmes dits prédictifs dans le domaine sensible de la justice », in *Archives de philosophie du droit*, 2018, n° 60, p. 147, cité par F. Terré & N. Molfessis, *op. cit.*, p.260.

[139] F. Terré & N. Molfessis, *op. cit.*, p.260.

délictueux doit être replacé dans un contexte social en analysant particulièrement l'environnement dont est issu l'individu qui a commis l'acte, car « chacun est le produit de son environnement »[140].

§2. LA NAISSANCE DE LA SOCIÉTÉ NUMÉRIQUE, DE « ZÉRO » À « UN »

47. Terme incompris par la société. Le grand public ne comprend même pas ce que signifie ce terme, qui semble d'un côté sympathique et « à la mode », et de l'autre « permet de susciter à volonté peurs et fantasmes, et de lancer des anathèmes sans appel contre les algorithmes qui ne nous plaisent pas »[141]. Certaines études académiques[142] ont montré que le niveau de perception et d'acceptation d'un certain processus technique diffère parmi le public en fonction du terme utilisé, par exemple algorithme, intelligence artificielle, apprentissage automatique (Machine learning), robot, intelligence artificielle. Concrètement, l'interaction entre l'homme et la machine, même si elle est similaire en termes d'expérience, peut être perçue différemment selon le mot utilisé pour la définir. Par exemple, le terme « algorithme » perturbe le plus la perception, car une partie des personnes interrogées dans le cadre de l'étude l'ont perçu comme « technique » et l'autre partie comme « abstrait ».

Le mot « algorithme » semble être un mot tout à fait approprié dans le domaine du droit pénal lorsque l'on souhaite ne pas trop effrayer ceux que l'on va surveiller à l'aide de celui-ci. On comprend donc parfaitement l'adoption de ce terme dans le domaine de la procédure pénale et surtout sa transcription dans la première loi européenne qui légitime la vidéosurveillance augmentée de la population, à savoir la loi n° 2023-380 du 19 mai 2023 relative à l'organisation des Jeux olympiques de 2024.

48. Méfiance. Le baromètre numérique pour l'année 2024[143] montre que l'utilisation des outils d'intelligence artificielle a augmenté de 13 % en France par rapport à l'année précédente, pour atteindre 33 %. Le niveau de méfiance de la population à l'égard des algorithmes et de l'intelligence artificielle est assez élevé, 56 % des personnes interrogées se déclarant méfiantes.

---

[140] *Ibidem*, p.260.
[141] F. J. Matthios, *« Le Parlement autorise une expérimentation de caméras dites "augmentées" : enjeux et garanties »*, in Revue pratique de la prospective et de l'innovation, n° 1, dossier 5, 2023.
[142] M. Langer, T. Hunsicker, T. Feldkamp, C. J. König, N. Grgić-Hlača, "*Look! It's a Computer Program! It's an Algorithm! It's AI! Does Terminology Affect Human Perceptions and Evaluations of Algorithmic Decision-Making Systems* ?", in Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (CHI '22, 29 avril–5 mai 2022, New Orleans, ACM Press), New York, 2022. p.1-20.
[143] Labo Société Numérique (ANCT**),** "*What relationships do the French have with artificial intelligence*?", 2025, en ligne : https://labo.societenumerique.gouv.fr/en/articles/what-relationships-do-the-french-have-with-artificial-intelligence

Un sondage réalisé par l'Institut français d'opinion publique (IFOP) pour la CNIL a montré que 83 % des Français déclarent avoir entendu parler des algorithmes, mais seulement 31 % d'entre eux affirment savoir exactement ce qu'ils sont[144]. Ce résultat reflète un niveau élevé de sensibilisation, mais une compréhension concrète assez limitée. Le sondage a été réalisé avant le lancement de ChatGPT et l'utilisation à grande échelle de l'intelligence artificielle, et il est possible que les données ne reflètent plus la réalité d'aujourd'hui.

49. La Roumanie, le plus haut niveau de confiance dans l'UE. Une autre étude[145] menée dans plusieurs États membres montre que la Roumanie est le pays le plus réceptif de l'UE, 80 % des personnes interrogées ayant une attitude positive à l'égard de l'Intelligence Artificielle. À titre de comparaison, le taux d'approbation en France était légèrement inférieur à 50 %. Dans d'autres pays européens, le taux moyen d'acceptation de l'IA est d'environ 63 %.

En ce qui concerne le niveau de confiance dans l'IA, les répondants roumains ont manifesté une confiance de plus de 90 % dans ses avantages, suivis par les Allemands avec 82 %. La même étude montre que les citoyens européens considèrent que l'adoption par les États de lois visant à les protéger contre l'IA est une mesure prioritaire et que les universités devraient se charger du développement bénéfique des nouvelles technologies.

A. Les racines des concepts courants d'aujourd'hui

50. La genèse de l'algorithme. Puisque nous avons constaté que le droit, en particulier la procédure pénale, a adopté le concept d'algorithme, je pense que c'est le moment opportun pour faire quelques remarques supplémentaires. Au IXe siècle, le mathématicien persan Muḥammad ibn Mūsā al-Khuwārizmī a introduit le symbole positionnel « zéro » — un cercle appelé « ṣifr », c'est-à-dire vide, qui marque l'absence d'un chiffre dans un emplacement numérique[146].

Ce symbole est devenu synonyme du concept de zéro et même de la notion abstraite de chiffre[147]. Le zéro et le système positionnel hindou-arabe ont fait leur apparition en Europe

[144] C. Girardot, « *Comment enquêter sur les algorithmes* ? », in La Revue des médias, INA, publié le 29 mai 2017.
[145] T. Scantamburlo et al., "*Artificial Intelligence across Europe: A Study on Awareness, Attitude and Trust*", arXiv, 2023.
[146] G. Ifrah, *Histoire universelle des chiffres*, Paris, Robert Laffont, 1981. Il est considéré comme l'un des livres les plus influents du XXe siècle. Des questions très simples que les étudiants ont posées, « *D'où viennent les chiffres ? Qui a inventé le zéro ?* », Georges Ifrah a fait une incursion très documentée dans le passé pour prouver les réalisations du présent.
[147] C. B. Boyer, Uta C. Merzbach, *A History of Mathematics*, 2e éd., New York, Wiley, 1991.

grâce aux traductions latines des œuvres d'al-Khuwārizmī[148], et Leonardo Fibonacci[149] a consolidé leur utilisation dans le *Liber Abaci* (1202), un outil essentiel pour le commerce et la gestion au Moyen Âge.

51. Le « zéro », source des mathématiques modernes. L'apparition du chiffre zéro est devenue intéressante lorsque la société a évolué et a eu besoin de représenter des nombres de plus en plus grands : « ces types de communautés n'ont pas seulement inventé davantage de symboles, mais se sont engagés sur une voie qui a conduit à la fois à la règle fondamentale de la position et à un concept très abstrait que nous appelons « zéro », d'où proviennent toutes les mathématiques »[150].

52. La société rejette le symbole du « néant »[151]. Le Moyen Âge semble avoir été une période extrêmement tumultueuse pour le concept du zéro, certaines théories avançant l'idée que ce chiffre était considéré comme satanique : « Le zéro a pris une connotation religieuse. Le concept du néant semblait avoir un lien avec l'âme et la spiritualité. Dans de nombreux contextes, il était interdit de parler du zéro. Les gens craignaient de commettre une hérésie. (...) La notion d'un symbole représentant le néant éveillait les spectres des signes maléfiques et des œuvres de Satan »[152].

D'autre part, les détracteurs[153] de cette théorie soulignent qu'il a été interdit dans plusieurs villes italiennes par traditionalisme et par crainte de fraude.

---

[148] Al-Khwārizmī, Encyclopædia Britannica, révisé par The Editors of Encyclopaedia Britannica, consulté le 9 septembre 2024 sur Encyclopædia Britannica: https://www.britannica.com/biography/al-Khwarizmi?utm_source=chatgpt.com

[149] Léonard de Pise, également connu sous le nom de Fibonacci (vers 1170-1240), est considéré comme le plus important mathématicien européen du Moyen Âge. Intellectuellement formé en Afrique du Nord, où il est entré en contact avec des marchands arabes, il a compris la supériorité du système numérique hindou-arabe sur le système romain. Dans son célèbre *Liber Abaci* (1202), Fibonacci promeut l'introduction d'algorithmes de calcul positionnel et à zéro chiffre en Europe, révolutionnant les pratiques commerciales et comptables.

[150] G. Ifrah, *Histoire universelle des chiffres*, Paris, Robert Laffont, 1981, p 18.

[151] Le concept de « rien » a provoqué de sérieux débats non seulement en mathématiques, mais aussi dans des domaines comme la philosophie ou la physique. « Pourquoi y a-t-il quelque chose plutôt que rien ? » est la question fondamentale de la métaphysique, selon Heidegger. Une des conclusions des philosophes et des physiciens est que le « rien » absolu n'existe pas. Spinoza et Einstein affirmaient que le vide lui-même contient de l'énergie et des structures. « Rien n'est juste l'absence de quelque chose, mais ce n'est jamais vraiment rien, parce que le terme même "rien" implique "quelque chose" ». – voir "Why Is There Something Rather Than Nothing", in *Philosophy Now*, n° 125, consulté le 1er septembre 2025 : https://philosophynow.org/issues/125/Why_Is_There_Something_Rather_Than_Nothing?

[152] S. G. Krantz, *The Proof Is in the Pudding: The Changing Nature of Mathematical Proof*, New York, Springer, 2011, p. 49-51.

[153] Ph. E. Nothaft, « *Medieval Europe's Satanic Ciphers : On the Genesis of a Modern Myth* », in British Journal for the History of Mathematics, vol. 35, n° 2, 2020 – Dans l'introduction de cet article, on peut lire que : « Le but de cet article est d'étudier la genèse et le développement d'un canard historique (faux récit), que l'on peut trouver aussi bien dans de nombreuses publications de popularisation que dans certains ouvrages universitaires consacrés à l'histoire des mathématiques. Selon l'un des éléments centraux de cette histoire, le chiffre ou le symbole zéro aurait causé beaucoup d'inquiétude dans l'Europe médiévale, parce que ses propriétés inhabituelles l'auraient associé au diable ou à la magie noire. »

53. La naissance de la société numérique, de « zéro » à « un ». Au XVIe siècle, il a été accepté par la société et a joué un rôle important dans le commerce. Le chiffre zéro a donné le coup d'envoi de la société numérique actuelle grâce à Claude Shannon, considéré comme le père de l'architecture numérique moderne[154]. Il a démontré que les circuits numériques peuvent être construits à l'aide de l'algèbre booléenne[155], dans laquelle les valeurs « 0 » et « 1 »[156] (on/off, vrai/faux) sont à la base du fonctionnement de tous les systèmes électroniques modernes.

B. Identification et protection binaire

54. L'individu est identifié dans le système binaire. Ce qui a commencé comme une convention mathématique s'est transformé en une véritable révolution de la connaissance scientifique : le zéro a permis de quantifier le vide, et les algorithmes ont institué la logique pas à pas comme modèle de raisonnement[157]. La société a commencé à devenir un monde géré numériquement, un espace où l'individu est identifié, connu, anticipé et réglementé par des données collectées par un système binaire.

55. « Zéro » = protection totale de la vie privée. À l'ère numérique, cette réflexion prend une signification juridique particulière. La différence entre « zéro » et « un » n'est pas seulement arithmétique, mais ontologique : l'absence totale de données signifie une protection totale, mais l'apparition d'une seule unité d'information rompt cet équilibre.

Les algorithmes exploitent cette impossibilité du « néant » intime, transformant les traces minimes en profils complexes. La vie privée absolue devient ainsi une fiction. Certains auteurs ont exprimé des opinions assez tranchantes sur ce nouveau défi : « enfoncer une touche sur un clavier, cliquer sur une souris, faire une recherche Google, acheter sur Amazon, balayer

---

[154] C. E. Shannon, *A Symbolic Analysis of Relay and Switching Circuits*, Master's Thesis, Massachusetts Institute of Technology, 1936.

[155] L'algèbre booléenne, également connue sous le nom de logique booléenne, est un système d'exploitation formel avec deux valeurs fondamentales : 0 et 1, sémantiquement équivalentes à faux/vrai, non/oui, ou off/on. Créée par le mathématicien anglais George Boole (1815-1864), cette discipline a marqué une rupture épistémologique, en ce qu'elle parvient à formaliser le raisonnement logique en langage mathématique rigoureux. Au niveau opérationnel, l'algèbre booléenne repose sur plusieurs fonctions essentielles : AND (∧) - conjonction logique, où le résultat est 1 seulement si les deux valeurs sont 1 ; OR (∨) - disjonction logique, où le résultat est 1 si au moins l'une des valeurs est 1 ; NOT (¬) - négation, qui inverse la valeur (0 devient 1 et 1 devient 0). Grâce à ces opérations élémentaires, Boole a démontré qu'il est possible de construire tout type de proposition logique complexe, qui a transformé la logique en un domaine mathématique autonome. Ainsi, à partir d'un système théorique conçu au XIXème siècle pour formaliser la logique de proposition, l'algèbre booléenne est devenue la pierre angulaire de l'ère algorithmique et de la société numérique. Elle montre comment l'abstrait peut être traduit en concret et comment la raison humaine peut être traduite en une architecture binaire, capable de supporter la complexité technologique du monde contemporain.

[156] G. Boole, *An Investigation of the Laws of Thought on which are founded the Mathematical Theories of Logic and Probabilities*, London, Walton and Maberly, 1854. Dans ce travail se trouve la source de la pensée algorithmique actuelle.

[157] B. Rotman, *Signifying Nothing: The Semiotics of Zero*, London, Macmillan, 1987.

un écran, insérer une carte, consulter Instagram, liker, tweeter, scanner, bref, tout ce que nous faisons dans cette nouvelle ère numérique peut être enregistré, stocké et surveillé »[158].

56. Des surnoms de la communauté à la combinaison de chiffres. Bien que le droit n'ait pas suffisamment de raisons pour comprendre les mécanismes purement mathématiques du fait que la société numérique est un univers construit entre zéro et un, que la « distance » entre un et deux n'est pas la même que la « distance » entre zéro et un, il devra trouver les meilleures méthodes pour normaliser ce monde entièrement nouveau. Un monde dans lequel l'identité numérique semble être totalement différente de l'identité classique évaluée par le nom de famille[159], le prénom, le nom des parents, la profession, le lieu de naissance, la religion ou même l'origine ethnique. La question classique « que faites-vous lorsque deux personnes d'un même village ont le même nom ? »[160] n'a plus aucun sens dans un contexte où tout se résume à une combinaison de chiffres. Lorsque la question ci-dessus se posait dans une communauté, la situation était résolue assez simplement en attribuant des surnoms[161]. En revanche, les chiffres ne peuvent pas recevoir de surnoms.

57. Importance du concept. Au lieu d'une conclusion à la discussion sur les algorithmes, nous exposons l'opinion du professeur Ifrah : « Si vous vouliez schématiser l'histoire des systèmes de numération, vous pourriez dire qu'elle comble l'espace entre le Un et le Zéro, les deux concepts qui sont devenus les symboles de la société technologique moderne. (...) Toute l'histoire de l'humanité s'étend entre le moment où l'on a réalisé que le vide était ”rien” et le moment où le sens de ”l'unité” est apparu pour la première fois »[162]. De manière apparemment surprenante, l'importance des calculs binaires a également été remarquée par Descartes (1641) : « l'idée du nombre infini diffère du nombre binaire »[163].

Section 4
IDENTIFICATION DES THÈMES D'INTÉRÊT POUR LA RECHERCHE

[158] B.-E. Harcourt, *La Société d'exposition : Désir et désobéissance à l'ère numérique*, Le Seuil, 2020, p.7.
[159] Le nom de famille a commencé à apparaître au XVe siècle avec le développement des villes et l'augmentation de la mobilité, et a commencé à être définitivement établi dans les documents au XVIIe siècle. Dans un premier temps, il a été inscrit dans les registres personnels établis par l'Église, puis dans les actes d'état civil, voir J. Desabie et M. Hayoun, « Le répertoire d'identification des personnes physiques », in *Pour une histoire de la statistique*, Tome II : *Matériaux*, Paris, INSEE / Éditions Joëlle Affichard, 1987.
[160] P. Delsalle, *Histoires de familles. Les registres paroissiaux et d'état civil, du Moyen Âge à nos jours* (1–). Presses universitaires de Franche-Comté, 2009, Chapitre 6. *Prénoms, noms, surnoms*, p.125-144.
[161] *Idem*, p.125 – 144.
[162] G. Ifrah, *op. cit.*, p.18.
[163] Descartes, « R*éponses aux secondes objections* », cité dans le Littré ; Le Littré, Dictionnaire de la langue française, Émile Littré, publié entre 1863-1873.

58. La rhétorique de l'anonymat. En 1998, le professeur Saint-Pau affirmait que l'anonymat est un droit de la personnalité et que « l'anonyme a quelque chose à cacher »[164]. Seulement, aujourd'hui, il est presque impossible de cacher ses données privées. Toute interaction avec la technologie créée par l'espace entre « zéro » et « un » laisse des traces qui ne peuvent être effacées définitivement[165]. Si le nom d'un nouveau-né est choisi par ses parents et inscrit sur son certificat de naissance, le code d'identification numérique est attribué automatiquement par l'État, sans possibilité de choix, et enregistré automatiquement dans une base de données classée par sexe, lieu de naissance, date de naissance, etc.

§1. OBSTACLES À L'OBTENTION ET AU MAINTIEN DE L'ANONYMAT

59. Définition de la réidentification. Une étude réalisée aux États-Unis en 1990 montre que la simple participation à un recensement peut aider à identifier avec précision une personne sans connaître ses données essentielles, telles que son nom, son adresse ou son numéro de téléphone[166]. Cette étude a démontré que 87 % des citoyens américains peuvent être identifiés par la simple combinaison du code postal, du sexe et de la date de naissance[167].

Cela a été le point de départ pour définir un nouveau concept étroitement lié à la vie privée, appelé réidentification. Des travaux récents évoquent même une science de la réidentification[168], qui décrit l'ensemble des techniques permettant de relier des données apparemment anonymes à une personne réelle. Une autre étude a montré que plus de 80 % des personnes ayant loué trois films sur Netflix ont été identifiées sur la base de l'analyse de deux critères : le moment de l'évaluation du film et le mode d'évaluation[169].

---

[164] J.-Ch. Saint-Pau, *L'anonymat et le droit*, thèse de doctorat en droit, Université de Bordeaux, soutenue publiquement le 14 janvier 1998.

[165] F. Hutmacher, M. Appel & S. Schwan, "*Understanding Autobiographical Memory in the Digital Age: The AMEDIA-Model"*, in Psychological Inquiry, vol. 35 (no 2), 2024, p. 83-105, publié en ligne le 17 septembre 2024, consulté le 9 septembre 2025 - https://www.tandfonline.com/doi/full/10.1080/1047840X.2024.2384125?

[166] L. Sweeney, "*Simple Demographics Often Identify People Uniquely*", in Data Privacy Working Paper 3, Carnegie Mellon University, Pittsburgh, 2000, consulté le 2 septembre 2025: https://dataprivacylab.org/projects/identifiability/paper1.pdf

[167] L. Sweeney, *op. cit.*- "Data holders often collect person-specific data and then release derivatives of collected data on a public or semi-public basis after removing all explicit identifiers, such as name, address and phone number. Evidence is provided in this document that this practice of de-identifying data and of ad hoc generalization are not sufficient to render data anonymous because combinations of attributes often combine uniquely to re-identify individuals".

[168] P. Ohm, "*Broken Promises of Privacy : Responding to the Surprising Failure of Anonymization*", in UCLA Law Review, vol. 57, 2010. p. 1701-1777; D. J. Sylvester & S. Lohr, "*The Security of Our Secrets: A History of Privacy and Confidentiality*", in Law and Statistical Practice, Denver University Law Review, vol. 83, 2005. p.147.

[169] A. Narayanan & V. Shmatikov, "*Robust De-Anonymization of Large Sparse Datasets*", in Proceedings of the 2008 IEEE Symposium on Security and Privacy (S&P 2008), Oakland, CA, États-Unis, 2008. p.111-125.

60. Collecte automatique des données. En ce qui concerne l'utilisation directe d'un système informatique, qu'il s'agisse d'un smartphone, d'un ordinateur ou d'une télévision connectée, les choses sont beaucoup plus claires : une simple connexion nous permet de définir notre groupe d'amis[170], nous suggère les profils d'anciens camarades de classe dont nous avions perdu la trace[171], identifie nos centres d'intérêt[172], voire notre pâtisserie préférée.

Bien que la discussion sur l'« amitié » sur les réseaux sociaux puisse avoir un caractère plus sociologique, elle peut également être envisagée d'un point de vue juridique lorsque nous parlons, par exemple, d'usurpation d'identité virtuelle[173] ou simplement de faux comptes et des infractions commises à l'aide de ceux-ci. Les utilisateurs deviennent amis avec de fausses identités, et ces fausses identités peuvent devenir amies avec d'autres identités tout aussi fausses. La citation d'Aristote sur le nombre impressionnant d'amis sur les réseaux sociaux semble très pertinente : « Ce n'est pas un ami celui qui est l'ami de tous »[174].

61. Études : nous ne pourrons pas devenir anonymes. Toutes ces données peuvent être facilement obtenues grâce à la géolocalisation de l'appareil, et la CNIL a émis plusieurs avertissements aux entreprises qui gèrent les réseaux sociaux concernant l'utilisation automatique des navigateurs GPS sans le consentement des utilisateurs, ce qui a pour effet direct de porter atteinte à la vie privée des utilisateurs[175]. Une autre étude publiée en 2019[176] montre que la réidentification est un problème qui dépasse le pouvoir des réglementations de

---

[170] J. Nocetti, «*Tous influencés par les réseaux sociaux?»,* in La Documentation française, 2025. https://shs.cairn.info/tous-influences-par-les-reseaux-sociaux--9782111578340?lang=fr

[171] Par exemple, Facebook a été critiqué pour le fait que dans la section « *Vous connaissez peut-être* » il identifie l'entourage réel d'une personne même si l'application est installée récemment et que le téléphone utilisé est neuf et vient d'être ouvert. La réponse de l'entreprise est que lors de la création du compte, l'application aurait pu intégrer les données de contact du répertoire téléphonique ou que d'autres ont autorisé l'application à accéder à votre numéro de téléphone, à la ville où vous habitez, au lieu de travail, etc. D'autre part, les enquêtes journalistiques montrent que Facebook propose des suggestions d'amis peu de temps après une rencontre réelle entre deux personnes qui ne se connaissaient pas auparavant et qui n'ont fait aucun échange de numéros de téléphone et ont gardé leur téléphone en poche tout le temps.

[172] K. Cadec, S. Proulx, « *Les représentations de l'amitié sur Facebook* », in Communication [En ligne], vol. 33, n° 2, 2015. - https://journals.openedition.org/communication/5755

[173] Haute Cour de cassation et de justice, Chambre chargée de trancher certaines questions de droit en matière pénale, déc., n° 4, 25 janvier 2021 : « *Le fait d'ouvrir et d'utiliser un compte sur un réseau social ouvert au public, en utilisant comme nom d'utilisateur le nom d'une autre personne et en saisissant des données personnelles réelles permettant de l'identifier, répond à deux des exigences essentielles de l'infraction de faux informatique prévue à l'article 325 du Code pénal, à savoir que l'introduction des données informatiques soit effectuée sans droit et que l'introduction des données informatiques ait pour résultat des données non conformes à la vérité* ».

[174] J.-M. Bruguière, « *La protection de l'entreprise sur les réseaux sociaux* », in JurisClasseur Communication, Fasc. 620, 2022.

[175] R. Perray, « *Données à caractère personnel. – Bases juridiques applicables aux traitements de données à caractère personnel. Dispositions spécifiques imposant le recueil du consentement* », in Répertoire de droit civil, Dalloz, Fasc. 932-72, 1re publ. 30 juin 2025.

[176] L. Rocher, J. M. Hendrickx, Y.-A. de Montjoye, "*Estimating the success of re-identifications in incomplete datasets using generative models*", in Nature Communications, vol. 10, 2019. article n° 3069, consulté le 2 septembre 2025 via Nature Communications - https://www.nature.com/articles/s41467-019-10933-3. L'étude montre qu'en utilisant 15 attributs démographiques, le risque de réidentification des personnes est de 99,98 %.

type RGPD de protéger les données et la vie privée et qu'une intervention législative spécialement adaptée à ce phénomène est nécessaire[177].

Concrètement, les études nous montrent que jamais, dans aucun contexte[178], nous ne pourrons devenir anonymes, même si nous effaçons toutes les traces de notre interaction avec la technologie.

§2. LE DROIT À L'OUBLI: ENTRE MÉMOIRE COLLECTIVE ET PROTECTION INDIVIDUELLE

62. Le droit à l'oubli, une « hydre juridique » ?[179] Le droit à l'oubli, dont les « ondes de choc »[180] se font encore sentir depuis la célèbre décision de la Cour européenne de justice[181] de 2014, semble être davantage une fiction juridique, car en réalité, il n'existe pas suffisamment de mécanismes techniques pour effacer complètement les traces laissées dans l'espace numérique. Comme l'oubli complet est difficile à obtenir à l'ère numérique, ce droit pourrait être rebaptisé « amnésie partielle ». À tout moment, l'oubli, tout comme l'anonymisation, peut être combattu par le processus de réidentification que nous avons décrit précédemment. Ainsi, même s'il est devenu une liberté fondamentale[182] utile pour la société numérique, l'utilisation de la métaphore « hydre juridique » par le professeur Hassler semble d'actualité. Le droit à l'oubli, composante plus restreinte du droit à la vie privée[183], apparaît sous une forme rudimentaire dès la loi Informatique de 1978, en ce sens que les données ne peuvent être conservées que pour la finalité pour laquelle elles ont été collectées. Dans le même temps, une loi du 12 avril 2000 instaure la possibilité d'archiver définitivement les données d'une personne

[177] G. D'Acquisto, J. Domingo-Ferrer, P. Kikiras, V. Torra, Y.-A. de Montjoye, A. Bourka, *Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics*, rapport technique, European Union Agency for Network and Information Security (ENISA), décembre 2015.
[178] P. Ohm, *op. cit.* "First, the power of reidentification will create and amplify privacy harms. Reidentification combines datasets that were meant to be kept apart, and in doing so, gains power through accretion: Every successful reidentification,even one that reveals seemingly nonsensitive data like movie ratings, abets future reidentification. Accretive reidentification makes all of our secrets fundamentally easier to discover and reveal".
[179] T. Hassler, « *Droits de la personnalité : rediffusion et droit à l'oubli* », in Dalloz, 2007. p.2829.
[180] L. François, « *Le droit à l'oubli numérique > à l'épreuve de la liberté d'information — CEDH 28 juin 2018, nº 60798/10 et 65599/10, M.L. et W.W. c/ Allemagne* », *AJ Pénal*, 2018. p.462.
[181] CJUE, Grande Chambre, 13 mai 2014, affaire C-131/12, *Google Spain SL et Google Inc. c/ Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*.
[182] C. Costaz, « *Le droit à l'oubli* », in Gazette du Palais, 2, Doctr., 1995. p.965.
[183] M. Ranquet, « *Le droit à l'oubli* : *vers un nouveau droit fondamental de l'individu ?* », in Communications, nº 104, 2019. p.149-159.

à des fins de recherche et d'histoire[184]. Ainsi, au-delà de l'incapacité technique à garantir ce droit, celui-ci n'est de toute façon pas absolu[185].

63. Entre le droit à l'oubli et le droit à la liberté d'expression. Une situation susceptible de donner lieu à de sérieuses tensions juridiques se présente en ce qui concerne la publication dans le milieu numérique d'articles de presse qui pourraient avoir un lien avec la vie privée d'une personne. Les demandes de suppression ou de désindexation des informations – manifestations du droit à l'oubli – doivent être mises en balance avec la liberté d'expression et le droit à l'information, et l'évaluation de la proportionnalité revient aux tribunaux. Jusqu'à présent, la pratique a montré que le droit à la liberté d'expression des journalistes est prioritaire[186]. Le défi pour le droit à l'oubli est de limiter l'accumulation infinie de données collectées et d'équilibrer les deux types d'identités : celle construite par l'individu et celle fixée par les archives des systèmes informatiques[187].

A. Mémoire hybride: humaine, numérique, algorithmique

64. Synergie entre la psychologie cognitive et l'intelligence artificielle. La théorie exprimée par Neisser, père de la psychologie cognitive, était que la mémoire est en grande partie reconstruite et ne représente pas une photographie fidèle et instantanée d'un moment donné[188].

Dans le développement de la science cognitive – « l'une des réalisations intellectuelles les plus remarquables et fascinantes de l'ère moderne »[189] – l'intelligence artificielle et la psychologie cognitive se sont développées ensemble et ont contribué de manière décisive à la constitution d'un cadre interdisciplinaire, dans lequel les modèles computationnels de l'IA ont fourni des outils de simulation des processus mentaux, tandis que la psychologie cognitive a fourni des hypothèses empiriques et des concepts sur le fonctionnement de l'esprit, générant ainsi une synergie qui a redéfini la compréhension des mécanismes de la connaissance et de la représentation de l'information.

---

[184] Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, chapitre II : *« Dispositions relatives à la transparence administrative* ».
[185] M. Ranquet, *op. cit.* : « *Le droit individuel à l'oubli n'est donc pas absolu mais subordonné à l'intérêt général justifiant une conservation historique, dans le cas des archives publiques* ».
[186] H. Surrel, « *Droit à l'effacement et liberté de la presse* », in *JCP*, 2018, n° 869.
[187] Boutin, C., « *Le droit à l'oubli numérique : entre mémoire et identité* », in Revue Lamy Droit de l'immatériel, 2016, n° 129, p.67-72.
[188] U. Neisser, *Cognitive Psychology*, Englewood Cliffs (NJ), Prentice Hall, 1967.
[189] M. A. Boden, *Mind as Machine: A History of Cognitive Science*, 2 vol., Oxford, Oxford University Press, 2006.

65. Mémoire sémantique et épisodique. En intégrant les éléments de la psychologie cognitive dans son analyse, Endel Tulving[190] a établi pour la première fois[191] la différence entre la mémoire sémantique[192] et la mémoire épisodique[193]. La société numérique a brutalement influencé la manière dont nous nous rapportons aujourd'hui aux théories mentionnées ci-dessus. Cette mutation soulève des questions essentielles pour le droit à la vie privée.

66. « Effet Google »[194]. Nous assistons à des changements profonds dans les comportements et les attitudes qui définissent la vie privée, à travers ce que la littérature appelle une véritable « externalisation cognitive »[195] - l'externalisation de la mémoire vers des appareils et Internet, un phénomène connu sous le nom d'« effet Google ». Le besoin de mémoire active est constamment compromis par la technologie. L'accès instantané aux informations par des moyens numériques réduit l'appel à la mémoire sémantique, car il réduit le besoin de stockage interne et d'acquisition de connaissances générales.

Si nous analysons ce comportement par référence à la théorie de « l'état d'esprit étendu »[196], concept qui suggère que les processus cognitifs ne sont pas limités aux « frontières de la peau et du crâne », nous pouvons comprendre qu'il n'y a pas de connotation négative implicite dans cette externalisation de la mémoire.

67. Mémoire autobiographique numérique[197]. En revanche, la mémoire épisodique semble caractériser de plus en plus le présent : « à l'ère numérique, la relation entre la mémoire humaine et les médias est intime et impossible à séparer »[198].

---

[190] E. Tulving, *Elements of Episodic Memory*, Oxford, Oxford University Press, 1983.

[191] E. Tulving, « *Episodic and Semantic Memory* », in E. Tulving & W. Donaldson (dir.), *Organization of Memory*, New York, Academic Press, 1972, p.381-402.

[192] Selon la vision de Tulving, la mémoire sémantique constitue l'ensemble des connaissances générales sur le monde, indépendamment de l'expérience personnelle. Elle organise les concepts, les faits et les règles linguistiques, étant accessible sans référence à un contexte temporel ou spatial particulier. En ce sens, la mémoire sémantique est « atemporelle », fournissant le cadre de compréhension nécessaire au raisonnement et à la communication, mais n'étant pas liée à un épisode vécu par l'individu.

[193] Saisissant des différences essentielles par rapport à la mémoire sémantique, la mémoire épisodique désigne la capacité d'évoquer des événements personnels situés dans un temps et un lieu spécifiques. Tulving la définit comme la forme de mémoire qui permet à l'individu de « voyager mentalement dans le temps », en réexpérimentant subjectivement des expériences passées. Celle-ci ne se limite pas au stockage de l'information, mais suppose la conscience autonoétique, c'est-à-dire la reconnaissance de soi comme acteur de l'événement remémoré. La mémoire épisodique confère ainsi une continuité à l'identité et différencie profondément l'expérience humaine de la simple accumulation de données.

[194] B. Sparrow, J. Liu, D. M. Wegner, "*Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips*", in Science, vol. 333, n° 6043, 2011.

[195] M. Gerken, "*Outsourced Cognition*", in Philosophical Issues, Wiley-VCH, vol. 24, n° 1, 2014. p.127–158.

[196] A. Clark, D. J. Chalmers, "*The Extended Mind*", in Analysis, Oxford University Press, vol. 58, n° 1, janvier 1998. p.7-19.

[197] F. Hutmacher, M. Appel, S. Schwan, "*Understanding Autobiographical Memory in the Digital Age: The AMEDIA-Model*", in Psychological Inquiry, vol. 35, no 2, 2024. p. 83-105, publié en ligne le 17 septembre 2024, consulté le 9 septembre 2025 - https://www.tandfonline.com/doi/full/10.1080/1047840X.2024.2384125?

[198] Y. Han, "*Evolution of mediated memory in the digital age: tracing its path from the 1950s to 2010s*", in Humanities and Social Sciences Communications, vol. 10, article n° 603, publié en ligne le 23 septembre 2023.

Le voyage que l'homme moderne peut faire dans le temps et reconstruire sa propre histoire est facilité par précisément cette mémoire épisodique. À l'ère numérique, cette mémoire est complétée et transformée par les « traces » électroniques qui font partie intégrante de notre biographie - « vivre à l'ère numérique signifie créer et partager d'énormes quantités de données »[199]. Qu'ils postent des photos de repas quotidiens ou des images de vacances sur Instagram, laissent le GPS enregistrer ses itinéraires quotidiens, font de courtes vidéos pour TikTok, participent à des manifestations et distribuent des slogans, capturent par des photos leurs peintures préférées ou des phénomènes astronomiques, ou enregistrent et partagent des fragments de matchs de football, l'individu produit toujours des traces numériques.

68. Mémoire collective vs mémoire collective numérique. Prises ensemble, ces pratiques constituent un véritable journal de vie en ligne : une autobiographie numérique écrite au quotidien, dans laquelle les expériences personnelles sont transformées en données, archivées et mises à la disposition des algorithmes et du regard public, devenant ainsi une mémoire numérique collective[200]. Le concept de mémoire collective est apparu pour la première fois en 1925 chez Maurice Halbwachs[201], un disciple d'Émile Durkheim. « Comment retrouver l`emplacement d`un village sur une carte de géographie où ne sont indiquées que les très grandes villes ? »[202] est une question par laquelle l'auteur tente de justifier la difficulté de localiser un souvenir.

B. Mémoire algorithmique et réécriture du passé

69. Localisation et reconnaissance. « Localiser, c`est avoir l`idée du moment où l`on a acquis un souvenir »[203] c`est ainsi que Halbwachs commence son argumentation pour souligner qu'il y a des différences essentielles entre ce que les psychologues appellent la reconnaissance et la localisation des souvenirs. Ainsi, « reconnaître, c'est avoir le sentiment qu'une personne qu'on voit ou qu'une image qui traverse l'esprit se sont présentées à nous auparavant, sans que nous puissions dire à quel moment »[204].

70. La raison est utilisée pour la localisation. Alors que la reconnaissance des souvenirs se fait automatiquement sans aucune réflexion, « la localisation met en jeu l`activité

[199] F. Hutmacher, M. Appel & S. Schwan, *op. cit.*
[200] V. Beaudouin, « *Comment s'élabore la mémoire collective sur le web ? Une analyse qualitative et quantitative des pratiques d'écriture en ligne de la mémoire de la Grande Guerre*. », in Réseaux, 214-215(2), 2019. p.141-169.
[201] M. Halbwachs, *Les cadres sociaux de la mémoire*, Paris, Félix Alcan, 1925.
[202] M. Halbwachs, *Les cadres sociaux de la mémoire,* p.110.
[203] *Idem* p.99.
[204] *Idem* p.99.

intellectuelle de l`esprit, puisque, pour retrouver la place d'un souvenir dans le temps, il faut un effort de réflexion »[205]. En analysant la situation factuelle actuelle, il semble que les algorithmes nous privent précisément de cette caractéristique essentielle de la localisation des souvenirs, à savoir l'utilisation de la raison et des capacités intellectuelles.

71. « Lifelogs » (journaux de vie) et reconstruction du passé numérique. D'autre part, il n`y a aucune raison de ne considérer que les aspects apparemment négatifs de la disparition de la mémoire épisodique classique, telle que nous la connaissons depuis Tulving. L'ère numérique fournit des outils capables de soutenir la mémoire épisodique chez les patients présentant des déficits cognitifs, en externalisant précisément et en reconstruisant des souvenirs autobiographiques. Les recherches[206] montrent que les photos numériques, les vidéos et les journaux électroniques fonctionnent comme des facteurs externes capables de réactiver des événements autrement inaccessibles à la mémoire interne. La création de « lifelogs »[207] a démontré des avantages significatifs pour rappeler les événements quotidiens chez les patients atteints d'Alzheimer et de formes d'amnésie. D'autres études récentes ont confirmé également que les supports numériques facilitent à la fois la réactivation du passé et la stimulation de la projection de scénarios futurs, renforçant le sentiment d'identité personnelle[208].

72. Le flux des expériences vécues devient une valeur sociale, d'intérêt juridique. La systématisation des concepts de « localisation » et de « reconnaissance » des souvenirs, créée et fondée par Halbwachs[209], nous permet aujourd'hui de mieux comprendre comment fonctionne la mémoire autobiographique. La capacité de situer un souvenir dans un temps et un espace précis et de le reconnaître dans le flux des expériences vécues est le fondement de l'identité individuelle d'aujourd'hui, ce qui met le droit dans un état constant de vigilance. Lorsque ces processus sont répliqués ou manipulés à travers des algorithmes, par exemple - à travers les fonctions de « réminiscences » des réseaux sociaux, à travers des suggestions de

---

[205] La conclusion de M. Halbwachs est que: « *la reconnaissance au contraire s'opérerait automatiquement : le sentiment de familiarité, qui accompagne par exemple le souvenir des mots d'une langue qu'on connaît, et le sentiment du déjà vu, qui naît à l'occasion d'une image, objet ou figure, ne sont pas des idées et ne supposent aucune réflexion. D'où il résulte qu'il entrerait bien une part de raisonnement dans la mémoire, mais dans la mesure seulement où nous localisons nos souvenirs* ».

[206] E. Berry, P. Kapur, N. Williams *et al.*, « *The use of a wearable camera, SenseCam, as a pictorial diary to improve autobiographical memory in a patient with limbic encephalitis* », in Memory, vol. 15, n° 5, 2007.

[207] Lifelog désigne l'archivage numérique continu des expériences quotidiennes en enregistrant automatiquement les photos, les sons, les lieux ou les activités des utilisateurs. Le chercheur canadien Steve Mann est considéré comme le père de ce phénomène, car depuis 1994 il a commencé à enregistrer et à transmettre sa vie sans cesse grâce à des caméras portables. Aujourd'hui, il y a une très grande communauté de personnes qui font du lifelogging. Dans la littérature, le lifelogging était présenté comme une forme de « externalisation de la mémoire », capable de créer une base de données personnelle qui peut être réactivée pour soutenir la mémoire épisodique (voir J. Gemmell, G. Bell & R. Lueder, « *MyLifeBits : a personal database for everything* », in Communications of the ACM, vol. 49, n° 1, janvier 2006).

[208] P. Piolino, B. Desgranges, F. Eustache, *La mémoire autobiographique : théorie et pratique*, Paris, Solal, 2000.

[209] M. Halbwachs, *La mémoire collective*, Paris, Presses Universitaires de France, 1950.

photos automatisées ou à travers la récupération numérique des itinéraires quotidiens - ils ne servent plus seulement l'individu, mais acquièrent une valeur sociale et politique.

73. Crise de la mémoire collective et remodelage comportemental. Si, de l'avis d'Halbwachs, la mémoire collective n'est jamais « la somme des souvenirs individuels »[210] cela ne semble plus être d'actualité étant donné que les plateformes numériques et les algorithmes créent une nouvelle forme de « mémoire collective algorithmique » où ce qui est « retenu » ou « oublié dépend » de la logique des moteurs de recherche, des tendances et des archives numériques. Certains auteurs français considèrent que nous traversons une crise de la mémoire collective précisément à cause de « l'inflation mémorielle à l`heure du numérique »[211]. Dans ce contexte, l'ordre public peut être affecté, car les algorithmes deviennent des acteurs qui influencent la sélection, l'interprétation et la circulation de la mémoire collective, remodelant les comportements et même les consensus sociaux.

74. Externalisation des souvenirs[212]**.** Il y a déjà pas mal d'études récentes montrant que les photos numériques améliorent la mémoire autobiographique et en même temps entraînent une augmentation de l'oubli – « les souvenirs deviennent numériques et influencent la mémoire en raison de la motivation croissante à prendre et partager des photos sur les réseaux sociaux »[213]. De toute façon, les photographies ne sont plus un simple acte de protection des images familiales, mais sont devenues un instrument d'exposition identitaire[214].

75. Identité virtuelle, une version idéalisée de soi-même. Bien qu'il soit difficile de définir le terme classique identité « omniprésente tant dans les sciences humaines que dans le débat social, l'identité n'est pourtant jamais clairement définie »[215], l'identité dans l'environnement virtuel est d'autant plus difficile à saisir dans les modèles classiques de conceptualisation. En général, l'identité photographique sur les réseaux sociaux est différente de l`identité réelle[216], les utilisateurs construisent des versions sélectionnées et souvent idéalisées d'eux-mêmes, il y a un phénomène d'hyperbolisation du niveau de vie, de l'état

[210] J. van Dijck, *Mediated Memories in the Digital Age*, Stanford, Stanford University Press, 2007, p.9.
[211] E. Hoog, *Mémoire année zéro*, Paris, Le Seuil, coll. « Essais », 2009, p.122.
[212] E.D. Eliseev, E.J. Marsh, « *Externalizing autobiographical memories in the digital age* », in Trends in Cognitive Sciences, vol. 25, n° 12, 2021, p.1072-1081.
[213] A. E. Keskin, « *Digitalization of Memories – An Analysis Relationship Between Autobiographical Memory and Digital Photography* », in Media Literacy and Academic Research, vol. 3, n° 1er, 2020, p.85-96.
[214] J. van Dijck, « *Digital Photography: Communication, Identity, Memory* », in Visual Communication, vol. 7, n° 1, 2008.
[215] J.-C. Kaufmann, *L'invention de soi. Une théorie de l'identité*, Paris, Armand Colin, 2004.
[216] D. Cardon, « *Réseaux sociaux de l'Internet* », in Communications, 88, 2011, *Cultures du numérique*, sous la direction de Antonio A. Casilli. p.141-148.

professionnel ou social[217]. Apparemment, c'est une attitude naturelle parce que dans l'ancien album photo de famille, personne ne protège ses photos des événements douloureux.

76. Vie privée devenue un spectacle. L'externalisation des souvenirs autobiographiques provient à la fois du désir intérieur de l'individu d'exposer volontairement ses données privées et du fait que nous assistons aujourd'hui à la construction de la société d'exposition[218], qui transforme la vie privée en spectacle[219] et dans laquelle la réalité vécue est remplacée par des représentations[220]. Cette identité virtuelle acquiert des valences juridiques importantes, notamment dans le contexte de la commission de délits en ligne, tels que la tricherie, le harcèlement ou encore l`atteinte à la vie privée.

77. La transparence. Un autre terme qui accompagne naturellement tout discours sur la vie privée à l'ère des algorithmes est la transparence. Tout ce que nous avons exposé peut être traduit non seulement par la naissance d'une société d'exposition et d'une société transparente. La transparence est devenue une valeur clé du discours démocratique contemporain, mais elle semble être une arme à double tranchant : d'une part, il est utile que « n`importe qui puisse obtenir des informations sur n'importe quoi » et d'autre part, « la transparence a un côté sombre » parce que derrière elle « se trouve la disparition de la confidentialité, l'homogénéisation et l'effondrement de la confiance »[221].

78. Mémoire médiée[222]. L'étude[223] qui a analysé les caractéristiques de la « mémoire médiée » sur une période assez longue, 1950 – 2010, a révélé une double représentation de la mémoire selon la méthode de recherche. Plus précisément, les sciences neurologiques et cognitives, utilisant des techniques de neuro-imagerie, ont montré que la mémoire est représentée par la technologie. D'autre part, les analyses menées par les méthodes des sciences

---

[217] D. C. DeAndrea, S. T. Tong, Y. J. Liang, « *When do people misrepresent themselves to others? The effects of social desirability, ground truth, and accountability on deceptive self-presentations* », in Journal of Communication, vol. 62, n° 3, 2012, p.400-417.

[218] Il y a une littérature assez vaste qui a écrit sur ce sujet, dans le domaine juridique mais aussi philosophique ou sociologique. Voir E., Harcourt, *La Société d'exposition : Désir et désobéissance à l'ère numérique*, Le Seuil, 2020 ; B.-Ch. Han, *The Transparency Society*, Redwood City (Calif.), Stanford University Press, collection *Stanford Briefs*, août 2015 ; J.-C. Kaufmann, *L'invention de soi. Une théorie de l'identité*, Paris, Armand Colin, 2004 ; G. Debord, *La société du spectacle*, Paris, Buchet-Chastel, 1967 ; B. E. Harcourt, *Exposed: Desire and Disobedience in the Digital Age*, Cambridge (Mass.), Harvard University Press, 2015.

[219] B.-Ch. Han, *The Transparency Society*, Redwood City (Calif.), Stanford University Press, collection *Stanford Briefs*, août 2015.

[220] « *Tout ce qui était autrefois vécu directement est devenu une simple représentation. Les images, détachées de chaque aspect de la vie, se fondent dans un flux commun, et l'ancienne unité de la vie est perdue à jamais. Perçu de manière fragmentaire, le réel se déploie dans une nouvelle généralité, comme un pseudo-monde à part, n'existant que comme objet de contemplation* », reprise de G. Debord, *La société du spectacle*, Paris, Bouquet-Chastel, 1967. Bien que l'auteur n'ait pas été témoin de la société numérique actuelle, il a exprimé des opinions assez radicales pour les années 1960 à propos d'une époque où l'exposition ne faisait que commencer.

[221] B.-Ch. Han, *The Transparency Society*, *op. cit.*, « Introduction ».

[222] La mémoire médiatisée fait référence au processus par lequel les souvenirs autobiographiques ne sont plus conservés exclusivement dans l'esprit de l'individu, mais sont produits, stockés et partagés grâce aux technologies médiatiques.

[223] B.-Ch. Han, *op. cit.*

sociales « mettent en évidence la représentation culturelle de la mémoire à travers les médias numériques, tels que la télévision, les ordinateurs, les smartphones, Internet et les réseaux sociaux »[224]. Il est certain qu'un tel processus dans lequel les algorithmes « médiatisent » ou plutôt « interviennent » dans la relation entre la mémoire et le passé ne peut être qu`un signe d`inquiétude pour la notion classique de la vie privée.

§3. LA TRANSFORMATION CONCEPTUELLE DU PUBLIC ET DU PRIVÉ

79. Redéfinition des concepts de public et privé. Cette mémoire médiatisée ne fait que changer le paradigme des notions d'espace public et privé. De la *République* de Platon aux réflexions de Jean Carbonnier, les deux dimensions ont été conçues dans une évolution relativement linéaire et bien définie, mais aujourd'hui elles sont devenues instables et beaucoup trop dynamiques. L'autobiographie numérique - composée de traces laissées sur les réseaux sociaux, les applications mobiles et les appareils connectés - reconfigure constamment les frontières entre la vie privée et l'exposition.

Dans ce contexte, il semble que la motivation de la CEDH dans l'affaire Hachette Filipacchi Associes (Ici Paris) c. France soit d`intérêt[225] : sanctionner une revue pour avoir porté atteinte à la vie privée d'un chanteur célèbre viole l'article 10 de la CEDH. La Cour a montré que « dans la mesure où le magazine a repris des informations librement divulguées et rendues publiques par l'intéressé lui-même, notamment dans son « autobiographie », sur ses biens et sur la façon dont il employait son argent, la Cour est d'avis que celui-ci ne conservait plus une espérance légitime de voir sa vie privée effectivement protégée ». Cet arrêt montre que lorsqu'une personne expose ses propres informations intimes dans l'espace public, le niveau de protection conféré par l'article 8 CEDH diminue en conséquence.

80. Le privé devient public et le public devient privé. Ce qui était auparavant privé devient public, et ce qui relevait de la vie publique se referme paradoxalement dans un registre privé de données et d'archives. Bien que les réseaux sociaux semblent s'inscrire dans le concept

[224] B-Ch. Han, *op. cit.*
[225] CEDH, 23 juill. 2009, *Hachette Filipacchi Associés (Ici Paris) c. France*, req. n° 12268/03, HUDOC, disponible sur https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-1413%22]}

de « sphère publique »[226] comme décrit par Habermas[227] et devraient être positionnés quelque part entre l'État et les citoyens[228], en réalité, nous assistons à une privatisation de l'espace informationnel en ligne[229].

81. Exemples de partage de rôles. Les exemples de ce partage de rôles public et privé sont multiples : des conversations privées entre amis, transférées sur WhatsApp ou Messenger, peuvent être diffusées de manière virale, devenant un sujet public ; des données médicales, considérées parmi les plus intimes, sont intégrées dans des applications de fitness et analysées par des entreprises commerciales; les photos de vacances ou de la vie de famille, autrefois destinées à un album personnel, sont publiées sur Instagram et accessibles à un public potentiellement illimité.

D'autre part, les actions dans l'espace public deviennent rapidement une partie d'une autobiographie numérique : un simple enregistrement sur Facebook[230] lors d'un concert ou à un restaurant est stocké et ensuite utilisé pour le profilage des consommateurs ; la participation à un événement sportif est capturée par des caméras de surveillance et associée à la reconnaissance faciale, transformant une expérience collective en un enregistrement d'identité permanent ; les voyages en transport public sont suivis via des cartes d'accès et les données deviennent publiques grâce au profilage des passagers ; une simple connexion à un réseau Wi-Fi public génère des données privées utilisées plus tard pour le marketing personnalisé.

82. Les notions de public et privé sont-elles binaires[231]? Le paradigme *de l'homo numericus* est de vivre dans un monde binaire, dans la vision de la technologie, dans l'univers

---

[226] En 1962, sans anticiper le développement des plateformes, pour Jurgen Habermas, « *la sphère publique* » désigne un espace intermédiaire entre la société civile et l'État, où les citoyens débattent rationnellement et équitablement, formant une opinion publique capable d'influencer le pouvoir politique. Née dans l'Europe du XVIIe et du XVIIIe siècles à travers les cafés, les salons et la presse écrite, la sphère publique bourgeoise était définie par l'accès à l'information et au débat critique. Habermas montre cependant qu'avec l'expansion des médias et des intérêts économiques, cet idéal a été érodé, devenant un espace dominé par le consumérisme et la logique commerciale.

[227] J. Habermas, *L'espace public : archéologie de la publicité comme dimension constitutive de la société bourgeoise*, Paris, Payot, 1978.

[228] N. Fraser, trad. M. Valenta, « *Repenser la sphère publique : une contribution à la critique de la démocratie telle qu'elle existe réellement* », in C. Calhoun (dir.), *Habermas and the Public Sphere*, Cambridge, MIT Press, 1992, p.109-142 ; trad. franç., *Hermès, La Revue*, n° 31, 2001, p.125-156.

[229] F. G'Sell, « *Les réseaux sociaux ou la privatisation de l'espace informationnel en ligne* », Revue de droit international et de droit comparé appliqué (RDIA), n° 5, 2022, p.42-57 – « *Il y a, effectivement, de quoi être troublé de constater que la simple prise de contrôle d'un réseau social par un nouvel actionnaire peut avoir des conséquences considérables sur la façon dont les informations sont présentées aux internautes sur la plateforme. La faculté d'intervenir sur les contenus se trouve entre les mains de quelques entreprises privées à but lucratif généralement pilotées de manière verticale par des dirigeants médiatisés* ».

[230] J. Burkell, A. Fortier, L. Y. C. Wong & J. L. Simpson, « *Facebook : public space, or private space ?* », in Information, Communication & Society, vol. 17, n° 8, 2014, p.974-985.

[231] Quelques définitions de *Le Petit Robert* pour le terme binaire :
a. Arithm. Vx. Composé de deux unités. Nombre binaire.
b. Mod. Qui comporte, peut compter deux états définis et distincts (et deux seulement). Numération binaire : système de numération de base 2. La numération binaire utilise les chiffres 0 et 1 pour écrire tous les nombres.

créé entre « zéro » et « un ». Étymologiquement, le terme binaire est utilisé depuis 1554 et vient du latin *binarius*, qui se traduit par « double ». Nous trouvons ce terme dans la musique (1643) avec la signification de rythme ou mesure binaire[232], en astronomie (1975) - il a été constaté que 50 pour cent des étoiles de la galaxie sont binaires, gravitant les unes autour des autres - ou en chimie à travers le système binaire de composition des éléments. Bien que nous ne puissions nier cette existence binaire du public et du privé, en ce qui concerne la protection de la vie privée, les deux notions doivent être comprises contextuellement[233], selon chaque individu. C'est un endroit où la renaissance de la jurisprudence se sent à l'aise.

83. Adaptation de la vie privée au contexte social. Le système binaire du droit[234] ne peut pas être appliqué simplement par des mécanismes classiques : légal/illégal, interdit/autorisé, coupable/non coupable, licite/illicite mais il doit être adapté à un contexte social plus large, voire numérique, etc. Par exemple, au délit de vol, les éléments typiques et les valeurs sociales protégées sont à peu près les mêmes depuis 1800 bien que les discussions autour des années 1900 sur le vol d'électricité aient donné lieu à des débats juridiques mémorables[235]. Des discussions similaires ont actuellement lieu concernant le vol d'objets virtuels. Une décision rendue en 2012 par la Haute Cour néerlandaise a établi que les éléments constitutifs du délit de vol d'un objet dans un jeu vidéo sont réunis si cet objet n'est pas seulement un fichier numérique,

---

Inform. Qui ne comporte que deux états. Code, langage binaire. Langage codé binaire. Élément binaire. ➞ 2. Bit ; booléen ; 2. digital ; et aussi bascule. Système binaire : code binaire d'une machine n'utilisant que deux symboles (1 et 0) correspondant à deux états d'une cellule électrique. Logique binaire. ➞ Bivalent.
c. Log. Relation binaire : relation établie entre deux éléments. - Math. Relation binaire dans un ensemble, relation de cet ensemble vers lui-même.

[232] « *C'est pourquoy je dis que nous ne devrions user que d'une marque dans la Musique Binaire et d'un seul autre (sic) dans la Ternaire, puisque ce n'est pas là où gît le lièvre. Mais puisque le mal a passé par contagion et qu'il nous faut suivre comme par force les vestiges et les traces de nos devanciers, je vous diray qu'il y a douze signes en la musique, quatre en la Binaire, quatre en la Ternaire et quatregeneralles* », A. Gantez, « *l'Entretien des musiciens* », 1643, in *D. D. L.*, II, 15.

[233] A. Gruzd, Á. Hernández-García, *"Privacy Concerns and Self-Disclosure in Private and Public Uses of Social Media*", in Cyberpsychology, Behavior, and Social Networking, vol. 21, no. 7, 1er juillet 2018. p.418-428.

[234] N. Luhmann, *Das Recht der Gesellschaft*, Francfort-sur-le-Main, Suhrkamp, 1993, p.166 : « Même si, logiquement, le schéma binaire du bien et du mal a un rôle primordial, car il fonde l'identification du système juridique, il représente historiquement une réalisation tardive et présuppose l'existence préalable d'un corpus normatif ».

[235] Cass. Crim. 3 août 1912, DP 1913, 1, p.439; S. 1913, 1, p.337, note Roux. Cette décision est un exemple clair de lutte entre le droit traditionnel et l'évolution technologique. Art. 379 du Code pénal napoléonien de 1810 – « quiconque soustrait frauduleusement une chose qui ne lui appartient pas est coupable de vol » ne pourrait pas prendre en considération le vol d'électricité. Pendant ce temps, l'électricité était fournie à la population, mais la définition dans le Code pénal restait inchangée. La question était claire : l'électricité volée était-elle un bien corporel ou non ? Initialement, les tribunaux ont considéré qu'il pourrait s'agir d'une violation de la responsabilité contractuelle et non d'un vol. La décision de 1912 change d'orientation et considère l'électricité comme un bien corporel : « *L'électricité est livrée par celui qui la produit à l'abonné qui la reçoit pour l'utiliser ; elle passe, par l'effet d'une transmission qui peut être matériellement constatée, de la possession du premier dans la possession du second et doit dès lors être considérée comme une chose au sens de l'article 379 du CP pouvant faire l'objet d'une appréhension* ». C'est un exemple clair d'une situation où la jurisprudence, par son attribut d'interprétation de la loi à la réalité empirique au moment de l'application, a aidé le droit à gagner la bataille avec la technologie.

s'il est contrôlé par le joueur et s'il a une valeur économique[236]. Les arguments de cette décision sont aujourd'hui utilisés pour déterminer la nature juridique des objets dans le métaverse.

En revanche, dans le délit d`atteinte à la vie privée, ces éléments semblent s`inscrire dans une dynamique continue[237]. Ce qui apparaissait auparavant comme une intrusion non autorisée dans la vie privée peut aujourd'hui être un geste encouragé par la victime présumée. Si, il y a dix ans, les journalistes perdaient des jours pour photographier un fonctionnaire dans la rue et qu'il se sentait harcelé, aujourd'hui ce même fonctionnaire publie volontairement son autobiographie numérique sur les réseaux sociaux.

Section 5
LES LIMITES DES TRANSFORMATIONS CONTEMPORAINES DU DROIT PÉNAL À L'ÈRE NUMÉRIQUE

84. Action répressive du droit pénal. Les délits relatifs à l'accès aux systèmes informatiques ou qui protègent la vie privée dans le but de limiter l'intrusion non autorisée de l'Etat ou des particuliers aux données personnelles doivent être constamment reconfigurés[238]. Les théoriciens de la criminologie[239] renforcent l'idée que nous devons être vigilants pour préserver nos droits, nos libertés, mais surtout notre humanité, et en même temps soutenir l'action répressive du droit pénal : « il faut donc surveiller, être en éveil, mais cette seule action demeure insuffisante. Elle nécessite de lui associer un éclairage préventif et un volet répressif ».

§1. INTERROGATIONS DU PRÉSENT EN DROIT PÉNAL

85. Catégories du comportement criminel à l'ère numérique. Dans une synthèse destinée au grand public[240], le professeur de criminologie français Alain Bauer divise les comportements infractionnels directement liés aux nouvelles technologies en trois catégories : « les crimes et délits de droit commun facilités par l`usage des nouvelles technologies, les

[236] A. R. Lodder, « *Dutch Supreme Court 2012: Virtual Theft Ruling a One-Off or First in a Series*? », in Journal of Virtual Worlds Research, vol. 6, n° 3, septembre 2013. p.1-12.
[237] M.-L. Rassat, *Droit pénal spécial*, 9e éd., Dalloz, Paris, 2024. p.584.
[238] Par exemple, l'acte d'un modèle de langage à grande échelle (LLM) du type Chat-GBT ne peut pas faire l'objet d'une incrimination pénale en fournissant simplement des informations fausses et délirantes aux utilisateurs, sauf si cette conduite incite à la haine publique, incite au suicide, fournit des données concrètes sur comment voler une banque, il enregistre sans autorisation les utilisateurs de smartphones et publie leurs discussions, etc.
[239] F. Archer, « *La criminologie confrontée aux nouvelles technologies* », in Dalloz IP/IT, n° 11, 2024. p.555-559 (dans le dossier « *Pour une intelligence artificielle responsable* »).
[240] A. Bauer, *La criminologie pour les nuls*, First, 2022, p.205.

cyber-infractions directement en lien avec lzusage des nouvelles technologies et le détournement des moyens de communication et d`information à des fins criminelles et délictuelles ». Dans un commentaire[241] sur cette division des comportements antisociaux, il est montré qu'en utilisant des algorithmes, les profits des délinquants sont beaucoup plus élevés, les risques sont plus faibles et l'ordre public est entré dans l'ère 2.0.

86. Imitation et innovation, la base du comportement antisocial. Dans le même contexte, il convient de mentionner la théorie du sociologue Gabriel Tarde, qui, se distançant du criminel atavique[242] de Cesare Lombroso, a expliqué que la base du comportement criminel est l'imitation et l'innovation, comme s'il y avait une réaction chimique[243] entre les deux.

87. *Sollen* et *Sein* – adaptation aux défis de la technologie. À la base de ce processus d'adaptation du droit pénal aux nouvelles réalités technologiques, il semble que la théorie de Hans Kelsen[244], reprise[245] et parfois contestée[246] par la doctrine française, soit la plus cohérente et efficace : la norme juridique est le *Sollen*[247], c'est-à-dire le *devoir-être*, et *Sein* est *être* (l`acte de volonté). En pratique, la norme juridique pénale ne décrit pas des faits réels[248] mais détermine ce qui doit être fait ou la sanction qui en résulte[249]. La prétention du droit à normaliser la réalité se manifeste par le recours à l'abstraction et non par des abstractions[250].

88. « Le droit est-il logique ? »[251]. Des explications supplémentaires proviennent de certains auteurs français[252] qui ont théorisé la logique et l'actualité des normes juridiques à travers des questions telles que « le droit est-il logique ? ». L'utilisation du mot « norme » en droit équivaut à « l'idée que quelque chose doit être ou se produire, en particulier qu'un homme doit se conduire d'une certaine façon »[253]. La question essentielle pour les juristes concerne la

---

[241] F. Archer, « *La criminologie confrontée aux nouvelles technologies* », in Dalloz IP/IT 2024. p. 555.
[242] P. Knepper, P.-J. Ystehede (dir.), *The Cesare Lombroso Handbook*, Routledge, Londres, 2013. 384 p.
[243] P. Semeraro, *Il sistema penale di Gabriel Tarde*, Padoue, CEDAM, 1984, X + 189 p. (Collana di Studi Penalistici, n.s., vol. XXXVI, dir. G. Bettiol et P. Nuvolone).
[244] H. Kelsen, *Théorie pure du droit*, trad. Charles Eisenmann, Paris, Dalloz, 1962.
[245] D. de Bechillon , *Qu'est-ce qu'une règle de droit ?*, Éditions Odile Jacob, Paris, 1997, p.166.
[246] F. Lecoutre, *La controverse entre Hans Kelsen et Eric Voegelin en théorie du droit et en théorie politique*, préface de Renaud Baumert, avant-propos de Carlos Miguel Herrera, Paris, Institut francophone pour la justice et la démocratie – Institut Louis Joinet, coll. « Collection des thèses », n° 195, 2020.
[247] H. Kelsen, *op. cit.*, p.102: « La proposition juridique qui énonce cette norme de droit pénal ne peut avoir que le libellé suivant : si quelqu'un commet un vol, il doit être puni. Mais le Sollen de la proposition juridique n'a pas, comme le Sollen de la norme juridique, un sens prescriptif ; il n'a qu'un sens descriptif. »
[248] *Idem* p.10, « Il est possible que le Code pénal contienne une phrase de ce genre : le vol sera puni de prison. La signification de cette phrase n'est pas, comme sa lettre paraîtrait l'indiquer, une énonciation relative à un certain événement effectif, mais une norme : à savoir l'ordre de punir ou l'habilitation à punir le vol de prison. »
[249] *Idem*, p.102, « La proposition qui décrit une norme de droit pénal en vigueur qui prescrit une peine de prison en cas de vol serait fausse, si elle déclarait que, conformément à cette norme, le vol est puni de prison ».
[250] F. Terré & N. Molfessis, *Introduction générale au droit*, 17e éd., Paris, Dalloz, 2025, p.3.
[251] C'est la question qui ouvre l'ouvrage de H. Rabault, *La logique juridique*, Paris, Dalloz, coll. « Connaissance du droit », 1re éd., 25 janv. 2024.
[252] H. Rabault, *La logique juridique*, Paris, Dalloz, coll. « Connaissance du droit », 1re éd., 25 janv. 2024.
[253] H. Kelsen, p.149, cité par C. Puigelier, « *Géraldine Aïdan*, *Le fait psychique, objet des normes juridiques* », in *RTD* civ. 2017, p.518. Consulté en ligne le 15.07.2025: https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=RTDCIV/CHRON/2017/0229. Thèse de droit public rédigée sous la

compréhension du sens normatif « qu'il faut attribuer logiquement à une certaine construction de langage donnée comme norme de droit »[254]. La logique de la genèse de la norme juridique ne peut être assimilée à un simple traitement de la pathologie des cas sociaux – « à sa façon, le droit est une grammaire »[255].

Lorsque nous discutons de l'acte d'émettre des théories juridiques susceptibles de générer une législation, « les statuts logiques et empiriques des énoncés théoriques s'avèrent parfois complexes à déterminer »[256]. La difficulté de trouver les meilleurs outils concernant la logique de la normalisation de la réalité empirique est accentuée par cette dynamique de la révolution numérique. Dans le même temps, la raison qui sous-tend une théorie juridique ne peut pas couvrir tous les faits auxquels elle devrait s'appliquer[257], mais cet écart peut être bénéfique pour l'évolution du droit[258].

§2. L'OBÉSITÉ DU DROIT ET LE CONTRÔLE DE LA PRODUCTION LÉGISLATIVE

89. Risque d'inflation normative[259]. L'engagement de l'UE à réglementer l'intelligence artificielle et à garantir une protection efficace de la vie privée se reflète dans deux instruments normatifs majeurs : le Règlement (UE) 2016/679 relatif à la protection des données à caractère personnel, applicable depuis le 25 mai 2018, et le Règlement (UE) 2024/1689 relatif à l'intelligence artificielle (AI Act), adopté le 13 juin 2024. Ces deux actes normatifs marquent une étape décisive dans la construction d'un cadre juridique européen capable de répondre aux défis numériques contemporains. En revanche, tant la France que la Roumanie connaissent déjà

direction du professeur Étienne Picard, Université Panthéon-Sorbonne (Paris I), 2012, 562 pages, CNRS éditions, 2017 (sous le titre *L'invention du sujet psychique en droit. De l'intime saisi par les normes juridiques*).

[254] M. Grawitz, *Méthodes des sciences sociales*, 11e éd., Paris, Dalloz, 2000, p.173.

[255] F. Terré & N. Molfessis, *op. cit.*, p.2.

[256] V. Champeil-Desplats, *Méthodologies du droit et des sciences du droit*, 3e éd., Paris, Dalloz, 2022, p.299.

[257] P. Feyerabend, *Contre la méthode. Esquisse d'une théorie anarchiste de la connaissance*, Seuil, 1979.

[258] « D'autre part, plus radicalement, il est possible qu'une contradiction entre des faits et des théories s'avère bénéfique à l'avancée de la science dès lors que l'on accepte de raisonner à partir de cette contradiction de façon contre-inductive. Scientifiquement, une théorie dont la fausseté serait finalement établie garde donc une utilité », Feyerabend, *Contre la méthode,* paraphrasé par Champeil-Desplats, *op. cit.*, p.299.

[259] *Lexique des termes juridiques 2025-2026*, sous la dir. de S. Guinchard et T. Debard, 33e éd., Paris, Dalloz, 2025 : « Expression qui désigne le phénomène contemporain de multiplication des textes juridiques (lois, décrets, arrêtés, règlements, directives), dû principalement à la pluralité des autorités normatives (Parlement, Gouvernement, assemblées locales, Union européenne, CEDH), la spécialisation du droit (et l'émergence de nouveaux domaines), mais aussi à la méconnaissance des règles de la légistique et à une tendance à considérer que la loi pourrait résoudre tous les maux de la société. Elle se traduit par des vices de la loi (dispositions inutiles, contradictoires, ou sujettes à interprétation divergente) et constitue ainsi un obstacle à l'intelligibilité et à l'accessibilité, qui sont pourtant des objectifs de valeur constitutionnelle, en lien avec le principe de sécurité juridique. Une mission parlementaire a présenté une multitude de propositions destinées à améliorer la fabrique de la loi. Une circulaire du Premier ministre du 26 juillet 2017 vise à réduire le flux des textes réglementaires et à mieux mesurer leur impact ».

de sérieux problèmes liés à l'inflation normative/législative[260] et l'élaboration de nouvelles réglementations spécifiques aux algorithmes s'inscrit dans un contexte tumultueux.

90. Le poids de la réglementation gouvernementale : France (115) vs Roumanie (124). La France pourrait même célébrer le centenaire du concept d'inflation législative, étant donné que les premières discussions sérieuses sur ce sujet ont eu lieu dès 1926[261]. Une étude réalisée en 2017[262] en comparant la situation de 138 pays place la France à la 115e place en termes de charge réglementaire gouvernementale.

La situation de la Roumanie n'est pas très différente, puisqu'elle occupe la 124e place dans ce classement. Cet indicateur mesure la perception du monde des affaires concernant le degré de rigidité, les coûts et la complexité de la législation imposée par les États.

91. Contrôle de la production législative : une nouvelle norme en remplace deux anciennes. Cette étude a été invoquée en 2017 dans une proposition de résolution relative à la simplification des règles qui entravent la vie économique[263]. Auparavant, le Premier ministre français avait publié une circulaire visant à contrôler le flux des textes juridiques et leur impact[264].

La tâche de superviser la production législative incombe au Parlement, mais cette directive, toujours en vigueur aujourd'hui, établit assez clairement le processus de simplification : « toute nouvelle norme réglementaire doit être compensée par la suppression ou, en cas d'impossibilité avérée, la simplification d'au moins deux normes existantes »[265].

A. Prédisposition à une réglementation excessive

[260] N. Nitsch, « *L'inflation juridique et ses conséquences* », in Archives Phil. dr. 1982. 167 ; J. Carbonnier, *op. cit.*, p.271 ; P. Deumier, « *Rapport sur la lutte contre l'inflation législativ*e », D. 2013. 1264.

[261] J. Henning, *Introduction historique au droit*, 1re éd., Paris, Dalloz, 2025, p.530 - « À partir de 1926, des journalistes commencent à parler "d'inflation législative" pour critiquer l'abondance de lois et de réglementations. Les lois se multiplient dans tous les domaines. Pour les questions seulement locales, on passe par une loi d'intérêt local. Sur une seule journée parlementaire, une chambre peut voter plus de vingt lois d'intérêt local. Surtout, et c'est là le phénomène nouveau, les lois sont de plus en plus longues en articles ».

[262] *The Global Competitiveness Report 2017-2018*, World Economic Forum, Genève, octobre 2017.

[263] Proposition de résolution n° 724 (2016-2017), « *Simplification des normes entravant la vie économique* », Sénat, déposée le 28 septembre 2017.

[264] Circulaire du Premier ministre du 26 juillet 2017 relative à la maîtrise du flux des textes réglementaires et de leur impact.

[265] « L'entrée en vigueur d'un décret réglementaire comportant des mesures constitutives de normes nouvelles contraignantes (obligations de mise en conformité, nouvelles formalités administratives, etc.) opposables aux acteurs de la société civile (entreprises, associations, particuliers), aux services déconcentrés et aux collectivités territoriales est désormais conditionnée par l'adoption simultanée d'au moins deux mesures d'abrogation ou, de manière subsidiaire, de deux mesures de simplification de normes existantes », *Circulaire du Premier ministre du 26 juillet 2017 relative à la maîtrise du flux des textes réglementaires et de leur impact*.

92. « L'obésité » du droit français en 2025. Le suivi ultérieur[266] des effets de cette circulaire, également connue sous le nom de « deux pour un »[267], a montré que son impact n'était pas significatif et que la prédisposition à une réglementation excessive était toujours d'actualité. Comme si l'inflation législative devait être combattue par une inflation de rapports et d'analyses « l'obésité du droit s'évalue et se diagnostique »[268], les statistiques publiées en 2025 ne sont guère encourageantes[269]. Le volume de la production législative est énorme : plus de 96.000 articles de loi et plus de 260.000 articles à valeur réglementaire (décrets, arrêtés ministériels, circulaires, etc.), qui ne représentent qu'une partie minoritaire du droit actuel[270].

93. Rapport : 400.000 textes législatifs. L'un des rapports précédents sur ce sujet montre que le nombre total de textes législatifs en vigueur est de 400.000[271], et les données plus récentes indiquent que le site Legifrance.fr a enregistré une augmentation de plus de 87 % au cours des dix dernières années, pour atteindre 42 millions de mots[272]. Toutefois, en analysant la situation au cours des 20 dernières années, telle qu'elle ressort du bilan publié en 2025, on constate une stabilité du nombre de lois adoptées chaque année, avec une moyenne de 50 lois par an. L'année 2024 a apporté une nouvelle relativement positive, avec 39 lois en moins par rapport aux années précédentes.

94. La longueur des lois et le nombre de mots ont augmenté. Les statistiques ont également montré que pour chaque loi promulguée, leur longueur, le nombre d'articles et le nombre de mots ont augmenté de manière constante[273]. En revanche, cette baisse de la production législative s'est traduite par une augmentation du nombre d'ordonnances promulguées par le gouvernement. Ces chiffres impressionnants ne font que dévaloriser les lois,

---

[266] M. Anthony Brosse, *Question écrite n° 1584 : Bilan de la suppression de normes*, Assemblée nationale, publiée le 27 septembre 2022, réponse publiée le 11 octobre 2022.

[267] « Circulaire du Premier ministre du 26 juillet 2017 relative à la maîtrise du flux des textes réglementaires et de leur impact. Depuis septembre 2017, le mécanisme du "2 pour 1" exerce un effet dissuasif certain dans la production normative : 38 décrets entrant dans le champ ont été publiés sur Légifrance après compensation ; 7 décrets ont été publiés après abandon des dispositions contraignantes envisagées ; 9 projets de décret ont été définitivement abandonnés », Rép. min. n° 1584, JO, 11 oct. 2022.

[268] F. Terré & N. Molfessis, *op. cit.*, p.502.

[269] Secrétariat général du Gouvernement (SGG), *Indicateurs de suivi de l'activité normative — édition 2025*, Paris, 5 mai 2025, publié sur Légifrance.

[270] F. Terré & N. Molfessis, *op. cit.*, p.504.

[271] Rapport Lambert-Boulard, *Mission de lutte contre l'inflation normative*, 26 mars 2013 (Doc. fr., 2013), cité par R. Cabrillac, *Introduction générale au droit*, 16e éd., Paris, Dalloz, 2025, p.186.

[272] C. Eoch-Duval, « *Un "mal français : son e-norme" production juridique ?* », in RDP 2022, no 2, p.421.

[273] « *L'inflation proprement législative tient d'ailleurs désormais moins au nombre de textes adoptés par le Parlement qu'à leur volume. Le phénomène est notable ; il conduit souvent à une indigestion du seul fait de la lecture des textes, tant leur longueur est parfois démesurée. Le nombre moyen d'articles contenus dans une loi a presque doublé entre 1990 et 2009, pour se stabiliser ensuite (mais la longueur des articles s'est accrue*) », F. Terré & N. Molfessis, *op. cit.*, p.504.

dégrader la qualité de la réglementation[274], son efficacité et la confiance de la population dans leur cohérence et leur nécessité[275].

La question suivante apparaît donc pertinente : « les machines des légistes, qui cherchent désormais à évaluer l'instabilité normative, pourront-elles un jour mesurer le taux de droit dans l'air que l'on respire ? »[276]. Paradoxalement, l'insécurité juridique est provoquée précisément par les réformes qui visent à réformer les réformes précédentes[277].

95. En Roumanie, une loi est publiée chaque jour. L'inflation législative en Roumanie est un sujet d'actualité, mais elle bénéficie de peu d'attention de la part de la littérature juridique ou des acteurs gouvernementaux. Il n'existe pas de rapports clairs similaires à ceux publiés en France, ni de registres répertoriant le nombre d'actes normatifs, le nombre d'articles ou le nombre de mots, ni de prises de position publiques sur ce sujet. Le Conseil législatif publie chaque année un registre des actes normatifs primaires sans autres critères statistiques de classification[278]. Selon ces registres, environ 12.500 actes normatifs primaires (lois, ordonnances gouvernementales, ordonnances d'urgence) sont en vigueur et, en 2024, une nouvelle loi a été publiée chaque jour, et une ordonnance d'urgence a été publiée tous les deux jours et demi. Concrètement, 500 actes normatifs primaires s'ajoutent chaque année au corpus législatif roumain.

B. La transposition des directives européennes, un problème typiquement français?

96. Surtransposition[279]. Au vu des chiffres et des critiques présentés ci-dessus, les réflexions exprimées par Montaigne semblent d'actualité : « nous avons en France plus de lois que tout le reste du monde ensemble et plus qu'il n'en faudrait pour régler le monde » et de Rousseau – « tout État où il y a plus de lois que la mémoire de chaque citoyen ne peut en contenir est un État mal constitué »[280].

---

[274] Ph. Martin, « *L'inflation législative et la qualité de la réglementation* », rapport pour le Conseil d'État publié le 29 mai 2017.
[275] R. Cabrillac, *op. cit.*, p.187.
[276] La question que l'on retrouve dans F. Terré & N. Molfessis, *op. cit.*, p.504, paraphrase l'article « *Laissez-nous respirer* !» titre Le Point, 31 juill. 2014 : Normes, formulaires, guichets. Le palmarès des réglementations absurdes.
[277] F.-X. Lucas, *Manuel de droit de la faillite*, 5e éd., Paris, PUF, 2024, n° 7 – « il semble que la réforme de la réforme de la réforme soit devenue l'activité favorite d'un législateur qui, pressé d'agir sur le cours des événements économiques, légifère en permanence, sans égard pour l'insécurité juridique qui résulte inévitablement de ces évolutions ».
[278] Le Conseil législatif, Répertoire de la législation roumaine, 29e édition, peut être consulté ici : http://www.clr.ro/repertoriile-legislatiei-romaniei/
[279] V. J. Martinez, « *La conception française des "surtranspositions" des directives* », in *RDP* 2021, p.1645.
[280] *Fragments politiques*, IV, « Des lois », § 6, cité par R. Cabrillac, *op. cit.*, p.187.

Au-delà du débat sur l'inflation normative en soi, le droit français est également confronté à un phénomène qui ne semble pas être connu du milieu juridique roumain : la transposition excessive des directives européennes ou « surtransposition »[281]. Bien que « le phénomène des ”surtranspositions” soit difficile à saisir », selon le rapport présenté à l'Assemblée nationale dans le but de définir et de lutter contre ce phénomène, il existe deux types de « surtransposition » : active, dans le cas où des mesures supplémentaires sont adoptées en rapport avec la transposition d'une directive dans le droit national, et par omission, lorsque la réglementation existante est maintenue alors que la norme européenne a évolué[282].

97. La transposition excessive, un problème typiquement français. Le zèle excessif[283] du législateur français en matière de transposition des directives a été observé notamment dans les études comparant la situation à celle d'autres États membres[284]. Compte tenu des débats doctrinaux et des tentatives de législation contre la législation excessive[285], la question « la ”surtransposition” du droit de l'Union : mythe ou réalité ? »[286] semble avoir une réponse on ne peut plus claire.

C. Vers une nouvelle ère de codification, dans un contexte instable

98. Vers la codification[287] des algorithmes dans un environnement juridique trouble. Les discussions et les actions relatives à la législation des algorithmes s'inscrivent dans le

[281] AN, Rapport d'information n° 532, « Mission d'information sur la surtransposition des directives européennes », 21 déc. 2017 : « a surtransposition est l'adoption ou le maintien de mesures législatives ou réglementaires allant au-delà des exigences minimales d'une directive ».
[282] AN, Rapport d'information n° 532, *op. cit.*
[283] D. Simon, « *Directive* », in Répertoire de droit européen, Dalloz, n° 76, « Problèmes liés à la “surtransposition” ».
[284] Direction de l'initiative parlementaire et des délégations, Service des études juridiques, *La surtransposition des directives européennes*, Note de législation comparée n° 277, févr. 2017.
[285] D. Simon, « *La “surtransposition” du droit de l'Union : mythe ou réalité* ? », in Europe. Mensuel d'actualité du droit de l'Union européenne, LexisNexis, n° 12, déc. 2024, p.11, « *La réflexion sur les risques politiques, mais aussi juridiques, liés à la ”surtransposition”, devenue pandémique, au-delà de multiples rapports et circulaires, a été à l'origine de nombreux projets et propositions de lois, voire de propositions de révisions constitutionnelles, mais sans qu'aucun de ces textes n'ait abouti*. »
[286] D. Simon, *op. cit.*
[287] *Lexique des termes juridiques 2025-2026*, sous la dir. de S. Guinchard et T. Debard, 33e éd., Paris, Dalloz, 2025, p.212 : « (1)La codification, dans sa conception originelle de rassemblement dans un unique code des règles intéressant une matière, vise à donner un souffle cohérent à cette matière (ex. : le Code civil de 1804, le Code de procédure civile de 1976). Aujourd'hui encore, nombre de codes correspondent à cette philosophie et regroupent, de manière ordonnée et cohérente, les matières qui font partie d'une même branche du droit (ainsi C. com., C. pén.). Certains de ces codes comportent une partie législative (dont les articles commencent par la lettre L) et une partie réglementaire (dont les articles commencent par la lettre R), par ex. C. com., CJA, COJ, C. rur. ; (2)Dans un sens plus contemporain: regroupement purement administratif, dans un texte d'origine généralement gouvernementale, d'un ensemble jusque-là épars, de dispositions législatives ou réglementaires intéressant une même matière. On parle de codification à droit constant, mais si les dispositions ainsi rassemblées conservent leur portée et leur force juridique originaires, cette méthode pose des problèmes délicats lorsque la codification ne respecte pas strictement la lettre des textes qu'elle rassemble. »

contexte de ce phénomène d'« indigestion »[288] normative, et la multiplication des réglementations concernant la société numérique augmente de manière exponentielle le risque de méfiance à l'égard de la capacité du législateur à respecter les critères de qualité de la loi : clarté, précision, prévisibilité et modération[289]. L'adoption des actes normatifs européens en matière numérique – du RGPD à l'AI Act – rend presque inévitable la constitution, au niveau national, d'un corpus cohérent de normes, équivalent à une codification sectorielle du numérique et des algorithmes, au-delà de la transposition ponctuelle des directives ou de l'application directe des règlements. D'autre part, certains critiquent le fait que la politique de surveillance de l'espace virtuel européen ne peut être mise en œuvre avec les pleins pouvoirs par les États membres, mais qu'elle est gérée conjointement par les organismes de l'UE[290] en raison d'une interprétation erronée du principe du pays d'origine[291].

99. Est-il trop tôt pour parler de codifications nationales des algorithmes ? Même les normes telles que les avis, les recommandations et les résolutions font partie de ce que l'on pourrait appeler le « droit souple »[292] – en 1930, le juriste britannique Arnold Mac Nair[293] a qualifié de « soft law » les engagements non contraignants pris par les États dans leurs relations internationales – elles seront intégrées dans une telle codification nationale des algorithmes. Je pense que la situation dans laquelle nous nous trouvons aujourd'hui est similaire, par exemple, à l'apparition du Code de la route en France (1921). Même si « le développement de l'automobile au début des années 1900 ne posait pas de difficultés dans la mesure où le nombre et la puissance des véhicules étaient assez faibles »[294], avec le développement technologique, l'élaboration de normes claires est devenue une obligation pour l'État.

100. Méfiance à l'égard de l'éthique des géants de l'informatique en matière de protection de la vie privée. Le besoin de réglementation[295] découle notamment de la méfiance manifestée tant par la société que par le milieu juridique à l'égard de la capacité et de l'intérêt des géants de l'informatique qui gèrent les algorithmes et l'intelligence artificielle à respecter les normes éthiques et la vie privée des utilisateurs[296]. Pour la codification révolutionnaire en

---

[288] R. Savatier, *L'inflation législative et l'indigestion du corps social*, Dalloz, 1977. Chron. 43.
[289] O. Décima, S. Detraz et É. Verny, *Droit pénal général*, 6e éd., Paris, LGDJ, 2024. p.44 .
[290] Th. Douville, « *De l'amputation discutable de la compétence des États membres de l'Union européenne pour encadrer le secteur numérique* », in *D.* 2024, p.19.
[291] J. Charpenet, « *Entre optimisation juridique des pouvoirs privés numériques et Digital Services Act, où en sommes-nous de l'application du principe du pays d'origine* ? », in Dalloz IP/IT 2024. p.237.
[292] B. Beignier & A.-L. Thomat-Raynaud, *Introduction au droit*, 9e éd., Paris, LGDJ-Lextenso, 27 août 2024, section 2 « *La source en puissance : le « droit souple »*.
[293] A. D. McNair, « *The Functions and Differing Legal Character of Treaties* », in British Yearbook of International Law, vol. 11, 1930, p.100-118.
[294] J. Henning, *op. cit.*, p.532.
[295] P.,BONIS, *et all., Enjeux numériques, Compliance et nouvelles régulations*, Annales des Mines, n° 30, 2025.
[296] W. Hoffmann-Riem, « *Artificial Intelligence as a Challenge for Law and Regulation* », in T. Wischmeyer et T. Rademacher (dir.), *Regulating Artificial Intelligence*, Cham, Springer, 2020.

matière pénale (1791) – méthode d'organisation rationnelle du droit – les objectifs étaient clairs : clarifier et rationaliser le droit[297].

Même si nous savons que la présomption de connaissance de la loi est une convention technique sans rapport avec la réalité sociale[298] et qu'une production supplémentaire de lois créées spécialement pour les algorithmes aurait également des effets négatifs, les objectifs initiaux peuvent être considérés comme tout aussi valables aujourd'hui. Dans ce contexte, la réglementation des algorithmes risque d'être traitée de manière plus formelle, sans examen critique détaillé des risques, de la clarté ou des effets réels.

Section 6
REPÈRES CONCEPTUELS DANS LA RECONFIGURATION DE L'ATTEINTE À LA VIE PRIVÉE : ÉLÉMENTS CLÉS DE LA RECHERCHE

101. Les mécanismes du droit pénal entre « être » et « devoir ». La distinction kelsenienne entre « être » (*Sein*) et « devoir » (*Sollen*) domine encore aujourd'hui les mécanismes du droit pénal, à une époque régie par les données et les algorithmes. L'ère numérique dans laquelle nous vivons aujourd'hui nous montre que le droit pénal fonctionne également sous la forme binaire exposée précédemment. Il est tout aussi utile d'analyser la dualité[299] entre ces deux concepts, qui peuvent être adoptés tant par le domaine juridique que par la philosophie, la sociologie ou même l'informatique. En conclusion, la norme de droit pénal capable de faire face aux chiffres et aux algorithmes doit être utilisée simultanément comme une épée et comme un bouclier[300], car elle doit établir une séparation assez claire avec la moralité.

102. Le doublement de l'action par l'expérience corporelle. Il ne faut pas perdre de vue que l'utilisation du verbe « être » ne se réfère pas seulement à la manière dont les théoriciens du droit décrivent l'action d'incriminer un comportement humain à ce qu'il « est », mais aussi

---

[297] J. Henning, *op. cit.*, p.429.

[298] R. Merle et A. Vitu, *Traité de droit criminel*, t. I, 7e éd., Paris, Cujas, 1997, n° 550.

[299] H. Rabault, *op. cit.*, p.20 : « *C'est ainsi que Kelsen insistait sur le « dualisme de l'"être" et du "devoir-être", de l'indicatif et du normatif* ». La distinction de Kelsen pose à vrai dire un problème dans la traduction française, car la distinction allemande entre *Sein* (être) et *Sollen* (devoir-être) ne connaît aucune équivalence littérale en français. Selon Kelsen, les propositions juridiques ont ainsi le sens non d'un « être » mais d'un « devoir-être ». Cela heurte certes l'expérience concrète du juriste, qui applique sans cesse des propositions formulées à l'indicatif. Mais Kelsen expliquait les choses ainsi : « Il est possible que le Code pénal contienne une phrase de ce genre : le vol sera puni de prison. La signification de cette phrase n'est pas, comme sa lettre paraîtrait l'indiquer, une énonciation relative à un certain événement effectif, mais une norme : à savoir l'ordre de punir ou l'habilitation à punir le vol de prison. »

[300] S. Van Drooghenbroeck, « *Droit pénal et droits de l`Homme le point de vue de la Cour européenne des droits de l`Homme* », in Les droits de l`Homme bouclier ou épée du droit pénal, Facultés universitaires Saint Louis, coll Publications des facultés universitaires Saint Louis 2007, p.75.

au sujet passif ou actif d'un délit. Bien que certains auteurs[301] soutiennent que le droit accorde un traitement spécifique à celui qui « agit »[302] et que l'action doit être doublée d'une « expérience corporelle »[303], face aux systèmes d'intelligence artificielle, les choses semblent changer radicalement.

103. Reconfiguration. Le droit pénal se reconfigure non seulement parce que « l'action » génératrice de danger public, l'élément matériel, n'est plus seulement un geste corporel extériorisé, mais aussi parce que l'objet juridique et les valeurs protégées sont en constante évolution. « Il y a de plus en plus de droit pénal »[304] est une affirmation que l'on retrouve de plus en plus souvent dans la doctrine pour montrer le besoin accru de sécurité[305], sans minimiser le rôle des autres branches du droit. Il est certain que le délit trouve son origine dans une réalité sociale en évolution et qu'il vise à empêcher un « acte dirigé contre la société, contre l'ordre établi, même si la victime est un simple particulier »[306].

§1. CONSENTEMENT DE LA VICTIME

104. Dématérialisation – atteinte à la vie privée. Dans l'évolution de cette dématérialisation, le délit d'atteinte à la vie privée de l'ancien Code pénal français (art. 368[307]) semble être un modèle digne d'intérêt : « le délit de captation de paroles suppose qu'une atteinte intolérable ait été portée à l'intimité de la vie privée de la personne qui s'en prétend la victime »[308]. Dans le même contexte, la Cour de cassation soutient que l'élément matériel du délit d'atteinte à la vie privée est constitué par le fait de soumettre la victime « à une atteinte à l'intimité de la vie privée sans que celle-ci soit nécessairement intolérable ».

105. Élément matériel de l'infraction d'atteinte à la vie privée. La discussion sur l'élément matériel de l'infraction d'atteinte à la vie privée, analysée en détail dans la thèse, est devenue controversée dans le contexte d'une intervention de la Cour de cassation du 16 mars 2016,

---

[301] N. Anciaux, *Essai sur l'être en droit privé*, Paris, LexisNexis, Hors collection, 1re éd., 17 oct. 2019, 374 p.
[302] N. Anciaux, *op. cit.*, p.26 : « *le droit réserve un sort à celui qui agit. Et justement l'aptitude à agir - avec le présupposé d'une conscience spécifique - permet de reconnaître « l'< être > » par différence d'avec d'autres entités, animaux [...], robots et personnes morales, embryons et entreprises*. »
[303] *Idem*, p.27 : « *Le droit se saisit de l'existence des hommes (ou des êtres humains) par la voie d'une personnification concrétisée par - outre l'action - une « expérience corporelle*. »
[304] P. Beauvais, D. Chilstein & E. Dreyer (dir.), *op. cit.*, p .4.
[305] *Ibidem*, p.4 : « *Il ne s'agit pas de dire que le pénal se développe au détriment des autres branches du droit mais de constater que le système juridique a tendance à se démultiplier afin de répondre à un besoin accru de sécurité lié à la complexification du monde moderne. Plus il y a de normes, perçues comme essentielles dans la société, et plus il y a d'occasions pour le législateur d'incriminer la violation de ces normes* ».
[306] Ph. Jeandidier, *Droit pénal général*, Montchrestien, coll. « Domat droit public », 1991, p.25.
[307] En vigueur de 1978 à 1994.
[308] Cour de Cassation, Chambre criminelle, 3 mars 1982, n° 80-95.226, Dalloz 1982, Jurisprudence, p.413.

lorsqu'il a été établi que la diffusion non autorisée[309] d'une photo intime ne remplit pas les conditions de typicité[310] si l'acte initial de capture de l'image dans un espace privé a été réalisé avec le consentement de la personne concernée[311].

La question du consentement de la victime est sensible lorsque l'on analyse le délit d'atteinte à la vie privée, car la règle veut que le droit pénal soit un droit d'ordre public et que la volonté individuelle ne devrait pas avoir de conséquences – « en principe, le consentement de la victime ne fait pas disparaître une infraction »[312].

106. L'élément central de l'atteinte à la vie privée : le consentement. Le consentement de la victime[313] est l'un des éléments centraux de l'analyse du délit d'atteinte à la vie privée, tant en droit pénal roumain qu'en droit pénal français.

La « voie du consentement »[314] n'est plus seulement un concept philosophique utilisé par Paul Ricœur pour décrire le « refus » et l'« acceptation » comme de simples dimensions de la liberté de conscience et de la responsabilité[315], mais représente un élément essentiel dans la structure logique et juridique des infractions qui protègent la vie privée. La difficulté de l'analyse provient du fait que « une grande partie de la doctrine française est hostile à la reconnaissance d'une efficacité du consentement en droit pénal, principalement au stade de la justification, c'est parce que traditionnellement, l'infraction est conçue uniquement comme un fait contraire à la loi pénale »[316].

Étant donné que, en droit pénal, le consentement n'a pas une valeur purement théorique[317], mais constitue un élément intrinsèque de l'infraction d'atteinte à la vie privée, il

---

[309] En référence à l'article 226-2 du Code pénal : « *Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1* ».

[310] Crim. 16 mars 2016, n° 15-82.676 , P nº 86 ; CCE 2016, comm. 42, note A. Lepage ; JCP 2016. 658, note J.-Ch. Saint-Pau, Légipresse 2016. 275 , n° 338, note I. Soskin.

[311] « *N'est pas pénalement réprimé le fait de diffuser, sans son accord, l'image d'une personne réalisée dans un lieu privé avec son consentement* », Cass. crim., 16 mars 2016 , n° 15-82.676 : JCP G 2016 , 658 , note Saint-Pau ; Dr. pén. 2016 , comm. 73 , obs. Conte ; D. 2016 , p. 935, note Serine.

[312] Ph. Salvage, *Le consentement en droit pénal* : Rev. sc. crim. 1991, p. 705 . - X. Pin, *Le consentement en matière pénale* : LGDJ 2002, cités en JCl. Not. Rép., V° Vie privée, fasc. 20, « Jouissance des droits civils. – Droit au respect de la vie privée. – Régime. Actions », par J.-Ch. Saint-Pau, LexisNexis, 1re publ. 10 mai 2019, dern. mise à jour 28 févr. 2024.

[313] V.-A. Fahmy-Abdou, « *Le consentement de la victime* », Paris, in *LGDJ*, Bibliothèque de sciences criminelles, t. XI, 1971, préf. R. Vouin.

[314] P. Ricœur, *Le volontaire et l'involontaire*, coll. « Philosophie de l'esprit », Aubier, Paris, 1948.

[315] Des explications supplémentaires sur la manière dont Ricœur comprend le terme « consentement » peuvent être trouvées dans l'ouvrage d'Olivier Abel, professeur émérite de philosophie et d'éthique (O. Abel, « *Le chemin du consentement ou L'adolescence du consentement* », article publié le 11 septembre 2022 sur le blog Olivier Abel).

[316] G. Rabut-Bonaldi, *Le préjudice en droit pénal*, vol. 159, Nouvelle Bibliothèque de Thèses, préf. J.-Ch. Saint-Pau, Dalloz, Paris, 2016, p.126.

[317] X. Pin, « *Le consentement en matière pénale* », Paris, in *LGDJ*, Bibliothèque de sciences criminelles, vol. 36, 2002, p. 116.

convient de mettre en balance les intérêts individuels et ceux liés à la politique de répression de l'État[318].

A. Interventions critiquables des tribunaux

107. Pratique non uniforme. Bien que la doctrine soit constante quant à la détermination de l'objectif de la répression, à savoir la protection d'un intérêt général et non particulier[319], « il arrive cependant que l'absence de consentement soit un élément constitutif de l'infraction parce que celle-ci, dans sa structure même, a pour objet de sanctionner la seule atteinte frauduleuse ou violente à la libre disposition d'un droit »[320]. La situation de ce type de comportement interdit par l'article 226-2 (diffusion non autorisée d'un enregistrement) mais étroitement lié aux dispositions de l'article 226-1 (captation de l'enregistrement) avait déjà donné lieu à une pratique non uniforme[321][322] en France au niveau des juridictions inférieures.

Une condition nécessaire avant de poursuivre l'infraction incriminée par l'article 226-2 est que tous les éléments constitutifs de la variante de l'article 226-1 doivent être prouvés. S'agissant d'une infraction résultant d'une violation du droit à la vie privée, elle ne peut être analysée indépendamment de celle-ci[323].

108. Interprétation restrictive vs interprétation extensive. La décision de la Cour de cassation de mars 2016 a reconfirmé cette rupture existant au niveau de la jurisprudence et a été critiquée par les juristes[324] sous l'angle de l'interprétation extensive des aspects favorables

---

[318] V. R. Merle et A. Vitu, *op. cit.*, nº 476.

[319] R. Merle et A. Vitu, *Traité de droit criminel*, Cujas, tome 1, *Problèmes généraux de la science criminelle, droit pénal général*, 7e édition, 1997.

[320] J.-Ch. Saint-Pau, « *Jouissance des droits civils. – Droit au respect de la vie privée. – Régime. Actions* », in JurisClasseur Notarial Répertoire, V° Vie privée, fasc. 20, LexisNexis, 1re publ. 10 mai 2019, dern. maj 28 févr. 2024.

[321] Cour d'appel de Rouen, chambre correctionnelle, n° 08/00962, 25 juin 2009, a estimé qu'il y avait atteinte à la vie privée par le biais de la diffusion, même si la photo avait été prise dans le cadre d'une « capture » acceptée par la victime - « sans doute animé d'un esprit de vengeance suite à une séparation qu'il supporta difficilement, fixer et diffuser en les téléchargeant sur le site Emule, sans le consentement de celle-ci, ces deux photographies de Mathilde D... prises dans un lieu privé et, ce faisant, David Y... a bien volontairement porté atteinte à l'intimité de la vie privée de cette personne. Ce délit prévu et réprimé par l'article 226-1 du Code pénal étant caractérisé en tous ses éléments constitutifs ».

[322] Cour d'appel de Montpellier, 3e chambre correctionnelle, 2 février 2006, a estimé qu'il n'y avait pas d'atteinte à la vie privée au sens de l'article 226-2, même si la victime avait accepté d'être photographiée dans un espace privé : « les dispositions de l'article 226-2 du Code pénal impliquent que les conditions de l'incrimination prévues par l'article 226-1 du Code pénal soient réunies, or les photographies conservées puis divulguées par M. B ont été prises avec l'accord de Mme S ; la cour ne peut dès lors que constater que les faits qui lui sont déférés ne constituent pas une infraction pénale ».

[323] E. Dreyer, *Droit pénal spécial*, Ellipses, 3e éd., 2016, n° 449. - V. Malabat, *Droit pénal spécial*, Dalloz, 7e éd. 2015, n° 617.

[324] I. Soskin, *Atteinte à l'intimité de la vie privée : dans l'attente de la loi pour une République numérique, débats autour de l'interprétation de l'article 226-1 du Code pénal*, Cour de cassation (crim.), 16 mars 2016, n° 15-82.676, Légipresse 2016, p.275.

du droit pénal[325]. L'interprétation restrictive d'une disposition pénale pourrait garantir une meilleure protection de la liberté individuelle[326] et le juge devrait se préoccuper davantage de l'interprétation restrictive (obligatoire) que de l'interprétation extensive (facultative) – « il serait cependant faux d'établir un parallélisme entre l'interprétation restrictive des règles défavorables et celle extensive des règles favorables, car dans le premier cas, l'interprétation restrictive est une obligation et le juge qui ne s'y conforme pas viole le principe de la textualité alors que, dans le second cas, l'extension n'est qu'une faculté accordée au juge qui s'y conformera ou non selon ce qui lui paraît opportun »[327].

109. Intervention rapide, résolution partielle du problème. D'autre part, cette décision de mars 2016 a incité le législateur à intervenir assez rapidement et le Sénat a ainsi adopté, dans le cadre de la loi sur la République numérique, un amendement visant à ajouter un nouveau paragraphe à l'article 226-2 afin de résoudre le problème signalé dans la pratique judiciaire : « est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou document obtenu à l'aide de l'un des actes prévus à l'article 226-1 ». Cet amendement n'est jamais entré en vigueur.

110. La reconfiguration qui a mis fin aux erreurs d'interprétation. Dans le même contexte, l'article 226-2-1 a été ajouté[328], qui vise à incriminer « toute diffusion d'image ou de paroles à caractère sexuel sans le consentement de la personne concernée, même si la personne a donné son accord exprès à la captation de ce document ou a elle-même capté ces images ou paroles »[329]. Enfin, par la loi n°2016-1321 du 7 octobre 2016 une République numérique[330], seule la modification relative à la diffusion d'images à caractère sexuel est entrée en vigueur,

---

[325] Voir le commentaire de I. Soskin, *Atteinte à l'intimité de la vie privée : dans l'attente de la loi pour une République numérique, débats autour de l'interprétation de l'article 226-1 du Code pénal*: « L'interprétation stricte de la loi conduit à en déduire que le consentement présumé doit porter sur chacun des actes et non sur un seul d'entre eux. L'analyse combinée des différents alinéas de l'article 226-1 devrait conduire à penser que l'absence de consentement à l'un des actes, dont notamment l'acte de transmission, est de nature à engager la responsabilité pénale de l'auteur. Or, la Cour de cassation semble faire une application non pas stricte, mais extensive de la loi, transposant la présomption de consentement à des actes matériels qui n'ont pas été spécifiquement autorisés ».

[326] M.-L. Rassat, *Le droit pénal*, 2e éd., coll. « Connaissance du droit », Dalloz, Paris, 2025.

[327] M.-L. Rassat, *op. cit.*, p.28.

[328] La forme de l'article 226-2-1 du Code pénal, entré en vigueur par la loi n°2016-1321 du 7 octobre 2016, est la suivante : « Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende. Est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1 ».

[329] Voir la motivation fournie dans l'amendement adopté par le Sénat - https://www.senat.fr/enseance/2015-2016/535/Amdt_651.html

[330] *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique,* JO, 2016. Voir https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746

dans le but de lutter contre le phénomène de la *revenge porn*[331], de plus en plus présent à l'ère numérique. Cette reconfiguration a mis fin aux erreurs jurisprudentielles qui ont conduit la Cour de cassation à rendre son arrêt du 16 mars 2016[332].

111. Recours en droit civil pour la transmission d'autres images et conversations. Ainsi, la question des photos sans contenu sexuel mais prises dans un espace privé et diffusées au public reste encore sans réponse dans le droit pénal français, le recours se trouvant actuellement exclusivement dans le droit civil[333].

B. Vision différente quant à la définition des termes

112. Israël, premier pays à avoir réprimé la diffusion d'images intimes sur Internet. Pour réprimer ce type de comportement, la vision du droit pénal a présenté certaines nuances d'un pays à l'autre[334], même si l'objectif est le même : par exemple, Israël a considéré que la diffusion dans l'espace public d'images intimes sans le consentement de la victime est un délit de nature sexuelle et que l'auteur est un « délinquant sexuel » ; Le Canada a introduit le délit de « diffusion d'images intimes » dans la section 162.1 du Code pénal, considérant qu'il s'agit d'un acte de cyberharcèlement[335].

113. Le droit pénal roumain a réagi sept ans plus tard. Le droit pénal roumain a réagi de manière inattendue tardivement, sept ans après le droit pénal français, et ce n'est qu'en juin 2023 qu'il a introduit une nouvelle infraction similaire à celle prévue par l'article 226-2-1[336]. Concrètement, pour les deux pays, il s'agit d'un délit considéré du point de vue de la protection de la vie privée dans le contexte numérique[337].

---

[331] La lutte contre le harcèlement sexuel en ligne est devenue une préoccupation des systèmes juridiques de la plupart des pays civilisés. Le premier pays à avoir adopté une telle loi est Israël (5 janvier 2014), suivi du Canada (décembre 2014) et du Royaume-Uni (avril 2014).

[332] X. Pin, *Droit pénal général : 2025*, 16e éd., Paris, Dalloz, coll. « Cours Dalloz – Série Droit privé », 2024, p.290.

[333] En matière civile, la Cour de cassation a statué à plusieurs reprises que le consentement peut être déduit de l'attitude de la personne (par exemple, le fait de regarder l'objectif de l'appareil photo) qui se considère par la suite comme victime de la diffusion de l'image, mais l'utilisation de la photographie ne doit pas être détournée du contexte dans lequel elle a été prise ni porter atteinte à la vie privée telle que définie à l'article 9 du Code civil : « La publication de l'image dont s'agit, utilisée dans une perspective différente de celle pour laquelle elle avait été réalisée, exigeait le consentement spécial des intéressés », Cour de cassation, 1re chambre civile, 14 juin 2007, n° 06-13.601.

[334] A. Flynn, *Image-Based Sexual Abuse*, Oxford Research Encyclopedia of Criminology, 2023.

[335] Pour plus de détails, voir A. Wayne MacKay, "Law as an Ally or Enemy in the War on Cyberbullying", *University of New Brunswick Law Journal*, vol. 66 (2015), p.3–60 (https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1783&context=scholarly_works).

[336] *Loi n° 171/2023 du 14 juin 2023 modifiant et complétant l'article 226 de la loi n° 286/2009 relative au Code pénal*, publiée au Journal officiel de la Roumanie, partie I, n° 532, du 15 juin 2023. Disponible à l'adresse : https://legislatie.just.ro/Public/DetaliiDocument/271253.

[337] Voir les détails statistiques et les études comparatives sur les atteintes à la vie privée à l'ère numérique dans *Assemblée nationale, Délégation aux droits des femmes et à l'égalité des chances entre les hommes et les femmes,*

114. Cour de cassation : définition imprécise des éléments constitutifs. Cette modification législative a été examinée par la Cour de cassation dans le cadre d'une Question prioritaire de constitutionnalité[338] (QPC), à l'occasion de laquelle il a été estimé que la formulation de l'article 226-2-1 « qui ne définit pas de manière claire et précise les éléments constitutifs de l'infraction, au regard notamment des textes auxquels il fait expressément référence, est susceptible de méconnaître le principe de légalité des délits et des peines ». Plus précisément, la Cour a estimé qu'il n'était pas clair ce que l'on entendait par mots ou images à caractère sexuel et si ceux-ci avaient été obtenus dans un cadre public ou privé, et que l'imposition du consentement exprès ou présumé de la victime « apparaît en contradiction avec l'article 226-1 du code pénal, auquel il se réfère expressément, et qui ne sanctionne, pour sa part, que la fixation, la captation, l'enregistrement et la transmission d'images ou de propos obtenus sans le consentement de la personne ».

115. Conseil Constitutionnel : la définition est suffisamment claire. Dans ce contexte, lors de la vérification effectuée en septembre 2021, le Conseil Constitutionnel a déclaré que le texte de loi respectait la Constitution et que les termes « présentant un caractère sexuel » et « absence d'accord de la personne pour la diffusion » étaient suffisamment clairs pour prévenir le risque d'interprétations arbitraires. Même si, après ces interprétations, l'article 226-2-1 « est sauvé, de nombreuses incertitudes continuent de planer sur son interprétation »[339].

116. La définition du code pénal roumain, plus claire que celle du code pénal français. Sans trop débattre le sujet dans cette partie de la thèse, je montre qu'en Roumanie, il n'y a pas eu de tensions juridiques aussi vives sur la question de la diffusion d'images à caractère sexuel, et ce pour deux raisons : l'incrimination a récemment été intégrée dans le corpus législatif et la définition de l'infraction est plus claire que la version française, l'article 226, paragraphe 2^2, définit précisément l'« image intime », et la diffusion sans le consentement de la personne concernée doit lui causer une souffrance psychique ou porter atteinte à sa réputation.

C. Interdiction de la commercialisation juridique du consentement

117. Transaction de la volonté ? En règle générale, nous savons déjà que ni l'ancien Code pénal de 1810 ni celui modifié en 1994 ne prévoient de disposition permettant la

Rapport d'information n° 3348 sur le projet de loi pour une République numérique (n° 3318), XIVe législature, par Catherine Coutelle, enregistré à la Présidence le 15 déc. 2015, 247 p.

[338] Cour de cassation, chambre criminelle, arrêt n° 892 du 23 juin 2021, affaire n° 21-80.682.

[339] A. Lepage, « *L'alinéa 2 de l'article 226-2-1 du Code pénal passe et obtient son brevet de constitutionnalité : Atteinte à l'intimité de la vie privée – paroles ou images présentant un caractère sexuel – QPC – principe de la légalité – interprétation* », Communication, commerce électronique, 2021, n° 12, p.33-34.

commercialisation juridique du consentement de la victime, La Cour de cassation s'exprimant ainsi : « accorder un effet exonératoire au consentement de la victime reviendrait à dire que l'accord intervenu entre l'auteur de l'infraction et sa victime serait susceptible de paralyser l'application de la loi pénale et l'exercice de la répression, qui sont d'ordre public »[340].

Le droit pénal français et roumain[341] interdisent clairement la négociation de la volonté de la victime en ce qui concerne les infractions touchant à la vie, à la santé et à l'intégrité physique, mais laisse place à des interprétations concernant les infractions touchant à la vie privée.

118. Consentement permissif en cas d'atteinte à la vie privée. En général, l'infraction est définie comme étant générée par un acte qui porte atteinte aux valeurs sociales, blesse, choque et perturbe l'ordre public, et que la société ne peut accepter. Toutefois, il peut devenir permis lorsque « la valeur sociale protégée n'a été ni menacée, ni lésée car alors la société n'a plus d'intérêt à la répression »[342]. Ainsi, pour exclure le préjudice de nature pénale, le consentement de la victime doit remplir quatre conditions[343] : être prouvé[344], être antérieur au moment de la commission de l'acte[345], être émis par une personne ayant la capacité d'ester en justice et comprenant la portée de l'accord[346], être exprimé librement. En exprimant son consentement permissif dans le cas de l'infraction d'atteinte à la vie privée, la personne concernée « ne fait qu'exercer sa faculté de disposition »[347].

119. Intervention catégorique des tribunaux. La jurisprudence a toujours soutenu que la défense de l'ordre public par le droit pénal prime, qu'il s'agisse du meurtre à la demande de la

[340] C. Mascala, « *Consentement de la victime* », in JurisClasseur Pénal Code, App. art. 122-4 à 122-7, fasc. unique, LexisNexis, 1re publ. 20 avril 2013, mise à jour 23 nov. 2022.
[341] « (2) Le consentement de la personne lésée n'a pas d'effet dans le cas d'infractions contre la vie, ainsi que lorsque la loi exclut son effet justificatif. »
[342] X. Pin, *Droit pénal général : 2025*, 16e éd., Paris, Dalloz, coll. « Cours Dalloz – Série Droit privé », 2024, p.282.
[343] *Idem*, p.292.
[344] Par exemple, conformément aux dispositions de l'article 226-1, si les actes de capture, d'enregistrement ou de transmission d'images ou de conversations ont été réalisés à la vue de tous et que les personnes enregistrées ne s'y sont pas opposées, cette situation constitue une preuve de consentement.
[345] En cas d'atteinte à la vie privée, l'action publique est engagée à la demande de la victime, qui peut ensuite la retirer et empêcher ainsi la poursuite pénale de l'auteur.
[346] X. Pin, *op. cit*., p.292: « *Ainsi, en cas de captation, enregistrement ou transmission de l'image, des paroles ou de la localisation du mineur, le consentement disculpant doit émaner des titulaires de l'autorité parentale* (C. pén., art. 226-1) ».
[347] *Idem*, p.292.

victime[348] (1828), des duels suivis de décès[349] (1837), de simples blessures corporelles[350] (1849), l'un des arguments étant que le mal fait à soi-même se répercute implicitement sur les membres de la famille ou de la communauté[351], sans qu'il puisse y avoir de consentement collectif de leur part.

À partir de ces décisions qui ont été à la base de la définition du droit pénal français et même roumain[352], nous pouvons nous poser la question légitime de savoir si, aujourd'hui, nous avons ou non la liberté totale de choisir ce que nous voulons faire de notre corps.

120. « Lancer de nain » : atteinte à la dignité humaine. Dans ce processus de modelage de la notion d'ordre public et même de l'institution du consentement, la décision du Conseil d'État du 27 octobre 1995[353], qui interdit une attraction bizarre présente dans la société française, le « lancer de nain »[354], apparaît comme pertinente. Dans le cadre de spectacles de divertissement, les spectateurs étaient invités à lancer des personnes handicapées comme s'il s'agissait de projectiles[355]. La Cour a estimé que des mesures de protection avaient été prises pour que les personnes lancées ne soient pas blessées, qu'elles avaient donné leur accord pour être l'objet d'un divertissement contre rémunération, mais que ces spectacles devaient néanmoins être interdits : « par son objet même, une telle attraction porte atteinte à la dignité de la personne humaine ».

---

[348] Cass. crim., 16 nov. 1827, *Sirey* 1828, I, p.135 : « *il importe peu que la mort ait été donnée par l'ordre de la personne homicidée... car les lois qui protègent la vie des hommes sont d'ordre public, les crimes et délits contre les personnes ne blessent pas moins l'intérêt général de la société que la sûreté individuelle des citoyens, et aucune volonté particulière ne saurait absoudre et rendre licite un fait que les lois ont déclaré punissable*. »

[349] Cass. crim., 22 juin 1837, *Sirey*, 1837, I, p.465: « *Une convention par laquelle deux hommes prétendent transformer de leur autorité privée un crime qualifié en action indifférente ou licite, se remettre d'avance la peine portée par la loi contre le crime, s'attribuer le droit de disposer mutuellement de leur vie et usurper ainsi doublement les droits de la société, rentre évidemment dans la classe des conventions contraires aux bonnes mœurs et à l'ordre public*. »

[350] Ch. réunies, 21 juill. 1849, *Sirey*, 1849, I, p.529. On parle d'une décision de la Cour de cassation qui interprète l'abrogation de l'ancien Code pénal concernant le délit de duel. La décision du tribunal précisait que la légitime défense associée au duel est contraire à la morale et à l'ordre public et qu'aucune forme d'agression sur son propre corps ne peut être acceptée par le droit pénal.

[351] R. Merle, A. Vitu, *op. cit.*, p.475: « *Quand un père de famille se bat en duel pour une question d'honneur, il expose stupidement sa femme et ses enfants à subir injustement les conséquences affectives et matérielles de son décès ou de ses blessures ; il crée, d'autre part, un désordre social dont l'État ne peut pas se désintéresser, car le duel est une forme de guerre privée incompatible avec l'ordre public*. »

[352] Le premier Code pénal est entré en vigueur le 1er mai 1865, sous le règne d'Al. I. Cuza, et s'inspirait largement du Code napoléonien de 1810, reprenant également certaines institutions juridiques du Code pénal prussien. À l'instar de la législation pénale française, les infractions étaient classées en crimes, délits et contraventions. Le Code pénal actuel n'utilise plus cette division en trois catégories, les termes « crime » et « délit » prêtant à confusion et ayant été totalement supprimés.

[353] Conseil d'État, Assemblée, *Commune de Morsang-sur-Orge*, 27 octobre 1995, requête n° 136727, Recueil Lebon, p.372.

[354] G. Glénard, « *La dignité de la personne humaine : un ordre de valeurs* ? », in Revue française de droit administratif (RFDA), 2015, p.869.

[355] F. Melleray, « *Relativité des exigences de la dignité de la personne humaine* », in Actualité juridique. Droit administratif (AJDA), 2024, p.269.

121. Limite d'intervention du droit pénal. Il existe déjà des débats sérieux sur ce sujet en rapport avec les sports très violents, le changement de sexe, la chirurgie esthétique ou d'autres méthodes de mutilation volontaire du corps[356].

Où le droit pénal devrait-il intervenir pour déterminer ce que nous avons le droit de faire de notre propre corps dans ce contexte d'évolution technologique ? Comment pouvons-nous modeler notre propre volonté pour nous sentir libres, mais en même temps ne pas nous faire de mal ? Faut-il laisser la vie privée à la disposition d'une transaction purement commerciale entre son « propriétaire » et les géants de l'informatique ? En fait, nous retrouvons cette question encore mieux formulée chez Xavier Pin : « doit-on opter pour un droit paternaliste protégeant l'individu contre lui-même ou pour un droit libéral accordant à l'individu une complète autonomie ? La réponse est certainement dans la voie médiane »[357]. À l'heure actuelle, le droit pénal français et roumain ont la même vision de ce qui peut être consenti ou non par la victime[358], mais il faut admettre qu'il existe des systèmes juridiques dans lesquels le principe d'autodétermination a une signification plus large.

122. Allemagne : la liberté peut être négociée en échange d'une mutilation physique. L'exemple le plus éloquent est celui de l'Allemagne[359], où la responsabilité pénale de ceux qui bénéficient du consentement de la victime en cas d'atteinte à l'intégrité physique est exclue, ou encore le cas d'une personne condamnée pour des infractions à caractère sexuel qui peut négocier sa liberté en échange de l'acceptation de la castration[360], bien qu'il existe des contestations virulentes à ce sujet[361].

En France, on fait référence à un type de traitement médical pouvant équivaloir à une « castration chimique »[362], mais un condamné ne peut en aucun cas négocier son intégrité physique. Le droit pénal italien a également rendu une décision controversée[363] dans laquelle

---

[356] B. Bouloc, *Droit pénal général*, 29e éd., Paris, Dalloz, coll. Précis, 2025, p.410.
[357] X. Pin, « *Le consentement à la lésion de soi-même. Vers la reconnaissance d'un fait justificatif* ? », in Droits, n° 49, 2009, p.83-106.
[358] « *En France on ne peut disposer de sa vie ou de sa santé ou de son intégrité tout homicide sur demande duel stérilisation ou opération chirurgicale non nécessité par l'impératif de la santé reste délictueux* », J. Pradel, *Droit pénal comparé*, 4e éd., Dalloz, Paris, 2016, p.154.
[359] X. Pin, « *La théorie du consentement de la victime en droit pénal allemand : éléments pour une comparaison* », in Revue de science criminelle et de droit pénal comparé (RSC), n° 2, 2003. p.369-392.
[360] K. Amelung, « *Grundsätzliches zur Freiwilligkeit der Einwilligung des Verletzten* », in Neue Zeitschrift für Strafrecht, 2006, p.317-320.
[361] Voir des détails dans Assemblée parlementaire du Conseil de l'Europe, Doc. 13215, 3 mai 2013, Rapport de Mme Liliane Maury Pasquier, Commission des questions sociales, de la santé et du développement durable.
[362] V. Peltier, « *Détention. – Exécution des peines privatives de liberté. – Surveillance judiciaire des auteurs de crimes et délits sexuels* », in JurisClasseur Procédure pénale, Art. 723-29 à 723-37, Fasc. 20, LexisNexis, première publication le 12 janvier 2011, dernière mise à jour le 16 mai 2022.
[363] Cass. Pen., 31 ianuarie 1934, în *Giustizia Penale*, 1934, II, p. 374; nota de E. Battaglini, *L'art. 50 C.p. e gli innesti omoplastici.*

un chirurgien a été acquitté par le tribunal après avoir accepté de transplanter, contre rémunération, les organes sexuels d'un citoyen italien à un citoyen américain[364].

123. La vie privée, plus vulnérable que l'intégrité physique. Ces exemples démontrent que si l'intégrité physique elle-même, valeur éminemment objective et tangible, peut faire l'objet d'une forme de mise à disposition ou de commercialisation, alors la vie privée et les données à caractère personnel, de nature beaucoup plus fragile et intangible, s'avèrent d'autant plus exposées et vulnérables. Nous avons fourni des explications supplémentaires sur la vulnérabilité de la vie privée à l'ère dominée par les algorithmes dans le contenu de la thèse.

D. Le code pénal roumain, en matière de consentement. Vision comparative

124. La vision du Code pénal roumain sur le consentement de la victime. Un danger auquel nous sommes confrontés dans l'analyse des infractions relatives à la vie privée est celui de considérer le consentement comme un fait justificatif[365]. En effet, le droit pénal roumain présente une vision assez hétérogène de la terminologie utilisée pour caractériser les éléments « atypiques » de l'infraction de violation de la vie privée. Certains auteurs préfèrent interpréter l'expression du législateur concernant les causes d'exclusion de l'infraction prévue à l'article 226, paragraphe 4 – la justification d'un intérêt légitime, le consentement de la victime, la commission d'une infraction surprise, des faits d'intérêt public surpris – en utilisant le terme « cause justificative spéciale »[366], d'autres « hypothèse spéciale d'exclusion de la typicité de l'acte »[367], « causes d'exclusion de l'infraction »[368] ou « conditions négatives de typicité »[369].

125. Différences entre le Code pénal français et le Code pénal roumain. À cet égard, il existe certaines différences entre les deux systèmes juridiques, qui peuvent soulever des questions supplémentaires : l'article 22, paragraphe 1, du Code pénal roumain[370] prévoit le consentement de la personne lésée comme cause justificative[371], alors que le Code pénal

---

[364] G. Fiandaca, E. Musco, *Diritto penale. Parte generale*, 3e éd., Zanichelli, Bologne, 2001, p. 227, cité par J. Pradel, *Droit pénal comparé*, p.155.

[365] J. Pradel, *op. cit.*, p.153 – « On serait tenté à première vue d'admettre le consentement de la victime comme cause de justification sur la base de l'adage *Volenti non fit injuria*. Au vrai la question est beaucoup plus délicate. »

[366] T. Toader, M.I. Michinici, A. Crișu-Ciocîntă, M. Dunea, R. Răducanu, S. Rădulețu, *Noul Cod penal. Comentarii pe articole*, Editura Hamangiu, București, 2014, p.388.

[367] M. Udroiu, *Sinteze de drept penal. Partea special,* vol. I, ediția 3, Ed. C.H. Beck, București, 2022, p.375.

[368] V. Cioclei, *Drept penal. Partea specială I*, vol. I, ediția 7, Ed. C.H. Beck, București, 2022, p.231-232.

[369] S. Bogdan, D.A. Șerban, *Drept penal. Partea specială. Infracțiuni contra persoanei și contra înfăptuirii justiției*, ediția a III-a, Ed. Universul Juridic, București, 2022. p.380.

[370] Art. 22 al. 2 du Code pénal - « (1) L'acte prévu par la loi pénale commis avec le consentement de la personne lésée est justifié si celle-ci pouvait disposer légalement de la valeur sociale lésée ou mise en danger ».

[371] M.-L. Rassat, *op. cit.*, p.80: « les faits justificatifs modifient objectivement la criminalité de l'acte en faisant obstacle à la constitution de l'infraction. »

français ne contient pas de telle disposition, ce qui a soulevé des questions dans la doctrine[372]. Concrètement, le Code pénal roumain prévoit quatre causes justificatives générales, tandis que le Code pénal français en prévoit trois.

126. Trois causes justificatives générales. Les deux codes ont un contenu assez similaire en ce qui concerne les trois causes justificatives classiques[373] : la légitime défense, l'état de nécessité et l'autorisation donnée par une loi ou par un ordre émanant d'une autorité légitime[374].

127. Le consentement français, fait justificatif uniquement dans la doctrine. Le consentement est considéré comme un fait justificatif par la doctrine française majoritaire[375], bien que là encore, les choses ne soient pas très claires[376]. Le discours d'autres auteurs[377] semble assez ferme dans le sens où il rejette cette idée : « ainsi, le consentement de la victime qui est parfois présenté comme une circonstance exclusive de l'incrimination (fait justificatif)[378] ne présente pas à la vérité un tel caractère ». L'exemple des infractions de vol ou de viol est donné pour souligner que l'existence du consentement de la victime rend inutile l'analyse du fait justificatif[379].

128. Cause objective de non-responsabilité. Le consentement de la victime[380] est considéré comme une cause objective de non-responsabilité[381] et ne doit pas être confondu avec d'autres

---

[372] B. Bouloc, *Droit pénal général*, 29e éd., Paris, Dalloz, coll. Précis, 2025, p.382 : « Le nouveau Code pénal retient trois faits justificatifs généraux. Dans le premier, celui de l'article 122-4, alinéa 1er, la justification résulte de la prescription ou de l'autorisation de la loi, ou de l'ordre donné par l'autorité légitime. Dans le deuxième, l'acte est imposé par la nécessité de se défendre et il est simplement permis par la loi ; il en est de même pour l'état de nécessité. Enfin, on se demande si, en outre, le consentement de la victime ne serait pas aussi un fait justificatif. »

[373] M.-L. Rassat, *op. cit.*, p.72-80.

[374] Dans le Code pénal roumain, la formulation est légèrement différente de celle utilisée en français (« l'exercice d'un droit ou l'accomplissement d'une obligation »), mais l'essence reste la même.

[375] M.-L. Rassat, *Droit pénal spécial*, 9e éd., Dalloz, Paris, 2024, p. 590 ; B. Bouloc, *Droit pénal général*, 29e éd., Paris, Dalloz, coll. Précis, 2025, p.408 ; C. Mascala, « Consentement de la victime », in *JurisClasseur Pénal Code*, App. art. 122-4 à 122-7, fasc. unique, LexisNexis, 1re publ. 20 avril 2013, mise à jour 23 nov. 2022 - l'auteur estime que dans le cas de l'infraction prévue à l'article 226, le consentement de la victime est une exception à la règle ; J. Pradel, *Droit pénal comparé*, 4e éd., Dalloz, Paris, 2016, p.153 : « Un fait justificatif pas toujours admis le consentement de la victime ».

[376] V.E. Dreyer, *Droit pénal général*, 6e éd., LexisNexis, 2021, n° 1283.

[377] A. Decocq, *op. cit.*, p.296.

[378] P. Doublier, *« Le consentement de la victime* », in Quelques aspects de l'autonomie du droit pénal, ouvrage collectif sous la dir. de G. Stéfani, Paris, Dalloz, 1956, p. 188 et s., cité par A. Decocq, *op. cit.*, p.296.

[379] A. Decocq, *op. cit.*, : « *Mais s'il est évident que l'individu qui a remis volontairement une chose qui lui appartient à autrui, ou a laissé autrui appréhender cette chose, n'est pas la victime d'un vol, ou qu'une femme qui a consenti à avoir des relations intimes avec un homme n'a point été violée, il est inexact de parler en pareilles hypothèses de fait justificatif.* »

[380] X. Pin, « *Le consentement à la lésion de soi-même. Vers la reconnaissance d'un fait justificatif* », *op. cit.*

[381] B. Bouloc, *op. cit.*, p.381.

causes qui suppriment le caractère pénal de l'acte[382], considérées par certains auteurs comme des causes subjectives de non-responsabilité[383] ou de non-imputabilité.

129. L'infraction d'atteinte à la vie privée, controverses roumaines. La confusion peut être amplifiée si l'on analyse les dispositions de l'article 22 du Code pénal par rapport à l'article 226, paragraphe 4, lettre b) – ne constitue pas une infraction l'acte prévu au paragraphe 1 (photographier, capturer, enregistrer) et du paragraphe 2 (divulguer, diffuser, présenter ou transmettre) – « si la personne lésée a agi explicitement dans l'intention d'être vue ou entendue par l'auteur ». En pratique, nous sommes face à une attitude qui peut se traduire par une approbation tacite du comportement de l'auteur, une présomption de consentement[384], ce qui équivaut à l'absence d'un élément constitutif de l'infraction, l'atteinte à la vie privée n'étant pas commise « sans droit ».

Dans cette situation, nous pourrions théoriquement discuter du consentement à la fois comme « condition essentielle »[385] de l'existence de l'infraction et du point de vue des causes justificatives prévues à l'article 22. Comme elle ne relève d'aucune des causes justificatives mentionnées au Titre II, Chapitre II, du Code pénal – légitime défense, état de nécessité, exercice d'un droit ou accomplissement d'une obligation et consentement de la victime –, nous pouvons comprendre les raisons pour lesquelles les auteurs mentionnés ont utilisé des termes différents pour caractériser les causes justificatives qui concernent spécifiquement le délit d'atteinte à la vie privée.

130. Le consentement présumé n'est pas une cause justificative. En conclusion, le consentement présumé de la victime tel que prévu à l'article 226, paragraphe 4, point b), considéré à tort comme une cause justificative spéciale[386], ne peut faire l'objet d'une analyse

---

[382] « *Il ne faut donc pas les confondre avec les causes de non-imputabilité, de non-responsabilité ou d'absence de culpabilité (erreur, contrainte, maladie mentale, minorité), qui font subjectivement disparaître la culpabilité ou la responsabilité de l'auteur en laissant objectivement subsister l'infraction. L'effet justificatif est donc très important.* », M.-L. Rassat, *op. cit.*, p.80.

[383] L'expression « *cause subjective de non-responsabilité* » appartient à B. Bouloc, *op. cit.*, p.412. L'auteur montre que l'article 64 de l'ancien Code pénal prévoyait deux causes d'irresponsabilité : l'aliénation mentale et la contrainte. Sans être clairement prévue par la loi, la troisième cause est l'erreur. Ces trois causes ont été conservées dans le nouveau Code, « *qu'il a cependant élargies notamment en substituant le trouble psychique à la démence*.»

[384] M. Udroiu*, op. cit.*, p.375.

[385] G. Antoniu, T. Toader (coord.), *Explicațiile Noului Cod penal (Explications du nouveau code pénal*), Académie roumaine – Institut de recherche juridique, Éditions Universul Juridic, 2016, p.263 « *La condition essentielle est que toutes ces activités [(...) actions d'interception de données, d'informations ou d'images à l'intérieur d'un logement, de pièces, de dépendances] soient réalisées sans droit, c'est-à-dire sans autorisation, sans le consentement de la personne dont la vie privée est violée.* »

[386] La doctrine analyse sans grande différence toutes les hypothèses qui conduisent à retenir l'absence de typicité de l'infraction de violation de la vie privée, en les désignant toutes de la même manière, avec des différences d'un auteur à l'autre. De toute évidence, la confusion trouve son origine dans la formulation du législateur concernant le consentement présumé de l'article 226, paragraphe 4, point b), mais je signale en même temps une différence majeure par rapport aux autres hypothèses (justification d'un intérêt légitime, découverte d'une infraction, découverte de faits d'intérêt public). J'estime que l'hypothèse relative au consentement de la victime devrait être analysée séparément des autres, qu'elle ne constitue pas en soi une cause justificative particulière (même si elle semble la plus appropriée parmi les appellations de la doctrine), mais qu'elle est un élément caractéristique de

simultanée avec le même consentement que l'on retrouve dans les causes justificatives prévues à l'article 22 du Code pénal. Il s'agit uniquement d'un élément qui retient l'absence de typicité[387] et non d'une cause justificative. Quoi qu'il en soit, la disposition de l'article 226, paragraphe 4, lettre b – relative au consentement de la victime – semble être davantage une répétition de ce qui ressort clairement de la définition de l'infraction à l'article 226, paragraphes 1 et 2.

E. Consentement dans le cas d'un acte médical

131. Analyse particulière : la nécessité du consentement pour l'acte médical. En ce qui concerne le fonctionnement du consentement, l'activité médicale semble être le meilleur exemple : le chirurgien qui ampute une jambe ou procède à l'excision d'un rein porte atteinte à l'intégrité physique du patient et n'est pourtant pas puni, qu'il ait obtenu ou non le consentement préalable de celui-ci[388]. Ce n'est pas l'absence de consentement de la victime qui élimine la répression pénale, mais le fait justificatif généré par l'autorisation légale de cette activité[389], art. 122-4 du Code pénal[390].

132. Dilemmes concernant le consentement en chirurgie esthétique. Si dans cette situation les choses sont assez claires[391], dans le cas de la chirurgie esthétique, elles semblent un peu plus compliquées car la nature de l'intervention chirurgicale a une importance juridique significative : son objectif est-il de corriger des traits physiques que le patient souhaite embellir ou de reconstruire un visage détruit dans un accident du travail ? En pratique, tout ce qui compte, c'est de savoir si l'objectif est l'embellissement ou la guérison. Dans le premier cas, l'absence de consentement entraîne une éventuelle responsabilité pénale pour coups et blessures volontaires, tandis que dans le second cas, le consentement constitue un fait justificatif[392]. Dans l'une ou l'autre de ces deux situations, lors d'une éventuelle analyse de la responsabilité pénale : « les atteintes à l'intégrité physique d'autrui à la suite d'interventions chirurgicales ne sont justifiées que si ces dernières ont été effectuées selon les règles de l'art chirurgical et de la

l'infraction qui complète l'article 226, paragraphe 1, et doit être analysée conjointement avec celui-ci, comme un tronc commun.

[387] T. Toader, M.I. Michinici *et al.*, *op. cit.*, p.62.

[388] C. Mascala, « *Consentement de la victime* », in JurisClasseur Pénal Code.

[389] V. Ph. Salvage, « *Le consentement en droit pénal* », in RSC, 699 s., spéc. nº 14, 1991.p.708.

[390] *Code pénal*, art. 122-4, version en vigueur depuis le 1er mars 1994 - « n'est pas pénalement responsable la personne qui accomplit un acte prescrit ou autorisé par des dispositions législatives ou réglementaires. »

[391] X.Pin, *Droit pénal général*, 17e éd., Paris, Dalloz, « Cours – Série Droit privé », 2025, p.300.

[392] B. Bouloc, *Droit pénal* général, p.411.

déontologie médicale (absence de faute professionnelle) »[393]. Si le médecin a fait preuve de négligence ou d'ignorance professionnelle, il est pénalement responsable[394].

F. Situation particulière : consentement vs circonstance aggravante

133. Débat : l'absence de consentement, une circonstance aggravante ? La difficulté de délimiter la nature juridique du consentement de la victime apparaît comme un sujet de débat. La question essentielle consiste à déterminer si l'absence de consentement doit être considérée comme un élément constitutif de l'infraction, indispensable à son existence, ou si, au contraire, certaines situations qui révèlent l'absence de consentement - la vulnérabilité de la victime, le rapport d'autorité, la violence ou la menace - doivent plutôt être considérées comme des circonstances aggravantes accompagnant l'infraction de base[395]. Si, dans le cas d'un viol, « l'absence de consentement doit être caractérisée par la circonstance que l'acte a été réalisé par violence, contrainte, menace ou surprise »[396], dans le cas d'une atteinte à la vie privée, l'absence de consentement peut être prouvée, par exemple, par le fait d'empêcher l'auteur de prendre une photo ou de réaliser un enregistrement (on peut voir sur l'image le geste de désapprobation)[397].

134. Élément clé : la qualité de la victime ou de l'auteur. La doctrine majoritaire[398] plaide en faveur du maintien d'une distinction claire : l'élément constitutif vise l'absence de consentement en tant que fait, tandis que la circonstance aggravante reflète une qualité de la victime ou de l'auteur ou un mode de commission, ce qui justifie l'aggravation de la sanction. Dans le cas du délit d'atteinte à la vie privée, « l'absence d'adhésion de la victime au comportement de l'auteur »[399] est un fait subjectif qui dépend uniquement de la capacité d'analyse d'un éventuel danger perçu par la victime.

---

[393] *Ibidem*.
[394] C. Mascala, *op. cit.*
[395] C. De Jacobet, De Nombel, *Théorie générale des circonstances aggravantes*, vol. 55, Nouvelle Bibliothèque de Thèses, préf. Ph. CONTE, Dalloz, Paris, 2006, p.174-175.
[396] P. Conte, S. Fournier & J. Larguier, *Droit pénal spécial*, 16e éd., coll. « Mémentos – Droit privé », Dalloz, Paris, 2024, p.231.
[397] M. Véron, *Droit pénal spécial*, 17e éd., coll. « Sirey université », Sirey, Paris, 14 août 2019, p.237: « En outre, l'article 226-1 établit une présomption de consentement lorsque les actes ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés alors qu'ils étaient en mesure de le faire : photos prises au cours d'une réunion privée, enregistrement des conversations par magnétophone posé sur une table. »
[398] P. Conte, S. Fournier & J. Larguier, *op. cit.* ; V. Malabat, « *Appréciation in abstracto et in concreto en droit pénal* », thèse Bordeaux IV, 1999; M. Dalloz, « *Les circonstances aggravantes légales en droit criminel français thèse* », Nice, 2001.
[399] C. De Jacobet, De Nombel, *op. cit.*, p.176.

G. La valeur du consentement dans l'espace numérique. Protection renforcée pour les mineurs

135. Dans l'interaction avec l'espace numérique, le silence signifie le refus. Si, dans le cadre du délit d'atteinte à la vie privée, le silence est considéré comme un consentement implicite, il en va autrement dans le cadre de la navigation sur Internet : « le silence de l'internaute vaut non plus acceptation mais refus et la poursuite de la navigation ne signifie pas consentement »[400]. Le consentement en matière d'algorithmes et d'intelligence artificielle est, en théorie, au cœur de ce nouvel univers numérique, car les données ne pourraient être collectées sans l'accord de l'utilisateur de la technologie[401]. À titre d'exemple, la CJUE a établi que, lors de la navigation sur Internet, une case pré-cochée ne remplit pas les conditions du consentement, car celui-ci doit être explicite et actif, et non implicite par inaction[402].

136. Protection de la vie privée des mineurs sur les réseaux sociaux. La question de la protection de la vie privée des mineurs sur Internet est également intéressante[403]. Une loi de février 2024[404] modifiant le Code civil a introduit la notion de vie privée dans la définition de l'autorité parentale, et « il s'agit de consacrer de manière expresse l'obligation des parents de veiller au respect de la vie privée de leur enfant, y compris son droit à l'image »[405]. Si les parents diffusent l'image de leur enfant sur les réseaux sociaux et portent gravement atteinte à sa dignité et à son intégrité morale, il y aura une délégation forcée de l'autorité parentale[406].

137. Le juge peut exclure les photos du mineur des réseaux sociaux. Une autre nouveauté est que le juge aux affaires familiales peut « en cas de désaccord entre les parents sur l'exercice du droit à l'image de l'enfant, interdire à l'un des parents de diffuser tout contenu relatif à l'enfant sans l'autorisation de l'autre parent »[407].

---

[400] J.-P. Pierron, (2021), « *Le chemin trouble du consentement. Du consentement formel au consentement existentiel* », in Les Cahiers de la Justice, 4(4), p.563-572.
[401] M. L. Jones et J. Lee, « *Comparing Consent to Cookies: A Case for Protecting Non-Use* », in Cornell International Law Journal, vol. 53, 2020, p.97-132.
[402] CJUE, arrêt de la Cour (Grande Chambre), *Planet49* (affaire C-673/17), 1er octobre 2019, « Renvoi préjudiciel – Directive 95/46/CE, Directive 2002/58/CE, Règlement (UE) 2016/679 – Cookies – Notion de consentement », *EUR-Lex*.
[403] A. Lepage, « *Droits de la personnalité – De certains droits de la personnalité en particulier* », in Répertoire de droit civil, LexisNexis, juill. 2022 (actualisation : mars 2024).
[404] *Loi n° 2024-120 du 19 février 2024 visant à garantir le respect du droit à l'image des enfants*, JORF, n° 39, texte n° 14, 20 février 2024.
[405] J.-Ch. Saint-Pau, *op. cit.*, V° Vie privée, fasc. 20.
[406] A. Gouttenoire, « *Autorité parentale – Délégation de l'exercice de l'autorité parentale* », in Répertoire de droit civil, Juillet 2024 (actualisation : mars 2025).
[407] J. Rochfeld, « *Données à caractère personnel – Données des mineurs* », in Répertoire IP/IT et Communication, LexisNexis, janv. 2025, comm. sous C. civ., art. 371-1 et 373-2-6.

D'autre part, certaines voix critiques[408] soutiennent qu'il faudrait une réglementation beaucoup plus stricte concernant l'attitude des parents qui exposent constamment[409] leurs enfants sur les réseaux sociaux (*sharenting*[410]) ou qui bloquent la pratique fréquente des parents consistant à faire des farces à leurs enfants et à les diffuser en ligne, appelée *kids pranks*[411].

138. Un enfant sur les réseaux sociaux est un mineur potentiellement en danger. L'adoption de la loi sur le droit à l'image des enfants s'inscrit dans le cadre d'un processus plus large de réglementation de l'espace virtuel français, qui a débuté avec la loi établissant que l'utilisateur des réseaux sociaux devient majeur à l'âge de 15 ans[412] et s'est poursuivi avec la loi sur la sécurisation et la régulation de l'espace virtuel[413]. Cette dernière loi vise à surveiller l'environnement en ligne afin de supprimer et de bloquer les contenus illégaux[414]. À l'heure actuelle, le droit pénal français tend de plus en plus à considérer qu'un enfant présent dans l'environnement virtuel est en réalité un mineur en danger potentiel[415].

---

[408] M. Saulier, « *Garantir le respect du droit à l'image des enfants : un objectif ambitieux, une efficacité douteuse ?* », in AJ famille 2024. p.116.

[409] A. Brosch, *Sharenting – Why Do Parents Violate Their Children's Privacy?,* in The New Educational Review, 2018, vol. 54, p.78.

[410] Le terme *sharenting* désigne la pratique consistant pour les parents à publier sur les réseaux sociaux ou d'autres plateformes numériques des photos, des données personnelles ou des fragments de la vie de leurs enfants, sans que ceux-ci aient la possibilité de donner leur consentement réel. Ce phénomène, qui se situe à la croisée de la liberté d'expression des parents et du droit de l'enfant à la vie privée, génère des risques spécifiques liés à une exposition précoce : perte de contrôle sur l'image, utilisation abusive des données et formation d'une identité numérique imposée. D'un point de vue juridique, le *sharenting* soulève des questions liées à l'exercice de l'autorité parentale, au respect de l'intérêt supérieur de l'enfant et aux limites du droit à la vie privée à l'ère numérique.

[411] Le terme *kids pranks* désigne la pratique consistant à diffuser en ligne des farces mettant en scène des enfants, généralement sur des plateformes vidéo. Bien que présentées comme des formes de divertissement familial, elles peuvent porter atteinte au droit à la dignité et à la vie privée du mineur, en l'exposant au ridicule et à l'exploitation numérique. Ce phénomène doit être replacé dans le cadre plus large de la protection de l'enfance dans l'espace numérique, en remettant en question à la fois la responsabilité des parents et les obligations des plateformes en matière de prévention des contenus préjudiciables.

[412] M. Saulier a commenté cette loi : « *Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne* », AJ famille 2023, p. 420: « Les raisons de l'adoption de la loi n° 2023-566 du 7 juill. 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne (JO du 8) se trouvent à la croisée de la protection de l'enfance et de la santé publique : les adolescents (15 %), mais surtout les adolescentes (50 %), utilisateur(rices) régulier(e)s des réseaux sociaux (plus de 50 % des 10-14 ans sont au moins présents sur un réseau, la 1re inscription ayant lieu en moyenne à 8,5 ans) souffrent d'importants problèmes de santé mentale (dépression, rapport au corps problématique, insatisfaction) et sont les victimes fréquentes de cyberharcèlement (« *Social media use and adolescent mental health : findings from the UK Millenium Cohort Study* », in The Lancet, 2019; CNIL, *Droits numériques des mineurs*, Consultation publique, janv. 2021). »

[413] *Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique*, JO, 22 mai 2024.

[414] A.-S. Chavent-Leclère, « *Loi n° 2024-449 du 21 mai 2024 sur l'espace numérique : durcissement des mesures de retrait et de blocage des contenus illicites en ligne », Procédures*, n° 1, janv. 2025 ; M. Le Roy, « *Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique : analyse des articles visant à protéger les personnes physiques* », in Communication – Commerce électronique 2025, n° 2, p.3.

[415] M. Saulier, « *Garantir le respect du droit à l'image des enfants : un objectif ambitieux, une efficacité douteuse* ? », in AJ famille 2024, p.116.

§2.« LIEU PRIVÉ » DANS L'ARCHITECTURE DU DROIT À LA VIE PRIVÉE. AMBIGUÏTÉS DANS LA DÉFINITION

139. Difficultés à définir le lieu privé. Une autre perspective pertinente pour la présente recherche doctorale est la définition, voire les controverses liées à l'expression « lieu privé », composante essentielle de l'adaptation des mécanismes de protection de la vie privée.

Nous sommes à deux doigts du lancement à grande échelle de l'ordinateur quantique[416], Interpol a ouvert un bureau d'enquête dans le Metavers[417], les algorithmes influencent notre autonomie cognitive, la formation de notre opinion et notre prise de décision[418], les aéroports nous identifient sans documents, uniquement sur la base de données biométriques[419], tous les pays membres de l'UE ont déjà signé le premier traité international sur la réglementation de l'Intelligence Artificielle[420], les appareils électroménagers de dernière génération surveillent

[416] M. Swayne, « *Quantum Leaders Tell FT: Quantum Computing Race Enters Final Stretch, But Scaling Challenges Still Loom* », in The Quantum Insider, 2025, disponible sur - https://thequantuminsider.com/2025/08/12/quantum-leaders-tell-ft-quantum-computing-race-enters-final-stretch-but-scaling-challenges-still-loom/

[417] Pour plus de détails à ce sujet, voir le chapitre « *La vie privée dans le métaverse* ».

[418] Comité des Ministres du Conseil de l'Europe, Déclaration sur les capacités manipulatrices des processus algorithmiques, adoptée le 13 février 2019. À ce moment-là, les 47 États signataires de la déclaration (la Russie a été exclue du Conseil de l'Europe après le début de la guerre en Ukraine) ont exprimé leur profonde inquiétude quant au fait que la vie privée des citoyens est menacée par l'utilisation des technologies numériques avancées et que les utilisateurs de ces technologies risquent de ne plus être capables de prendre des décisions par eux-mêmes sans l'aide de systèmes automatisés. Cette déclaration tire également la sonnette d'alarme quant à la perte de la capacité à se forger une opinion et à changer de comportement social et politique. Cet organisme international demande une intervention urgente du droit : « la nécessité de cadres de protection supplémentaires en matière de données, qui dépassent les notions actuelles de protection des données à caractère personnel et de la vie privée et abordent l'impact significatif de l'utilisation spécifique des données sur les sociétés et sur l'exercice des droits de l'homme au sens large ».

[419] Des détails à ce sujet peuvent être trouvés dans la section « technologies biométriques de reconnaissance et d'authentification » du sommaire de la thèse.

[420] Conseil de l'Europe, Convention-cadre sur l'intelligence artificielle, les droits de l'homme, la démocratie et l'État de droit (CETS n° 225), adoptée par le Comité des ministres le 17 mai 2024 et ouverte à la signature à Vilnius le 5 septembre 2024. Il s'agit du premier instrument juridique international contraignant visant à garantir que la conception, le développement et l'utilisation de l'intelligence artificielle respectent les normes en matière de droits fondamentaux. Le texte prévoit expressément la nécessité de protéger la vie privée et les données à caractère personnel, dans le cadre du respect de la dignité humaine et de l'autonomie individuelle. L'importance de cette convention est majeure, car elle établit un précédent normatif au niveau mondial, offrant un cadre réglementaire avant d'autres puissances telles que les États-Unis. Grâce à cette initiative, l'Europe affirme son rôle de leader mondial dans la définition des règles éthiques et juridiques applicables aux algorithmes et aux technologies émergentes.

même notre rythme cardiaque, notre sommeil ou notre glycémie[421], et pourtant, le droit pénal a encore de sérieuses difficultés à définir la notion de « lieu privé »[422].

140. La jurisprudence impliquée dans la définition du « lieu privé ». Bien que cela semble simple, « d'une manière générale, est privé tout lieu qui, par nature, n'est pas public »[423], la définition même du terme a été largement élaborée par la jurisprudence, étant donné que la formulation de l'article 226-1 et suivants laisse place à des interprétations. En France, la jurisprudence relative à l'atteinte à la vie privée est vaste[424] et comporte des interprétations assez diverses du « lieu privé ».

A. Termes clés du Code pénal français : à titre privé ou confidentiel et « lieu privé ».

141. Différences entre les deux codes. Même si le droit pénal roumain et le droit pénal français tentent, par le biais de l'infraction d'atteinte à la vie privée, de bloquer le même type de comportement et de protéger les mêmes valeurs humaines, les différences sont significatives en ce qui concerne la détermination de la nature du lieu où l'espionnage visuel ou auditif est effectué. Dans le code français, on trouve des différences dans la terminologie utilisée pour décrire la nature du lieu où sont commis les deux types d'espionnage : (1) l'enregistrement d'une conversation est puni quel que soit le lieu où elle a lieu si cette conversation est de nature privée ou confidentielle[425] (2) l'enregistrement de l'image d'une personne « se trouvant dans un lieu privé » est puni. Pour plus de clarté, les termes clés sont « à titre privé ou confidentiel » pour l'enregistrement d'une conversation et « lieu privé » pour la prise de vue[426].

---

[421] « *Les objets connectés semblent anodins et s'intègrent facilement dans la vie quotidienne mais les données qu'ils traitent ne sont pas anodines. Il faut être vigilant sur la manière de partager et de donner des accès à ces données* », c'est l'un des nombreux messages que l'on trouve sur le site Internet de la CNIL. À cette occasion, la CNIL conseille aux utilisateurs d'« objets intelligents » dans leur logement de saisir de fausses données lorsqu'ils se connectent à ceux-ci, afin de protéger leur vie privée (par exemple, si la connexion au réfrigérateur, à la machine à laver ou à la télévision nécessite la saisie de la date de naissance, du nom, de l'adresse e-mail, la CNIL recommande d'entrer une fausse date, un pseudonyme et une adresse e-mail différente pour chaque objet).

[422] « Si l'exigence d'un *lieu privé* n'est donc pas contestable, il reste que la définition de cette notion est délicate », J.-Ch. Saint-Pau, « *Jouissance des droits civils. – Droit au respect de la vie* privée. – Régime. Actions », *op. cit.*

[423] *Ibidem*.

[424] M. Véron, *Droit pénal spécial*, 17e éd., Sirey, collection Sirey université, Paris, 2019, p.236 : « une abondante jurisprudence est conduite à apprécier le caractère public ou privé du lieu où l'image d'une personne a été fixée ou enregistrée. »

[425] M.-L. Rassat, *Droit pénal spécial*, 9e éd., Dalloz, Paris, 2024, p.584 : « La loi ancienne ne punissait que la captation des conversations tenues dans un lieu privé. Cette notion disparaît, pour l'espionnage auditif, en sorte que tous les propos privés et confidentiels sont couverts, même s'ils sont échangés dans un lieu public, ce qui pourra donner lieu à des difficultés de preuve. »

[426] P. Conte, S. Fournier & J. Larguier, *Droit pénal spécial*, 16e éd., coll. "Mémentos – Droit privé", Dalloz, Paris, 2024, p.231.

142. Le lieu de l'intrusion, un aspect essentiel pour l'intervention du droit pénal. Cette distinction très claire faite par le législateur français est utile pour comprendre les limites de la protection offerte aux victimes potentielles, plus précisément, quelle est la surface couverte par le droit pénal et quelle est celle couverte par le droit civil. Le lieu où les actes d'intrusion[427] ont été commis, ainsi que le consentement de la victime, l'intention et le but de l'auteur, les moyens et les méthodes utilisés par celui-ci sont essentiels dans cette analyse de l'opportunité d'une intervention du droit pénal. Dans de nombreux cas, la pratique judiciaire a souligné la nécessité d'un examen nuancé des circonstances dans lesquelles l'acte illicite a été commis.

143. Atteinte à la vie privée, entre droit civil et droit pénal. L'une des principales difficultés dans l'analyse du délit d'atteinte à la vie privée et des délits qui y sont étroitement liés ne réside pas dans l'intrusion ou la violation de la vie privée en soi, « mais l'usage de moyens incriminés pour y porter atteinte, en particulier l'usage de procédé permettant de capter ou de fixer la voix ou l'image d'une personne sans son consentement »[428]. Ainsi, l'adoption d'un comportement incriminé par les articles 226-1 à 226-7 du Code pénal, qui porte atteinte à la vie privée d'une autre personne, relève naturellement du droit civil, conformément à l'article 9 du Code civil[429].

144. Innovation : atteinte à la vie privée quel que soit le lieu où se trouve la victime. Une loi de 2020 relative à la protection des victimes de violence domestique[430] a introduit une incrimination innovante : l'atteinte à la vie privée par la capture, l'enregistrement et la transmission de la localisation d'une personne, en temps réel ou a posteriori, sans son consentement et sans que cette localisation soit confidentielle. La particularité de cette infraction réside dans le fait qu'elle s'applique quel que soit le lieu où se trouve la victime, privé ou public, l'accent étant mis sur l'atteinte à la liberté de mouvement[431], « peu important qu'elle n'ait par exemple effectué que des déplacements ordinaires et tout à fait connus »[432]. Concrètement, la modification de cette dualité classique concernant l'intimité d'une personne (la voix et l'image) élargit considérablement les limites d'application de l'infraction, qui ne punit plus seulement la capture ou la diffusion de données intimes, mais également les données relatives à la localisation d'une personne[433].

---

[427] P. Bonfils et L. Grégoire, *Droit pénal spécial*, Paris, Lextenso, janv. 2022.
[428] B. Perrier, « *Faits justificatifs – Lanceur d'alerte* », in JurisClasseur Pénal Code, art. 122-9, fasc. 20, LexisNexis, 1re publ. 3 janv. 2024.
[429] J.-B. Perrier, *op. cit.*
[430] Loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales, Journal officiel n° 0187, 31 juillet 2020.
[431] M.-L. Rassat, *op. cit.*, p.587.
[432] V. Malabat, *Droit pénal spécial*, 10e éd., Dalloz, collection HyperCours, Paris, 20 octobre 2022, p.442.
[433] V. Malabat, *op. cit.*, p. 442.

B. Analyse conceptuelle : le véhicule est un « lieu privé ou public ». Vision différente

145. Différence essentielle entre le droit pénal roumain et le droit pénal français. Un exemple représentatif permettant de souligner les différences conceptuelles entre le droit pénal roumain et le droit pénal français en matière de « lieu privé » peut être proposé à travers l'analyse de l'arrêt rendu le 28 mars 2023 par la Cour de cassation[434]. L'accusation portait sur le fait qu'un agent de police municipale avait arrêté un conducteur et l'avait filmé alors qu'il était au volant. En première instance, le 1er mars 2022, la cour d'appel d'Aix-en-Provence a condamné le policier à quatre mois d'emprisonnement avec sursis, 500 euros d'amende et l'interdiction définitive d'exercer sa profession pour avoir commis l'infraction prévue à l'article 226-1. Le tribunal a estimé que le conducteur, qui se trouvait dans l'habitacle de sa voiture, c'est-à-dire dans un lieu privé, n'avait pas donné son accord pour être filmé par le policier, même s'il l'avait vu réaliser le film et ne s'y était pas opposé. Le juge a estimé que le conducteur n'aurait pas pu s'opposer à être filmé car le policier bénéficiait de l'autorité de sa fonction, et que le consentement ne pouvait donc être présumé[435]. Le prévenu a interjeté appel et la cour d'appel a annulé la décision de première instance et renvoyé l'affaire pour réexamen au motif que la charge de la preuve du consentement présumé incombait au procureur et non au prévenu[436]. Le commentaire du professeur Philippe Conte[437] sur la décision de la Cour de cassation est catégorique : « pareille solution est exacte. (...) Lorsque l'image d'un individu en garde à vue ou, comme ici, soumis à un contrôle d'identité est fixée « au vu et au su » de celui-ci, la présomption de consentement à cette fixation devrait opérer dès l'instant qu'il ne s'y oppose pas ».

146. Filmer un conducteur dans sa voiture n'est pas un délit en Roumanie. En droit pénal roumain, une telle discussion ne pourrait avoir lieu que si la voiture dans laquelle le conducteur était filmé était en réalité le « domicile » de la victime. Plus précisément, si les caractéristiques du véhicule avaient permis de conclure que son objectif était d'y habiter, même temporairement,

---

[434] Cour de cassation, chambre criminelle, arrêt du 28 mars 2023, no 22-83.069.

[435] Cour d'Appel Aix-en-Provence (§ 8): «*si la fixation de l'image du conducteur dans l'habitacle de son véhicule, lieu privé, a été accomplie au vu et au su de celui-ci, sans qu'il soit établi qu'il s'y est opposé, le consentement de l'intéressé ne saurait être présumé, dès lors qu'il n'était pas en mesure de s'opposer à être filmé et enregistré dans les circonstances d'un contrôle d'identité opéré par des policiers municipaux qui lui reprochaient plusieurs infractions routières.*»

[436] Cass. crim., 28 mars 2023, n° 22-83.069 (§ 11): «*Il appartenait à la cour d'appel de rechercher ensuite, dans les éléments de la procédure, ceux qui pouvaient être de nature à emporter sa conviction que le conducteur était opposé à être filmé, la charge de cette preuve ne pesant pas, contrairement à celle relative à l'admission de la présomption légale, sur le prévenu, mais sur le ministère public*.»

[437] Ph. Conte, « *Atteinte à l'intimité de la vie privée – Absence de consentement à la fixation de l'image* », Droit pénal, n° 7-8, juill.-août 2023, comm. 115, note ss Cass. crim., 28 mars 2023, n° 22-83.069.

alors, en théorie, le policier aurait pu faire l'objet d'une enquête pénale pour atteinte à la vie privée. En droit pénal roumain, l'habitacle d'un véhicule circulant sur la voie publique n'est pas assimilé au terme « domicile », comme l'exige l'article 226 du Code pénal. La question pourrait rester ouverte pour les véhicules de type caravane ou les camions qui sont également utilisés comme « domicile ».

Section 7
ENTRE LA RECONNAISSANCE DE LA PERSONNALITÉ JURIDIQUE ET LA RÉDACTION DU DROIT. LES LIMITES DE LA RECHERCHE

147. L'abstraction de l'être. Dans le contexte de la révolution numérique à laquelle nous assistons aujourd'hui[438], la doctrine identifie une « abstraction sélective en ce qui concerne la personnalité de l'être » et « une oscillation entre la personne et la chose en ce qui concerne le corps de l'être »[439]. La définition trinitaire donnée par Edgard Morin de « l'humain » – « ne peut pas dire que l'humain est à 33 % individu, à 33 % société, à 33 % biologie. Ce qu'on peut dire, c'est que l'humain est à 100 % individu, à 100 % social et à 100 % biologie »[440] semble ne plus être d'actualité en cette ère dominée par les algorithmes.

§1. LES ALGORITHMES DONNENT L'IMPRESSION D'AVOIR LEUR PROPRE IDENTITÉ

148. Apparence d'autonomie. Le système binaire de calcul est capable de créer des algorithmes qui imitent le comportement humain[441], peuvent pleurer à certains stimuli prédéfinis, manifester des réactions de joie ou de tristesse[442], reproduire des modèles linguistiques complexes ou anticiper des décisions.

En accumulant ces fonctionnalités, les algorithmes finissent par donner l'impression qu'ils possèdent leur propre identité, distincte de celle de leurs créateurs. Cette apparence

[438] B. Barraud, «*Le droit en datas : comment l'intelligence artificielle redessine le monde juridique*», in Revue Lamy Droit de l'Immatériel, nov. 2019, nº 164.
[439] Voit le commentaire fait par Catherine Puigelier sur la thèse de doctorat publiée par Nicolas Anciaux, *Essai sur l'être en droit privé*, thèse de droit privé, dir. Bernard Teyssié, Université Panthéon-Assas (Paris II), 2018, 607 p, in *RTD* civ. 2019, n° p.447.
[440] E. Morin, *Penser global. L'humain et son univers*, Paris, Robert Laffont, 2015, p.12.
[441] J. Martinez-Miranda et A. Aldea, « *Emotions in human and artificial intelligence* », in Computers in Human Behavior, vol. 21, 2005, p.323-341.
[442] M. Minsky, *The Emotion Machine. Commonsense Thinking, Artificial Intelligence, and the Future of the* Human Mind, New York, Simon & Schuster, 2007, p.66-68.

d'autonomie et de personnalité soulève des difficultés conceptuelles et juridiques majeures : si l'algorithme ou les systèmes d'intelligence artificielle « semblent » avoir une identité, comment réglementer la responsabilité de leurs actions et quelles garanties doivent être accordées à l'individu dont la vie privée est affectée par l'interaction avec ces systèmes[443] ? Le droit a apporté certaines réponses, mais cela ne semble être que le début de réponses plus claires et plus fermes.

149. « Le phénomène criminel est le « produit » de l'homme » est une affirmation qui appartient à Bernard Bouloc[444] et semble difficile à contester, si l'on admet que l'*homo numericus* n'est que le résultat de l'évolution technologique réalisée par l'*homo sapiens*. À propos des procès dont les acteurs sont des entités non humaines, l'auteur s'exprime de manière assez sévère : « Les procès intentés aux animaux, aux choses et même aux cadavres ne sont plus de nos jours « qu'une curiosité historique ». Seul un être humain doué d'intelligence et de volonté peut commettre un acte contraire à l'ordre social, dont la société soit en droit de lui demander des comptes »[445].

A. La voie est-elle ouverte à la reconnaissance de la personnalité juridique pour l'intelligence artificielle ?

Controverse : accepter la responsabilité pénale pour les algorithmes ? Ce type de raisonnement, que l'on retrouve également chez d'autres auteurs[446], annule complètement les théories récentes qui évoquent une acceptation timide de la responsabilité pénale de

[443] W. Barfield (éditeur), *The Cambridge Handbook of the Law of Algorithms*, Cambridge University Press, 2021.
[444] B. Bouloc, *Droit pénal général*, 29e éd., Paris, Dalloz, coll. Précis, 2025, p.10 : « *C'est qu'en effet le phénomène criminel est le « produit » de l'homme. Ni les choses ni les animaux – encore que par leur fait ils portent quelquefois atteinte à la sécurité publique et provoquent un trouble social – ne sont des agents du phénomène criminel*».
[445] B. Bouloc, *op. cit.*, p.11.
[446] « *En tant que réalité humaine, le crime est un acte humain, procédant d'un être doué d'intelligence et de volonté. Il importe donc de découvrir les causes de ce crime dans la personne de son auteur, c'est-à-dire dans son individualité physique et aussi dans son environnement social* », soutenait en 1991 Ph. Jeandidier, *Droit pénal général*, Montchrestien, coll. « Domat droit public » p 25 – sans rien prévoir sur ce que suivrait concernant l'évolution de l'intelligence artificielle.

l'intelligence artificielle[447][448] et soutient implicitement celles qui affirment qu'une telle discussion est prématurée[449], voire « monstrueuse »[450].

150. Argumentation similaire à celle utilisée lors de la naissance de la personne morale. Si l'on analyse strictement la notion de personne morale telle qu'elle apparaît dans la doctrine – « le droit appréhende donc la notion de personne de manière très abstraite comme une entité appelée à jouer un rôle sur la scène du monde juridique »[451], ceux qui soutiennent la transformation de l'intelligence artificielle en sujet de droit peuvent avoir des arguments apparemment sérieux. De plus, le terme « personne » désignait dans la Rome antique le masque de théâtre, et les juristes utilisaient ce mot pour désigner le « visage juridique de l'homme correspondant en quelque sorte à son statut »[452]. Concrètement, si nous acceptons que la « personne » n'est qu'un masque et que nous complétons l'argumentation par les débats qui ont été à l'origine de la genèse de la personne morale – « ne serait qu'une pure abstraction de l'esprit à défaut de toute consistance matérielle ou biologique »[453], il semble qu'il n'y ait plus qu'un petit pas à franchir avant d'accorder ce statut aux algorithmes et à l'intelligence artificielle.

151. Frankenstein invoqué dans une résolution du Parlement européen. Quoi qu'il en soit, cette question juridique a fait son apparition sur la scène publique lorsque, le 16 février 2017, le Parlement européen a adopté une résolution[454] visant à réglementer le statut juridique des robots : « en vertu du cadre juridique actuel, les robots ne peuvent être tenus pour responsables en tant que tels des actions ou omissions causant des dommages à des tiers ». Pour justifier la nécessité sociale d'accorder la personnalité juridique aux systèmes autonomes basés sur des algorithmes, les auteurs de la résolution ont rédigé une introduction faisant référence à la littérature classique : « Du monstre de Frankenstein de Mary Shelley au mythe classique de Pygmalion, en passant par l'histoire du Golem de Prague et jusqu'au robot de Karel Čapek, qui

---

[447] A. Bensoussan, « *Droit des robots : science-fiction ou anticipation* ? », in Recueil Dalloz, n° 28, 2015. p.1640.
[448] D. Rose, « *Faut-il une responsabilité pénale appliquée à l'intelligence artificielle* ? », in Dalloz IP/IT, n° 11, nov. 2024, p.574–577 (dans le dossier *« Pour une intelligence artificielle responsable* ») : «*Les risques que soulève l'intelligence artificielle pour l'ordre public et l'intérêt des individus ne sont pas exclusifs d'une qualification pénale. Toutefois, parce qu'elle est un outil au service de l'homme, envisager une responsabilité pénale personnelle appliquée à cette technologie doit être rejeté au profit d'une responsabilité du fait de l'intelligence artificielle.*»
[449] L. Cluzel-Métayer, *Le droit de l'intelligence artificielle*, 1re éd., Paris, Dalloz, coll. « À savoir », 2025, p.124 : « dès lors qu'il est pour l'heure exclu de conférer la personnalité juridique à l'IA, il revient aux fournisseurs, déployeurs et autres utilisateurs de maîtriser les risques en amont et de réparer les éventuels préjudices que l'utilisation des SIA pourrait causer. »
[450] G. Loiseau, « *La personnalité juridique des robots : une monstruosité juridique* », in La Semaine juridique. Édition générale (JCP G), n° 22, 2018, p. 1039-1042.
[451] J.-Ch. Saint-Pau (dir.), *Droits de la personnalité*, Paris, LexisNexis, coll. « Traités », 2013, p.58.
[452] J.-Ch. Saint-Pau (dir.), *op. cit.,* p.58.
[453] Idem, p.79.
[454] Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL)),A (https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_FR.html)

a inventé le mot, les hommes ont rêvé de la possibilité de construire des machines intelligentes, le plus souvent des androïdes aux traits humains ».

152. Une description dystopique pour définir clairement les robots. S'ensuivit une description digne d'un film hollywoodien dystopique : « alors que l'humanité est à l'aube d'une ère où les robots, les bots, les androïdes et autres manifestations de l'intelligence artificielle (IA) de plus en plus sophistiquées semblent sur le point de déclencher une nouvelle révolution industrielle, qui ne laissera probablement aucune couche de la société intacte ». La même résolution affirmait qu'il était nécessaire de définir clairement les robots[455] et l'intelligence artificielle, « de manière flexible et sans entraver l'innovation ».

153. Révolte contre l'octroi de la personnalité juridique. Ce type d'argumentation a suscité la révolte parmi les experts en intelligence artificielle, en robotique et en droit, plus de 150 d'entre eux ayant rédigé une lettre ouverte[456] dans laquelle ils exprimaient leur désapprobation quant à l'octroi de la personnalité juridique aux robots autonomes, imprévisibles ou basés sur des systèmes d'apprentissage automatique. Sans contrebalancer les opinions de ceux qui ont bloqué ce projet de réglementation européenne, d'autres auteurs[457] ont estimé qu'il ne s'agissait que d'une question de temps avant que l'intelligence artificielle ne devienne un sujet de droit.

§2. L'INTELLIGENCE ARTIFICIELLE, LÉGISLATEUR POTENTIEL ? LES LIMITES DES DÉBATS DOCTRINAUX

154. Connaissance du droit et de ses destinataires. La création du droit dans le contexte actuel ne peut se faire qu'à travers une connaissance et une compréhension aussi claires que possible de son essence et de ses destinataires : « le droit est en soi une science de la connaissance du droit, parce qu'il est fait de son application même. Si l'on préfère, le droit ne préexiste pas à son application, il est intriqué dans ce qu'en font ses destinataires »[458]. En ce qui concerne la connaissance du droit pénal à l'ère numérique, Emmanuel Dreyer fait une remarque

[455] Le terme « robot » a été utilisé pour la première fois en 1920 par l'écrivain tchèque Karel Capek sous la forme « robota », qui signifiait « travail pénible » ou « corvée » – « un androïde capable d'exécuter des travaux à la place de l'homme ». Pour plus de détails sur l'étymologie du mot, voir https://www.cnrtl.fr/etymologie/robot. Même s'il est souvent utilisé en lien étroit avec le terme « intelligence artificielle », la robotique a un champ d'application plus restreint.

[456] La lettre peut encore être signée aujourd'hui (juillet 2025) par les experts qui souhaitent empêcher l'octroi du statut juridique de « personne électronique » aux robots utilisant l'intelligence artificielle, et le nombre de signataires n'a cessé d'augmenter pour atteindre 285. En raison de cette contestation véhémente de la part des experts, le projet a été bloqué et des solutions alternatives sont actuellement recherchées pour réglementer l'intelligence artificielle. La lettre peut être consultée ici : https://robotics-openletter.eu/

[457] A. Bensamoun et G. Loiseau, « *L'intégration de l'intelligence artificielle dans l'ordre juridique en droit commun : questions de temps* », in Dalloz IP/IT, avr. 2017, p.239.

[458] F.Terré, & N.Molfessis, *Introduction générale au droit* (17e éd.) Paris, Dalloz, 2025, p.785.

intéressante : « ce qui gêne ici, c'est la présomption de connaissance du système pénal qui, du fait de son extension, semble de moins en moins vraisemblable »[459].

155. La métamorphose de la création juridique à l'ère numérique. L'importance de cette évolution technique est incontestable pour les juristes français. Par exemple, la dernière édition de l'*Introduction générale au droit*[460] offre une perspective très actuelle sur l'impact de « l'ère *ChatGPT* » sur le droit et soutient que si, dans le passé, la connaissance du droit transmis par la coutume était essentielle à la survie du groupe, il est désormais essentiel d'adapter nos méthodes de compréhension, notamment en fonction de l'évolution de l'intelligence artificielle[461]. Le lancement de ChatGPT en 2022 a constitué un véritable phénomène social, car c'était la première fois que l'intelligence artificielle n'était plus un simple outil destiné uniquement aux spécialistes et aux laboratoires de recherche : « au-delà de l'innovation technique que représente cet outil, ChatGPT a surtout permis au grand public de prendre conscience des potentialités de l'intelligence artificielle et des changements majeurs qu'elle annonce dans l'organisation de nos modes de vie »[462].

A. L'intelligence artificielle risque-t-elle d'écrire elle-même le droit ?

156. L'intelligence artificielle générative. L'une des questions qui mérite une attention particulière à l'ère actuelle concerne l'implication de l'intelligence artificielle générative[463] dans la rédaction du droit et, implicitement, dans la rédaction des normes qui la concernent directement. La création d'une production artistique, littéraire ou même musicale par des systèmes d'intelligence artificielle générative[464] est déjà une réalité[465][466], le débat dans le milieu

---

[459] P. Beauvais, D. Chilstein & E. Dreyer (dir.) (2024) *Le droit pénal de l'avenir, op. cit.* p.4.
[460] F.Terré, & N.Molfessis, *op. cit.*
[461] *Ibidem* p.740: « *L'invention de l'imprimerie autrefois, celle de l'informatique et du numérique à notre époque ont changé l'acte d'apprendre le droit ; elles n'ont pas aboli la nécessité de l'apprendre. L'avènement et les progrès de l'intelligence artificielle pas davantage – ce sont les méthodes qui doivent évoluer*».
[462] A. Latil, « *Droit de l'intelligence artificielle (droit international et droit européen)* », in JurisClasseur Communication*,* Fasc. 988, 24 juill. 2024.
[463] Ce terme apparaît sous cette dénomination dans la législation sur l'intelligence artificielle du Parlement européen, plus précisément dans le document intitulé « Amendements du Parlement européen, adoptés le 14 juin 2023, à la proposition de règlement du Parlement européen et du Conseil établissant des règles harmonisées en matière d'intelligence artificielle (législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union (COM *(2021)0206 – C9-0146/2021 – 2021/0106(COD)* https://www-europarl-europa-eu.docelec.u-bordeaux.fr/doceo/document/TA-9-2023-0236_FR.html
[464] J-M. Bruguière & J-M. Deltorn (2023), *Intelligences artificielles génératives. Y a-t-il exploitation des œuvres, au sens du droit d'auteur ? N'y aurait-il pas d'autres modèles à considérer ?*, in Recueil Dalloz, p.1657-1662.
[465] Un moment important où l'intelligence artificielle a réussi à prouver son « esprit artistique » s'est produit en septembre 2021, lorsque des chercheurs allemands ont annoncé qu'ils avaient utilisé des algorithmes pour terminer avec succès la Symphonie n° 10, que Beethoven avait laissée inachevée à sa mort en 1827. À partir de croquis manuscrits et de fragments incomplets, les algorithmes ont réussi à générer une symphonie appréciée par le public.
[466] Les systèmes d'intelligence artificielle sont déjà utilisés pour restaurer les tableaux de peintres célèbres. Il ne s'agit pas simplement de reproduire des peintures célèbres, mais de remplacer la vision du peintre et de créer des

juridique étant envisagé sous deux angles[467] : si l'utilisation des données collectées précédemment pour la réalisation de la production respecte les droits d'auteur[468] et quel est le régime juridique du « produit fini »[469].

157. L'immatérialité des algorithmes, transformée en « chose ». En ce qui concerne la responsabilité civile, nous constatons déjà une préoccupation sérieuse de la part du droit européen[470] quant à la définition du terme « produit »[471] et à l'acceptation de son immatérialité[472]. À l'heure actuelle, le droit civil national, face aux défis technologiques, utilise les instruments obsolètes[473] de l'institution de la responsabilité civile délictuelle[474], de la définition du terme « chose »[475] et du produit défectueux.

œuvres d'art originales, basées sur les modèles étudiés précédemment. Par exemple, en 2017, après avoir inséré plus de 340 tableaux peints par Rembrandt dans un modèle d'intelligence artificielle, un tableau a été généré que le peintre aurait peint s'il était encore en vie.

[467] A. Zollinger, « *Creations generated by artificial intelligence in literary and artistic property: the new death of the author?* », in Eastern Journal of European Studies, 2024.

[468] Dans son étude, Zollinger analyse d'un point de vue comparatif la législation en matière de droits d'auteur en France et en Roumanie et conclut que les normes juridiques doivent s'adapter à cette évolution de l'intelligence artificielle générative, et que le droit d'auteur reste applicable lorsque la forme originale de la production est identifiée : « *copyright is still applicable when it is possible to establish the existence of an original formal contribution* ».

[469] «*En France règne traditionnellement une conception subjective de l'originalité, définie depuis Desbois, comme l'empreinte de la personnalité de l'auteur. La jurisprudence et la doctrine ont adopté une conception anthropocentrique du droit d'auteur, qui protège le travail créateur de l'être humain. L'œuvre doit dès lors pouvoir être retracée jusqu'à son auteur, qui en est l'origine, qui a laissé en elle des traces de sa personne – même si l'exécution personnelle n'est pas une condition requise pour cela*», explication extraite de A Bensamoun, & J Farchy, (2020). Intelligence artificielle et culture : Rapport final de la mission du Conseil Supérieur de la Propriété Littéraire et Artistique. Paris : CSPLA. Disponible sur : https://www.culture.gouv.fr

[470] Voir *Directive (UE) 2024/2853 du Parlement européen et du Conseil du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil* (Texte présentant de l'intérêt pour l'EEE).

[471] Voir le paragraphe 3 de la *Directive UE 2024/2853* qui justifie la nécessité d'adapter le droit aux nouveaux défis numériques : « *La Directive 85/374/CEE a été un instrument efficace et important, mais il serait nécessaire de la réviser à la lumière des évolutions liées aux nouvelles technologies, notamment l'intelligence artificielle (IA), aux nouveaux modèles commerciaux basés sur l'économie circulaire et aux nouvelles chaînes d'approvisionnement mondiales, qui ont conduit à des incohérences et à une insécurité juridique, en particulier en ce qui concerne la signification du terme "produit"* ».

[472] Voir le paragraphe 13 de la Directive précitée : « *Les produits de l'ère numérique peuvent être matériels ou immatériels. Les logiciels, tels que les systèmes d'exploitation, les micrologiciels, les programmes informatiques, les applications ou les systèmes d'IA, sont de plus en plus répandus sur le marché et jouent un rôle de plus en plus important dans la sécurité des produits. Les logiciels peuvent être mis sur le marché en tant que produits autonomes, puis être intégrés dans d'autres produits en tant que composants, et peuvent causer des dommages lors de leur fonctionnement.* »

[473] A. Vial, *Systèmes d'intelligence artificielle et responsabilité civile : droit positif et proposition de réforme*, thèse de doctorat en droit privé et sciences criminelles, Université Bourgogne Franche-Comté, soutenue à Besançon le 12 décembre 2022, sous la direction de Pascal Kamina, p.75.

[474] Tant l'article 1349 du Code civil roumain que l'article 1240 du Code civil français définissent la responsabilité civile délictuelle de manière similaire : la personne qui cause un préjudice à autrui est tenue de le réparer si les conditions suivantes sont remplies : il existe un fait illicite (une action ou une inaction), il existe un préjudice, un lien de causalité direct entre le fait et le préjudice et une faute (par négligence ou imprudence).

[475] A. Vial, *Systèmes d'intelligence artificielle et responsabilité civile*, th., UBFC, 2022, p.80 : « *La notion de « chose » entendue au sens de l'article 1242 alinéa 1er in fine du code civil vise les biens meubles « corporels, dangereux ou non* ». Or le caractère corporel de ces choses, entendu comme tel par certains auteurs, bien que contesté dans une moindre mesure par d'autres, exclut les systèmes d'intelligence artificielle comme ils sont entendus dans cette étude. En effet, et à condition d'infléchi la position soutenue quant à la nature de ces systèmes, il n'est possible d'envisager à travers cette disposition que la question de la réparation des dommages causés par

Concrètement, la directive 2024/2853 relative à la responsabilité du fait des produits défectueux était attendue par les deux systèmes juridiques nationaux[476] afin de redéfinir le produit immatériel et de transformer l'immatérialité des algorithmes[477] en une « chose » susceptible de générer de nouveaux rapports juridiques entre l'utilisateur et le système informatique, par exemple.

158. Écrire le droit actuel. Lorsque nous analysons la relation entre l'homme et la machine, le paradigme de Turing semble quelque peu dépassé, car l'homme d'aujourd'hui « imagine une vie éternelle ; il se rêve chimère, il se figure machine »[478]. Lorsque nous discutons de l'écriture du droit actuel, j'estime qu'il existe au moins deux phénomènes observables qui devraient nous confirmer que les algorithmes écrivent leur propre droit : la justice prédictive et la crise de la doctrine. Depuis la première collecte automatisée de données privées à l'aide de la tabulatricie mécanique de Hollerith dans les années 1890[479], jusqu'aux ambitions du Plan de calcul de la France en 1966[480], à la création du concept de Big Data[481], et même à la construction d'immenses laboratoires étatiques de surveillance biométrique[482], le droit semblait contrôler assez bien la situation. Aujourd'hui, face aux algorithmes, le droit semble parfois être un simple spectateur, notamment en ce qui concerne l'intrusion dans la vie privée des utilisateurs.

---

les systèmes d'intelligence artificielle qui seraient combinés à des dispositifs « robotiques », et ce davantage parce que leur action connait une manifestation matérielle que parce qu'ils mettent en œuvre un raisonnement au service d'une prise de décision. »

[476] Tous les États membres sont tenus de transposer cette directive avant le 9 décembre 2026. À cette même date, la Directive 85/374/CEE sera abrogée.

[477] Voir A. Cornuéjols, L. Miclet, *Apprentissage artificiel : concepts et algorithmes*, Editions Eyrolles, 2011.

[478] N. Anciaux, *op. cit*. p.503.

[479] Herman Hollerith (1860-1929), statisticien et ingénieur américain, a inventé la tabulatricie mécanique pour le recensement américain de 1890. Cet appareil utilisait des cartes perforées pour enregistrer et traiter les données, réduisant ainsi considérablement la durée des calculs. Son succès a conduit à la création de la Tabulating Machine Company (1896), qui, à la suite de plusieurs fusions, est devenue en 1924 IBM, pionnière de l'informatique.

[480] En 1966, le gouvernement français a lancé le Plan Calcul, un vaste programme industriel visant à assurer la souveraineté technologique de la France et à réduire sa dépendance vis-à-vis d'IBM. En créant la Compagnie Internationale pour l'Informatique (CII), l'État a investi massivement dans la production d'ordinateurs « made in France ». Le plan n'a pas réussi à créer un champion mondial, mais il a marqué le début des politiques publiques de stratégie numérique nationale. Par la suite, l'infrastructure qui en a résulté a favorisé des projets tels que SAFARI (1970), déclenchant le débat sur la protection des données personnelles et conduisant à la loi de 1978 « Informatique et Libertés » et à la création de la CNIL.

[481] Le terme « Big Data » est apparu au début des années 1990 et désigne un nouveau régime épistémologique de l'information, défini par le volume, la vitesse et la variété. Le concept ne vise pas la simple accumulation de données, mais la capacité des algorithmes à extraire des corrélations et des modèles prédictifs à partir de masses d'informations hétérogènes. Le Big Data marque ainsi une mutation structurelle dans les domaines de la science, de l'économie et du droit, remplaçant l'analyse causale classique par la rationalité statistico-prédictive.

[482] Les États modernes ont développé des laboratoires de surveillance biométrique d'une ampleur sans précédent, intégrant la reconnaissance faciale, les empreintes digitales, l'iris et l'analyse comportementale. La Chine est en tête avec son système « Skynet », qui compte des centaines de millions de caméras intelligentes, suivie par les États-Unis, la Russie et les États européens avec des projets pilotes. Ces infrastructures soulèvent des dilemmes majeurs concernant les libertés fondamentales, en particulier le droit à la vie privée et le contrôle démocratique.

B. « Un Carbonnier non publié sur internet ne vaut plus grand-chose »[483]

159. L'importance de la doctrine. Les principaux objectifs de la doctrine sont assez clairs : systématiser et décrire le droit[484]. La systématisation représente la partie qualitative de la doctrine, la construction du cadre conceptuel, moins visible, tandis que la description du droit représente la partie quantitative, plus impressionnante, qui suppose la description des règles et des principes spécifiques au droit[485]. D'autres auteurs soutiennent que la doctrine a un rôle informatif – elle contribue à la compréhension et à la connaissance du droit positif et offre des solutions aux problèmes pratiques ; réflexif – elle guide le législateur dans le processus législatif, aide à la formation d'un certain type de jurisprudence ou critique les imperfections du système juridique[486]. Tout cela se passe dans l'ombre des projecteurs[487], sans être une source directe du droit[488], d'autant plus que dans de nombreux cas, les opinions des auteurs sont contradictoires. D'un autre point de vue, la doctrine assure la fonction de « légitimation du droit positif »[489]. En pratique, « le fondement de l'ordre social moderne n'est pas le bourreau, mais le professeur »[490]. Certains auteurs considèrent que l'utilisation du terme « doctrine » est inappropriée et que le terme correct est « droit savant »[491], qui a une plus grande dose d'universalité.

160. La crise de la doctrine ? « De quelle façon, jurisconsultes, travaillons-nous en fait ? De quelle façon devons-nous travailler ? » est la question posée[492] en 1922 par le juriste français François Gény (docteur *honoris causa* de l'Université de Iași - 1934). Cette question reste d'actualité, surtout si l'on parle d'une crise de la doctrine[493] en général, ou, plus précisément, d'un éloignement de l'âge d'or de la doctrine française[494]. Il ne faut pas non plus ignorer les voix

---

[483] F.Terré, & N.Molfessis, *op. cit*., p.766

[484] M. Van Hoecke et F. Ost, « Legal Doctrine in Crisis: Towards a European Legal Science », in *Legal Studies*, vol. 18, n° 2, 1998, p.197-215

[485] *Idem*.

[486] J.-Syl. Bergé & P. Courbe, *Introduction générale au droit*, 19e édition, Paris : Dalloz, collection Mémentos, 2025, p.87-88.

[487] F. Ost et M. van de Kerchove, *Jalons pour une théorie critique du droit*, Bruxelles, Facultés universitaires Saint-Louis, 1987, p.43.

[488] R. Cabrillac, *op. cit.*, p.178.

[489] A. Meynaud-Zeroual, « Roger Latournerie, itinéraire d'une conscience juridique au service de l'État », in *Revue française de droit administratif* (RFDA), 2017, p.374.

[490] E. Gellner, *Nations and Nationalism*, Ithaca (NY), Cornell University Press, 1983, p.34.

[491] Ph. Jestaz, *Les sources du droit*, 3e éd., Paris, Dalloz, coll. « Connaissance du droit », 2022, p. 164 : « En France, l'idée de désigner le droit savant sous le nom de « la doctrine » paraît aujourd'hui naturelle, mais l'expression ne date que du milieu du XIXe siècle. Auparavant, les juristes invoquaient la doctrine des auteurs, autrement dit leurs opinions, implicitement considérées comme individuelles. Le nouveau terme, en tant qu'il désigne l'ensemble des ouvrages et des auteurs (selon une définition communément admise), tend à mettre l'accent sur l'aspect collectif du phénomène doctrinal ».

[492] F. Gény, « *Science et technique en droit privé positif : nouvelle contribution à la critique de la méthode juridique* », in LGDJ, 1922, p.3.

[493] M. Van Hoecke et F. Ost, *op. cit*.

[494] F. Hakim & F. Melleray, « *La belle époque de la pensée juridique française* », in N. Hakim & F. Melleray (dir.), *Le renouveau de la doctrine française*, Paris, Dalloz, 2009, p.5 ; v. aussi O. Jouanjan & E. Zoller, *Le «*

qui affirment avec force que la doctrine française « jamais assurément égalée »[495]. La divergence d'opinions peut souvent être une qualité constructive de la doctrine. Par exemple, un autre auteur soutient qu'à l'heure actuelle, le rôle de la doctrine est en déclin, « il n'est pas comparable à celui joué par la doctrine Outre-Manche ou par les auteurs du XIXe siècle en France »[496].

161. Critiques. De nombreuses critiques ont déjà été formulées selon lesquelles le déclin de la doctrine serait dû, entre autres, à l'ère numérique, à la massification[497], à l'augmentation de la quantité d'informations analysées et au nombre élevé de revues juridiques, conduisant à une « asphyxie doctrinale »[498]. On soutient également que la doctrine est victime de la mode : « la colloquomanie », la multiplication des colloques, sur des sujets qui souvent ne le méritent guère, aux fonctions plus mondaines que scientifiques »[499]. Les créations basées sur l'intelligence artificielle, y compris les avis juridiques émis par ChatGPT, s'appuient sur des bases de données très volumineuses, collectées en permanence auprès des utilisateurs de la technologie, très souvent sans respecter le consentement ou les droits d'auteur[500].

162. Critères d'indexation des moteurs de recherche. Dans le même temps, la doctrine identifie un autre problème concernant son propre déclin, à savoir que le principal moteur de recherche de la doctrine, Google, « la recherche juridique n'est plus fonction de l'importance des auteurs mais de l'adéquation de l'écrit à ce dont on a besoin, ce que les mots-clés sont censés refléter »[501]. Concrètement, un auteur inconnu, qui connaît bien les critères d'indexation des moteurs de recherche, peut devenir plus précieux que Carbonnier pour un public non averti ou superficiel. Cette réalité s'inscrit déjà dans le contexte d'une « déscientification »[502] des écrits juridiques, une contestation assez courante[503].

163. Les algorithmes influencent déjà la rédaction du droit. Dans ce contexte assez sombre, des questions commencent à se poser : combien de temps faudra-t-il avant que les algorithmes commentent entièrement la jurisprudence ou que les revues juridiques classiques

---

moment 1900 ». Critique sociale et critique sociologique du droit en Europe et aux États-Unis, Paris, Éditions Panthéon-Assas, 2015, note citée par V. Champeil-Desplats, *Méthodologies du droit et des sciences du droit*, 3e éd., Paris, Dalloz, 2022.

[495] V. Champeil-Desplats, *Méthodologies du droit et des sciences du droit*, 3e éd., Paris, Dalloz, 2022, p.1.

[496] R. Cabrillac, *Introduction générale au droit*, 16e éd., Paris, Dalloz, 2025, p.181.

[497] Ph. Jestaz, *op. cit.*, p.164.

[498] D. Bureau et N. Molfessis, « L'asphyxie doctrinale », in *Études offertes à Bruno Oppetit*, Paris, Litec, 2009, p.45.

[499] R. Cabrillac, *op. cit.*, p.182.

[500] Vivant, M. & Bruguière, J.-M., *Droit d'auteur et droits voisins*, 5e éd., Paris : Lefebvre-Dalloz, 05 décembre 2024, p.189.

[501] *Idem*, p.766.

[502] *Idem*, p.767.

[503] A. von Bogdandy, « The Past and Promise of Doctrinal Constructivism: A Strategy for Responding to the Challenges Facing Constitutional Scholarship in Europe », in *International Journal of Constitutional Law*, vol. 7, no 3, juillet 2009, p.364-400.

soient englouties par les systèmes automatisés de production du droit ?[504] Ce qui est certain, c'est que la rédaction du droit par des algorithmes se fait par le simple fait que les grands éditeurs juridiques en ligne disposent de moteurs de recherche basés sur l'intelligence artificielle et que les recherches des auteurs sont influencées par des codes binaires et peut-être même par les « intérêts » particuliers des algorithmes. Concrètement, sans que nous le souhaitions, les informations que la machine juge pertinentes nous sont présentées pour validation, tandis que celles qui sont réellement pertinentes peuvent être facilement dissimulées.

164. Similitude : la doctrine paulienne. Le droit écrit par des algorithmes pourrait fonctionner selon les principes de la doctrine paulinienne *Omnis potestas a Deo*, modifiée par la suite en *Omnis potestas a Deo per populum* : « tout pouvoir vient de Dieu, à charge, pour son titulaire, de l'exercer au bénéfice de la communauté »[505]. La différence essentielle est que le pouvoir ne vient plus de la divinité, mais du créateur direct, nul autre que l'homme.

a). Justice prédictive, les algorithmes collectent-ils des données pour écrire le droit ?

165. Justice prédictive. La situation est encore plus claire en ce qui concerne la tentation « post-humaniste »[506] d'utiliser des algorithmes pour la justice prédictive, là où les acteurs de la justice peuvent demander l'aide de l'intelligence artificielle[507]. Les algorithmes deviennent de véritables sociologues de la justice et les dernières études montrent qu'ils peuvent imiter le juge et transformer les faits en décisions judiciaires sur la base de critères prédéfinis[508]. La justice prédictive, bien que son nom soit contesté dans la doctrine[509], importe le principe du précédent à partir des bases de données jurisprudentielles et le juge devient à la fois la « matière première » et le destinataire du résultat, étant considéré à la fois comme victime et instigateur[510].

---

[504] F.Terré & N.Molfessis, *op. cit*., p.767.

[505] L. Anselmi, R. Bernardini, C. Chatel-Petit, F. Picod & Y. Strickler (éds.), *Mélanges en l'honneur de Jean-François Renucci*, Paris : Dalloz, coll. Études, Mélanges, Travaux, 2024, p.31.

[506] A. Garapon, « Un nouveau modèle de justice : efficacité, acteur stratégique, sécurité », in *Esprit*, 2008, p.98-122.

[507] V. E. Vergès, « *Le juge face à la boîte noire : l'intelligence artificielle au tribunal* », D. 2022. 1920.

[508] É. Vergès, C. Bazzoli et G. Vial, « *La modélisation des décisions de justice à partir des faits. Comment l'intelligence artificielle imite les raisonnements des juges à partir d'une grille de critères* », in La Semaine Juridique. Édition générale, suppl. au n° 6, 10 févr. 2025, LexisNexis.

[509] On propose le terme « probabiliste » - Laëtitia Janicot, « L'anonymisation du juge », in Pierre Bourdon (dir.), *La communication des décisions du juge administratif*, LexisNexis, 2020, 81, p.85. ; « prévisible » - François Thévenot, « *L'open data et la justice prédictive* », in Frédérique Ferrand, Jonas Knetsch et Martin Zwickel (dir.), *Le droit civil et la justice civile à l'ère de la numérisation en France et en Allemagne*, FAU University Press, 2020, p.321 ; « quantitative » - Bruno Pireyre, « *Allocution d'ouverture* », in Nathalie Blanc et Mustapha Mekki (dir.), *Le juge et le numérique : un défis pour la justice du XIXe siècle*, Dalloz, 2019, 1, p.4. ; « jurisprudence chiffrée » - Thierry Kirat, « L'intelligence artificielle, l'avocat et le juge », in *La Tribune*, 2017. En l'occurrence, cette expression est propre à un rapport du GIP Mission de recherche.

[510] C. Bordère, *La justice algorithmique. Volume 243. Analyse comparée (France/Québec) d'un phénomène doctrinal*, Paris : Dalloz, Nouvelle Bibliothèque de Thèses, 2025, p.227.

L'ambition de ce type de justice pénale est de transformer l'acte de juger « en une opération automatique fondée sur l'objectivation de données factuelles ou de « facteurs de risques » »[511]. Dans le même temps, nous pouvons admettre que ce qui domine l'espace juridique au début du XXIe siècle, « c'est l'imprécis, l'incertain, l'instable, ou encore, en termes plus provocateurs, le flou, le doux et le mou »[512]. Ainsi, pour les algorithmes, le moment semble le plus propice pour tenter d'écrire leur droit, même si cela ne semble pour l'instant qu'une fiction.

Conclusion : *homo algoritmus*, construit exclusivement à partir de données fournies volontairement

166. Le paradigme de la cohabitation. La surveillance[513] par tous les moyens, y compris par la collecte continue de données, semble être l'un des piliers de la société actuelle[514] et, en même temps, la source qui maintient en vie l'*homo numericus* et lui confère les attributs d'une personne physique. Dans cette nouvelle paradigmatique de la cohabitation, « le capitalisme de surveillance revendique unilatéralement l'expérience humaine comme matière première gratuite à traduire en données comportementales »[515], et la gouvernance algorithmique[516] transforme l'identité[517] en flux profilables et implicitement exploitables[518]. Dans le même temps, les instruments classiques de surveillance ont connu des changements radicaux et structurels, devenant une « coproduction » orchestrée à la fois par l'État et le secteur privé[519], et le surveillant devient surveillé par une exposition permanente sur les réseaux sociaux[520].

---

[511] P. Beauvais, D. Chilstein & E. Dreyer (dir.) (2024), *op. cit.*, p.404.
[512] M. Delmas-Marty, *Le pluralisme ordonné. Les forces imaginantes du droit, II. L'un et le multiple : les divers pluralismes. Introduction*, Paris, Seuil, 2009, p.7-32.
[513] David Lyon, *Surveillance Studies: An Overview*, Polity, 2007 — defin., p.14.
[514] L. Laref, M. Laref (dir.), *Surveillance*, Paris, Dalloz, coll. "Themes & commentaires – Actes", 1re ed., 28 nov. 2024, p.13.
[515] S. Zuboff, *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, New York, PublicAffairs, 2019, p.7.
[516] A. Rouvroy, T. Berns, « *Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation* ? », in Réseaux, 2013/1 (n° 177)
[517] A. Rouvroy, T. Berns, *op. cit.* : *« Dans la gouvernementalité algorithmique, chaque sujet est lui-même une multitude, mais il est multiple sans altérité, fragmenté en quantité de profils qui tous se rapportent à 'lui-même', à ses propensions, ses désirs présumés, ses opportunités et ses risques*. »
[518] *Idem* – « le mode de gouvernement par les algorithmes prétend s'adresser à chacun à travers son profil. Plutôt que d'un accord, ou même d'un consentement, ce à quoi nous avons ici affaire relève de l'adhésion par défaut à une normativité aussi immanente que celle de la vie même. »
[519] L. Laref, M. Laref (dir.), *op. cit*., p.8 – « *Si la surveillance étatique continue de nourrir les réflexions, la surveillance privée n'est cependant pas en reste. Parfois encouragée par les pouvoirs publics au nom d'une coproduction de la sécurité exaltée, beaucoup sont enclins à apporter leur pierre à l'édifice dès lors que cette surveillance se drape de l'objectif de sécurité*. »
[520] *Idem*, p.8 : *« Le surveillé devient à son tour surveillant dans une forme de « contre-surveillance », le plus souvent par le truchement de ses appareils connectés, au premier rang desquels se trouvent les smartphones et les réseaux sociaux qui encouragent une exposition permanente*. »

167. Prochaine étape : l'*homo algorithmicus*. Nous avons établi dans la présentation ci-dessus que l'*homo numericus* décrit l'individu réduit à des données numériques, acteur de la révolution numérique[521], modelé par la collecte et le stockage massif d'informations personnelles. La prochaine étape est l'*homo algorithmicus*, où il ne s'agit plus seulement de quantifier l'existence, mais de la gouverner par des algorithmes : les données sont traitées pour anticiper, orienter et même prescrire des comportements. Si l'*homo numericus* exprime l'ère de la quantification, l'*homo algorithmicus* marque l'ère de la décision automatisée, dans laquelle les algorithmes imposent des normes subtiles qui peuvent éroder le rôle du droit classique.

168. Le parcours de l'*homo algorithmicus*. Toutes ces transformations sont basées sur le résultat de l'interaction entre l'homme et la machine, entre l'être et le nouvel espace numérique découvert entre « zéro » et « un ». Le passage entre les deux identités s'est fait de manière apparemment naturelle : la numérisation massive de la vie par la collecte de données a consolidé l'*homo numericus* ; big data + machine learning : les données collectées ont été corrélées et ont permis de générer des prédictions ; automatisation de la décision : les banques, la police, les assurances, les véhicules sans conducteur, les services secrets, etc. confient l'autonomie de la décision à des algorithmes ; législation/réglementation implicite : les recommandations algorithmiques font partie de la vie quotidienne de l'individu et du droit, réussissant à régir les comportements et même à sanctionner ceux qui sont répréhensibles. Tel est le parcours de l'*homo algorithmicus*!

[521] A. Supiot, *La gouvernance par les nombres*, Paris, Fayard, 2015, p.19.

Section 8. PLAN DE THÈSE

§1. PLAN D'ÉTUDES

169. L'une des propositions de cette thèse est d'apporter des réponses, sans prétendre être à chaque fois les meilleures, à ce type de questions. En même temps, bien que cela puisse sembler un paradoxe, ce ne sont pas les réponses qui sont utiles pour résoudre le problème en soi, mais la signalisation même du problème. Ainsi, il sera possible de découvrir au contenu de cette thèse des problèmes juridiques surdimensionnés pour lesquels la loi n'a pas encore trouvé de réponses concrètes et pour lesquels nous n'avons fait que de les signaliser.

En général, l'approche consiste à considérer les choses du point de vue du droit pénal, dernière redoute contre une atteinte sans précédent à la vie privée individuelle et même à l'autonomie de la volonté[522]. Certains auteurs apprécient le fait que lorsque les gens se surveillaient, la vie privée avait ses propres zones de protection. Dans le contexte où nous vivons dans un monde où les systèmes d'information effectuent cette surveillance, « pour la première fois dans l'histoire, il est possible que la vie privée soit complètement annihilée »[523].

En même temps, j'ai évité d'aborder une analyse cantonnée au seul discours sévère et rigoureux du droit pénal et j'ai essayé d'aborder le sujet avec des références à d'autres domaines tels que l'histoire, l'informatique, la sociologie, la philosophie, la médecine, la théologie, etc. J'ai procédé de telle manière précisément parce que je considérais qu'une vision diachronique et systémique de certains phénomènes et réactions sociaux était les prémisses de quelques règlements juridiques avec lesquels nous devons vivre au quotidien.

Partie I. La protection pénale de la vie privée à l'ère numérique. Dans la première partie de cet ouvrage, nous avons abordé l'évolution du concept de vie privée, les mécanismes de protection pénale, les particularités des systèmes pénaux roumain et français en matière d'identité physique et virtuelle de l'individu, mais aussi la vulnérabilité de cette identité.

Partie II. Le droit pénal face à l'évolution technologique : intrusion, défis, adaptation. La deuxième partie de l'ouvrage aborde les défis contemporains du droit pénal dans le contexte du développement des algorithmes et de l'intelligence artificielle, tout en analysant

[522] La première chose qui me vient à l'esprit quand je pense à l'autonomie de la volonté est liée aux campagnes d'élection au cours desquelles les systèmes d'intelligence artificielle sont utilisés afin d'influencer le libre arbitre des électeurs. Des controverses à ce sujet ont surgi lors des campagnes électorales pour les élections présidentielles en France (2017), aux États-Unis (2017) ou en Roumanie (2024), ou lors d'autres moments où le vote populaire a décidé du sort d'un pays : le Brexit (2016) ou l'indépendance de la Catalogne (2017).
[523] Y. N. Harari, *Nexus - Scurta istorie a retelelor informationale din epoca de piatra pana la IA*, Editura Polirom, Iași, 2024, p.214.

les formes concrètes d'intrusion dans la vie privée, tant de la part de l'État que des acteurs privés. Dans le même temps, l'ouvrage ouvre le débat sur l'avenir de la protection de la vie privée et sur les limites auxquelles le droit se heurte face à la dynamique des évolutions technologiques et sociales.

§2. MOTIF DE LA RÉALISATION D'UNE ÉTUDE COMPARATIVE FRANCE - ROUMANIE

170. Je pense qu'il est très important d'effectuer une analyse comparative entre les deux systèmes juridiques, français et roumain, car ils sont très étroitement liés. L'influence française sur la Roumanie a été déterminante pour la construction de l'État roumain moderne. Les élites politiques et juridiques roumaines formées à Paris au XIXe siècle ont importé non seulement des techniques législatives, mais aussi des valeurs culturelles et politiques qui ont orienté le développement des institutions. Le soutien diplomatique de la France a été essentiel à la reconnaissance de l'indépendance de la Roumanie (1878) et de la Grande Union (1919). Cet héritage juridique et culturel explique pourquoi la Roumanie fait aujourd'hui partie de l'espace francophone et pourquoi l'étude comparative du droit franco-roumain est si pertinente.

Par exemple, le premier Code pénal roumain (1865) s'est inspiré principalement du Code pénal français (1810). Cette recherche porte sur la réglementation « du délit d'atteinte à la vie privée » prévue à l'article 226 du nouveau Code pénal roumain. D'une manière générale, il s'agit d'un délit similaire à celui du Code pénal français (« de l'atteinte à la vie privée»), avec une définition similaire. Il a été introduit pour la première fois dans le droit pénal roumain en 2014.

Je souligne que dans la législation pénale française, cette infraction est entrée en vigueur dans l'ancien Code pénal le 1er janvier 1978, avant d'être reprise dans le Code actuel en 1994. Elle a subi des modifications substantielles depuis l'entrée en vigueur de la première réglementation jusqu'à aujourd'hui, avec l'ajout de dispositions très actuelles, qui visent principalement l'évolution numérique. De l'analyse que j'avais menée pour l'élaboration de cette thèse de recherche, il ressort clairement que depuis 2014 jusqu'à présent l'article 226 du Code pénal français a été modifié 27 fois, avec toutes les infractions connexes et assimilées prévues par différents paragraphes et l'article 226 du Code pénal roumain a fait l'objet de trois modifications/compléments par la loi 171 du 14 juin 2023. Certaines des modifications apportées à l'article 226 du Code pénal français concernent les menaces terroristes contre la

France ou l'organisation des Jeux olympiques de 2024 ou même le phénomène de la violence domestique.

§3. MÉTHODES DE RECHERCHE UTILISÉES POUR L'ÉLABORATION DE LA THÈSE

171. L'objet principal de la recherche est la manière dont la vie privée est limitée par les actes normatifs des législations roumaine et française, en analysant notamment le droit pénal. La recherche scientifique part de l'hypothèse que la vie privée n'est pas un droit absolu et que les limitations normatives imposées génèrent des controverses tant dans la conception des textes du droit, comme dans leur interprétation, mais aussi dans la pratique judiciaire ou la doctrine. L'approche de la thèse est particulièrement d'orientation dans le domaine de la vie privée, pour analyser diachroniquement / synchroniquement, systématiquement, téléologiquement, historiquement, logiquement ce domaine et de générer des idées ou des éclaircissements utiles tant pour les protagonistes d'un éventuel litige que pour les juristes impliqués dans sa solution.

Afin d'atteindre les objectifs principaux fixés, il est nécessaire d'utiliser des méthodes de recherche qui ne permettent pas d'émettre des idées/allégations ou des thèmes de travail aléatoires, malins, favorables à l'hasard ou contradictoires. La méthode analytique[524] semble être la plus facile à appliquer dans une telle recherche. Grâce à cette méthode, il est facile d'exposer et d'analyser les concepts avec lesquels je travaillerai, de clarifier le sens des termes, des normes juridiques et des idées abordées

172. La méthode comparative[525] est peut-être la méthode la plus utilisée dans l'élaboration d'une recherche juridique. Évidemment, cette méthode occupe une place centrale dans l'élaboration de la thèse de doctorat car elle vise à trouver, sur des critères objectifs, des éléments similaires ou différents lors de l'analyse des controverses liées à la vie privée, l'évolution de ce concept et les perspectives futures. Pour que cette méthode soit efficace et que les résultats soient scientifiques, un certain nombre de critères essentiels doivent être respectés : seul ce qui est comparable peut être comparé (par exemple, si les systèmes de droit comparés

[524] J.-P. Chazal, « *Philosophie du droit et théorie du droit, ou l'illusion scientifique* », Revue interdisciplinaire d'études juridiques, vol. 46, n° 1, 2001. p. 39-80

[525] T. Rambaud, *Introduction au droit comparé. Les grandes traditions juridiques dans le monde*, 2e éd., Paris, PUF, coll. « Quadrige », 2017; M. Troper, « *L'histoire du droit, le droit comparé et la théorie générale du droit* », Revue internationale de droit comparé (RIDC), 2015. p. 331; N. Cornu-Thénard et L. Bonne, « *Enjeux d'une critique fondée sur l'histoire du droit et le droit comparé* », Revue critique de législation et de jurisprudence (RCLJ), 2018, p. 6

sont opposés dans leur substance, idéologiquement, le résultat de la comparaison sera sans importance); les termes soumis à la comparaison doivent être analysés dans leurs liens réels, rapportés au contexte social, politique, culturel dont ils sont issus; les termes à comparer doivent se rapporter non seulement au sens actuel qu'ils ont mais aussi à l'évolution antérieure, au fil du temps, dans le processus d'application d'une certaine norme juridique; l'identité des phénomènes juridiques générés par la comparaison doit être fondée sur la découverte d'un nombre suffisant d'indices communs. Certainement, la méthode comparative facilite la construction des typologies juridiques et de leurs classifications, jouant un rôle déterminant dans le processus législatif ou dans la création d'une jurisprudence nationale ou européenne en matière de vie privée.

173. Dans le contenu de la thèse, la méthode comparative cohabitera avec l**a méthode historique et celle sociologique**[526]. Quant à la méthode historique, les choses sont assez claires, en ce sens qu'elle inclura l'approche des concepts et notions de droit du point de vue de la dimension historique. Partant des données que l'histoire nous fournit, nous serons en mesure de mieux comprendre le concept de vie privée tel qu'il est actuellement perçu.

174. Partant d'une méthode de travail sociologique, on peut accéder plus facilement au domaine de la **recherche juridique empirique**[527]. Grâce à des outils empruntés à la sociologie, nous serons en mesure de mesurer, par exemple, l'impact des campagnes de manipulation de l'information sur la vie privée. La situation d'une réglementation juridique précaire du contenu pouvant être diffusé sur les réseaux sociaux et comment ce contenu peut influencer abusivement la volonté des utilisateurs sera également abordée. La recherche juridique empirique peut s'avérer utile lorsqu'il s'agit de discuter de la nécessité d'élaborer des normes qui correspondent aux réalités sociales actuelles, sans avoir un correspondant dans le passé.

[526] J. Carbonnier, *Sociologie juridique*, 1re éd., Paris, Armand Colin, 1972 ; nouv. éd., Paris, PUF, coll. « Quadrige », 1978
[527] L. Epstein & A. D. Martin, *An Introduction to Empirical Legal Research*, Oxford, Oxford University Press, 2014

Première partie
LA PROTECTION DE LA VIE PRIVÉE À L'ÈRE NUMÉRIQUE

„Quand on me présente quelque chose comme un progrès, je me demande avant tout s'il rend plus humain ou moins humain"
George ORWELL[528]

175. Même si aujourd'hui la protection de la vie privée est une préoccupation assez active du droit, en réalité, l'évolution technologique crée un mécanisme qui semble mettre l'individu dans la même situation qu'il avait dans l'Antiquité: sous la surveillance étroite des autres, de la communauté à laquelle il appartient ou de l'Etat. Depuis l'Antiquité, les concepts d'espace privé et d'espace public ont représenté deux préoccupations sociales continues des individus, l'intérêt pour la délimitation du privé du public représentant, en substance, le besoin de l'homme d'organiser sa vie aussi bien que possible.[529]

Titre I
LE FONDEMENT JURIDIQUE DE LA PROTECTION DE LA VIE PRIVÉE

176. En analysant la société actuelle, nous pouvons indéniablement apprécier que le privé coexiste avec le public, sont des espaces interdépendants, mais chacun est guidé par des valeurs et des règles distinctes. En substance, ces concepts reflètent deux dimensions distinctes de la même vie humaine, mais avec leurs propres caractéristiques et rôles.[530] L'espace privé de l'individu occupe l'espace personnel et intime de sa vie, tandis que l'espace public occupe l'espace commun de sa vie. Ni le privé ni le public ne se contredisent et s'annulent dans la lutte pour le pouvoir, mais les deux ont une position similaire dans l'organisation de la société. D'autant plus que les deux sont interdépendants et ne peuvent exister l'un sans l'autre.[531]

---

[528] L'affirmation de George Orwell exprime son scepticisme à l'égard des progrès technologiques ou sociaux, qui doivent être jugés non seulement en fonction de leur nouveauté, mais aussi en fonction de leurs conséquences sur l'humanité. L'auteur invite à une analyse critique de ce qui est présenté comme un progrès, en remettant en question le fait que l'innovation contribue à améliorer la vie humaine ou, au contraire, la rend plus artificielle, plus distante et plus inhumaine. La citation place l'être humain au centre de l'évaluation. Un progrès qui déshumanise ou qui n'apporte pas d'amélioration réelle ne peut être considéré comme un progrès, quel que soit son niveau technique.
[529] S. Marcos, éditeur. *Entre espace public et espace privé : les élites en représentation*. Presses universitaires de Perpignan, 2018. L'auteur analyse la manière dont les élites antiques représentaient les limites entre le public et le privé. Dans l'Antiquité, ces sphères n'étaient pas strictement séparées : dans la maison, les temples, les espaces civiques, la vie privée devenait un instrument de prestige public. L'ouvrage souligne que la vie privée servait souvent à consolider la vie publique et que la distinction entre intimité et visibilité collective n'existait pas encore en ces termes.
[530] P. Kayser, *La protection de la vie privée*, 2e éd., Revue internationale de droit comparé. Vol. 43 N°1, Janvier-mars 1991. pp. 269-271.
[531] V. Velasco, *La difficile formalisation d'un droit à la vie privée, La vie privée à l'heure des médias*, édité par Patrick Baudry et al., Presses Universitaires de Bordeaux, 2002.

Chapitre 1
L'EFFET DES ÉVOLUTIONS TECHNOLOGIQUES SUR LA VIE PRIVÉE

177. Intérêt. L'évolution de la notion de vie privée de la sphère de la philosophie à la sphère de la sociologie et plus tard du droit a suivi un parcours assez difficile. L'intérêt du système juridique pour la vie privée s'est manifesté lorsqu'il y avait un réel besoin de protéger l'individu contre l'intrusion de l'État ou d'autres[532], et il redevient actuel à l'époque de la Restauration, lorsque des personnes politiques ou notoires sont « victimes privilégiées d'indiscrétions et de divulgation de leur vie privée dont la valeur marchande attise les convoitises ».[533]

Section 1. D'UN CONCEPT PHILOSOPHIQUE À UN DROIT FONDAMENTAL

178. Les débuts du concept de vie privée. La notion de vie privée, mais surtout le besoin de la protéger, ont peu à peu évolué d'un simple concept philosophique vers des normes juridiques à caractère civil ou pénal. D'un concept philosophique dont on retrouve la genèse dans l'Antiquité chez Platon[534] et plus tard chez Aristote[535], la vie privée est progressivement devenue un droit fondamental[536]

§1. PREMIÈRES APPROCHES PHILOSOPHIQUES DU CONCEPT

[532] P. Kayser, „*La protection de la vie privée par le droit: protection du secret de la vie privée*", Economica, éd.3, 1995. p. 11 - 18

[533] J. C. Saint-Pau (coord), „*Droits de la personnalité*", Paris, LexisNexis SA, 2013. p.676

[534] Dans ses dialogues, Platon souligne l'idée que les gardiens de la cité ou les philosophes ne devraient pas bénéficier des mêmes privilèges de la vie privée comme les gens ordinaires. Dans la plupart des situations trouvées dans la République, la vie privée est utilisée dans le même contexte que la vie publique. À titre d'exemple, je cite quelques passages de Platon : Œuvres Complètes : La République. Traduction Nouvelle avec Introduction et Notes par Robert Baccou, Librairie Garnier Frères, 1938: "*Pour moi, telle est mon opinion : dans le monde intelligible l'idée du bien est perçue la dernière et avec peine, mais on ne la peut percevoir sans conclure qu'elle est la cause de tout ce qu'il y a de droit et de beau en toutes choses ; qu'elle a, dans le monde visible, engendré la lumière et le souverain de la lumière; que, dans le monde intelligible, c'est elle-même qui est souveraine et dispense la vérité et l'intelligence ; et qu'il faut la voir pour se conduire avec sagesse dans la vie privée et dans la vie publique*" (page 251) ou "*Et pour ce qui est des honneurs, il aura en vue le même but; il acceptera, goûtera volontiers ceux qu'il croira fi même de le rendre meilleur, mais ceux qui pourraient détruire en lui l'ordre établi, il les fuira dans la vie privée comme dans la vie publique*" (page 352). Cette version a été consultée en format pdf (http://ugo.bratelli.free.fr/Platon/PlatonRepublique.pdf) .

[535] Aristote, *Les Politiques*, Édition de Pierre Pellegrin, Paris, Flammarion, 2015. voir le Livre VI, chapitre VIII, Livre VII, chapitre X, Livre VII, chapitre XI.

[536] Conseil de l'Europe, *Convention européenne des droits de l'homme,* Roma, 1950. https://www.echr.coe.int/documents/d/echr/Convention

179. La contribution d'Aristote à la définition du concept. Définissant l'homme comme un être social, Aristote est l'un des premiers philosophes antiques à tracer un cadre représentatif de la délimitation entre le *privé* et le *public*. En substance, l'homme est celui qui ne met à jour ses capacités « que dans et à travers la société »[537], la société se matérialisant sur deux niveaux : l'individuel (humain ou subjectif) et le collectif (social ou objectif). Les deux plans coexistent, sont interdépendants mais distincts, ayant en leur centre l'individu lui-même qui tend vers le but absolu d'atteindre le Bien Suprême. Nous ne parlons pas ici du Bien abstrait et transcendant pratiqué par Platon à travers son école philosophique[538], mais du Bien qui est susceptible d'être réalisé dans la pratique, le Bien accessible à l'homme[539]. Les adeptes de l'école aristotélicienne apprécient que pour atteindre le Bien-but, il faut définir clairement la relation entre l'Etat et l'individu, entre le bien individuel et celui de la communauté, entre l'homme et le citoyen, cette délimitation n'étant possible que par le biais de l'État qui légifère les normes morales afin d'obtenir un comportement exemplaire de la part des citoyens.

180. Définition du concept de vie privée à l'ère actuelle. Le *Privé* devient une forme particulière de la relation individuel-universel, reconnaissant l'immanence de l'universel humain, les valeurs suprêmes de l'être humain étant matérialisées par rapport à la vie réelle, car ce n'est que dans un monde aussi terrestre et réalisable qu'il est possible de transformer les déterminations de l'être humain en valeurs effectives[540].

A. La vie privée n'est pas une invention de la modernité

181. Les civilisations de l'Antiquité et le concept de vie privée. Dans la Grèce antique[541] ou à Rome[542], le concept de vie privée n'avait pas d'intérêt qu'en tant qu'antithèse de la vie publique et ne correspondait évidemment pas au sens contemporain du terme. La vie de l'individu était majoritairement publique, toute activité ou passion étant facilement observée par les autres membres de la communauté. La vie privée n'est en aucun cas une invention de la

[537] I. Banu, *Sistemul filozofic al lui Aristotel*, Univ. București, 1977.
[538] W. André, *Aristote, L'Éthique à Nicomaque,* Bulletin de l'Association Guillaume Budé*, n°1, 1972. p.115-116.* Dans son œuvre, l'auteurs affirme que « *de la morale du Bien en soi à la morale de la finalité opérable, il existe une entière distance séparant le platonisme de l'aristotélisme* » www.persee.fr/doc/bude_0004-5527_1972_num_1_1_3178_t1_0115_0000_1
[539] Une idée qui revient constamment tout au long du traité aristotélicien *l'Éthique à Nicomaque*, (maison d'édition Stiintifica și Enciclopedica Bucuresti, 1988), à savoir que ce bien – finalité, qui pour Aristote était un principe de premier ordre moral est opérable et peut être modélisé en fonction des intérêts des gens.
[540] Voir l'œuvre d'I. Banu, *Sistemul filozofic al lui Aristotel*, Univ. București, 1977. p.217-218
[541] E. R. Dodds, *The Greeks and the Irrational*, University of California Press, 2004, p.71. – „*and the strongest moral force which Homeric man knows is not the fear of god, to but respect for public opinion*"
[542] A.M. Riggsby, „*A. Roman Law and the Legal World of the Romans*", Cambridge University Press, 2010.

modernité[543]. Pour comprendre la situation dans laquelle nous nous trouvons aujourd'hui, il faut comprendre certains aspects pertinents du passé. On trouve par exemple dans les textes religieux une impulsion humaine minimale vers l'intimité. Bien que cela semble surprenant comme moyen d'expression, l'intrusion dans la vie d'autrui n'étant pas un péché parmi les péchés majeurs, le Coran interdit aux croyants d'espionner les autres[544] et le Talmud[545] donne des indications précises sur la façon de poser les fenêtres d'une maison afin que la vie privée d'une personne ne soit pas affectée. Chez les chrétiens, le concept apparaît simultanément à l'expulsion du couple primordial de l'Eden, et la relation de l'homme avec la divinité est mieux organisée dans l'environnement privé de chacun[546].

182. La vision de Platon sur le concept de privé. En se référant strictement à la façon dont les anciens percevaient la vie privée, nous trouvons des détails intéressants dans les *Lois* de Platon[547]. Dans la conversation sur la façon d'obtenir le meilleur gouvernement étatique en édictant des lois appropriées, l'étranger athénien dit à Clinias que le meilleur système politique est celui où il n'y a pas de vie privée, dans lequel tous les biens sont partagés, y compris les femmes et les enfants[548]. Selon Platon, plus les communautés sont nombreuses, plus la surveillance de l'individu doit être prudente. On retrouve ici l'idée qu'un gouvernement totalitaire est bien plus adapté aux grandes villes motivée par le fait que la propriété privée peut conduire à une richesse ostentatoire (831c), que le placement des maisons privées doit être effectué selon des lois strictes (779b-c) et les voyages privés doivent être supervisés (950d). Dans les mêmes dialogues[549], des règles strictes sont imposées y compris sur le déroulement des funérailles en ce sens qu'« il serait indécent d'ordonner ou de verser des larmes sur le mort » mais ils sont interdits « les lamentations et les cris hors de la maison », de pleurer le défunt dans la rue ou de faire marcher le cortège funéraire à la vue de la foule, justement pour ne pas

---

[543] A. Acquisti, L. Brandimarte, J. Hancock, *How privacy's past may shape its future*, Science, vol.375, issue 6578, 2022. p.270-272 https://www.science.org/doi/10.1126/science.abj0826#body-ref-R1

[544] Coran verset 49.11, "*Vous les croyants, éloignez-vous promptement du soupçon, car il est des soupçons qui confinent au péché. Ne vous espionnez pas mutuellement ! Ne médisez pas les uns des autres!*".

[545] Mishneh Torah, Neighbors, versetul 7:1, "*When a person has a window in his wall and a colleague comes and builds a courtyard next to it, the owner of the courtyard cannot tell the owner of the window: "Close this window, so that you will not look at me". If his colleague desires to build a wall opposite the window to block the invasion of his privacy, he must leave a space of four cubits next to the window, to avoid casting a shadow upon it"*.

[546] Bible, Matthieu, verset 6:6, « *Mais toi, quand tu pries, retire-toi dans la pièce la plus retirée, ferme la porte et pris ton Père qui est présent dans le secret »,*.

[547] Platon, *Œuvres complètes*, Edition Flammarion, Paris, Nouvelle édition revue et corrigée, 2023.

[548] Platon, *op. cit.* – pg 795: "*Eh bien, tiennent la première place, la cité, la constitution et les lois les meilleures, où se réalise le plus possible pour toute la cité le vieux dicton qui veut que « vraiment tout est commun entre amis ». Dans cette situation, qu'elle existe maintenant quelque part ou qu'elle doive exister un jour, les femmes sont communes, les enfants sont communs, les richesses sont communes; par tous les moyens, tout ce que l'on prétend avoir en propre a été partout retranché de la Vie de tous les jours. On est parvenu, dans la mesure du possible, à faire ainsi que les yeux, les oreilles et les mains paraissent voir, entendre et agir en commun, à faire que tous à l'unisson émettent éloges aussi bien que blâmes, se réjouissent et s'affligent des mêmes choses*" (739c d)

[549] Platon, *op. cit*. – Livre XII.

déranger les autres membres de la communauté. Quiconque croit que les agences de surveillance de masse étaient une invention de l'ère moderne semble se tromper. Pour que ce type de gouvernement totalitaire fonctionne bien, Platon dit qu'un organe de surveillance est nécessaire pour vérifier comment les citoyens vivent leur vie, appelé le Conseil Nocturne (951d-e).

Certains auteurs[550] ont noté que la vie privée de l'homme ancien, telle qu'elle est exposée dans les *Lois*, est assimilée à l'utilisation du terme ἰδιώτης, utilisé en grec ancien avec le sens d'homme profane ou plébéien, et la traduction actuelle en anglais est idiote[551]. Les valeurs sociales et politiques de la Grèce antique accordaient une grande importance à la participation civique, à l'implication dans la vie publique et au suivi de l'individu par la communauté.

B. Évolution du concept de vie privée. Définition

183. Vers une définition de la vie privée : approche diachronique. Afin de pouvoir entamer une discussion pertinente sur la vie privée, il est nécessaire d'exposer brièvement une définition et l'évolution de ce concept. Selon le dictionnaire Larousse, le terme « privé, privée » désigne un attribut se référant à une personne dans sa vie personnelle (*Qui concerne quelqu'un dans sa personne même, dans sa vie personnelle*)[552]. En ce qui concerne la signification de la notion de « privé » en roumain, le Dictionnaire explicatif de la langue roumaine (DEX) indique pour elle des significations telles que *« particulier, individuel* ; *qui appartient à une personne en tant qu'individu isolé ; qui est d'une seule personne* »[553]. On remarque donc une différence d'approche linguistique, la définition française étant beaucoup plus proche du concept qui fait l'objet de ce matériel.

La vie privée est définie comme étant *la sphère d'intimité de chaque*[554] et se rapporte, dans la plupart des approches doctrinales, par opposition à la vie publique. Ni dans la législation française, ni dans celle roumaine, il n'y a de définition catégorique de cette notion, les tribunaux appréciant au cas par cas quand nous sommes dans une situation de protection de la vie privée. En systématisant la jurisprudence des tribunaux, les juristes français ont proposé la définition

[550] L. Brisson,"*Le dialogue socratique comme moyen d'accorder l'usage privé du discours à son usage public",* Études platoniciennes, vol.6, 2009. p.55-61.
https://journals.openedition.org/etudesplatoniciennes/764?lang=en
[551] J.S. Black, *Privacy, Ancient and Modern*, Academica, 2014.
https://www.academia.edu/5646291/Privacy_Ancient_and_Modern
[552] Dictionnaire Larousse, *Définition „privé/e"*, consulté le 19.08.2020
https://www.larousse.fr/dictionnaires/francais/priv%C3%A9/64013
[553] Dexonline, *Définition „privat*", consulté le 19.08.2020. https://dexonline.ro/definitie/privat.
[554] G. Cornu, *Vocabulaire juridique*, PUF, 12-e édition, 2018. p.1075

générale suivante du droit à la vie privée : « comme le droit reconnu à chaque personne d'exiger de l'État et des particuliers le respect de la liberté d'action personnelle et du secret des renseignements personnels »[555]. Une définition claire de la notion de vie privée avait été proposée précédemment par Jean Carbonnier[556] : « le respect de la vie privée se traduit essentiellement par un devoir d'abstention : laissez-moi tranquille ».

184. Implication du droit dans la protection de la vie privée. Dans la République de Platon il n'y avait pas de place pour la vie privée, les individus menaient des vies principalement publiques, dans l'agora, dans le forum, et ne ressentaient pas le besoin d'isolement[557]. La protection de la vie privée a été théorisée par des philosophes réputés depuis la première moitié du XIXe siècle, tel fut l'éloge de Benjamin Constant[558] à la liberté privée, considérée comme le fondement de la vie moderne, et par John Stuart Mill[559], qui affirmait que la seule justification pour le retrait dans la solitude est d'éviter tout mal à ceux qui nous entourent. De ces types de théorisations conceptuelles de certains des grands penseurs du XIXe siècle, la vie privée est devenue une préoccupation juridique.

185. Tentatives de délimitation entre public et privé. En ce qui concerne l'évolution du concept de vie privée, il a été montré dans un article publié à la bibliothèque municipale de Lyon[560] qu'il trouve ses racines à la fin de l'époque médiévale. Les notions de « public » et « privé » n'étaient pas bien définies au Moyen Âge, les deux concepts se confondant jusqu'à la fin de cette période historique. La confidentialité était inexistante à l'époque. Dans les sociétés traditionnelles, l'individu, pris dans la solidarité collective, féodale et/ou communautaire, est soumis à une surveillance quasi permanente de son entourage. Il n'a ni ses biens ni son corps, qui peut par exemple être soumis au travail ou à la punition, par décision du supérieur ou par décision collective d'autres membres de la communauté. Le village, la petite ville et le quartier

---

[555] *Op. cit*., pg.688, *Droits de la personnalité*. Une définition similaire se trouve également en JurisClasseur Notarial J.-C. Saint-Pau, *Répertoire V° Vie privée, Fasc. 15 â: Jouissance des Droits civils. „Droit au respect de la vie privée. Consentement à une atteinte à la vie privée"*, Lexis 360 Intelligence, 2017. (dernière mise à jour: 28 février 2024)

[556] J. Carbonier, „*Droit civil, Les personnes*", 21e éd., PUF, Coll. Thémis, 2000. „*Le respect de la vie privée se traduit essentiellement par un devoir d'abstention: laissez-moi tranquille. Cette tranquillité qui est la valeur psychologique protégée, revêt des aspects multiples et concrètement dissemblables*".

[557] E. Tanislav, *Ocrotirea penală a dreptului la intimitate*, nr.3, ed M.of.,1998. p.42

[558] Benjamin Constant (né le 25 octobre 1767 à Lausanne - décédé le 8 décembre 1830) était un penseur, écrivain et politicien français, l'un des premiers penseurs politiques à se qualifier de libéral et aussi d'important doctrinaire du libéralisme du XIXe siècle. Benjamin Constant fut le principal théoricien et fondateur du démocratisme politique libéral de la période française moderne. Sa principale préoccupation était l'analyse de la liberté de l'individu en étroite corrélation avec la Constitution : « *pas de liberté sans la Constitution et pas de Constitution sans liberté* ». Dans son opinion, dans la société moderne, la liberté de l'individu est personnelle, civile et citoyenne, et consiste en son indépendance vis-à-vis de l'État, de l'autorité.

[559] John Stuart Mill (né le 20 mai 1806 – décédé le 8 mai 1973) était un philosophie britannique de l'époque victorienne, l'un des penseurs libéraux les plus influents du XIXe siècle, qui a contribué au développement de l'utilitarisme.

[560] *Vie Privé*, L'Influx, 2013. http://www.linflux.com/monde-societe/droit-justice/vie-privee/# consulté le 19.08.2020

étaient un environnement familier dans lequel chacun se connaissait, s'espionnait, et au-delà duquel s'étendait l'inconnu dans lequel seules les imaginations pouvaient exister dans la sphère de la connaissance.

Dans la Grèce antique, la vie publique des citoyens se déroulait principalement dans l'agora, lieu central de la ville, où étaient discutées les questions politiques, commerciales et sociales. À l'opposé, l'espace privé était représenté par l'*oikos* (la maison), où se déroulait la vie familiale. Par cette séparation entre l'agora et l'*oikos*, les Grecs anciens définissaient deux dimensions fondamentales de l'existence.[561] Une distinction entre public et privé commence à s'opérer plus clairement dans l'ère moderne. Ainsi, la période de la Renaissance est un tournant pour le concept de vie privée. Pour l'historien Alain Corbin[562], la constitution du concept de privé relève d'un grand mouvement qui a commencé à la Renaissance et a vu l'individu s'émanciper de ses vieux liens avec la divinité, donnant libre cours à une préoccupation personnelle non publique. Et pour l'historien Philippe Aries[563], cette période marque le début de la conquête de la vie privée. En étudiant les traités de civilité de l'époque, le sociologue Norbert Elias observe un raffinement de sensibilité appelé pudeur qui conduit à la privatisation de certains actes tels que le moucheron, la défécation, les relations sexuelles, auparavant réalisées en public. Cependant, rappelle l'historien Georges Vigarello[564], au XVIe siècle, dans les châteaux, des pratiques connues aujourd'hui comme ayant un caractère privé, à savoir l'accueil d'amis, la garde d'enfants, la détente, etc., avaient lieu dans la salle de cérémonie. Au XVIIIe siècle, il y a eu un changement.[565] Les premières formes modernes d'intimité trouvent leur origine au XVIIIe siècle, lorsque l'espace intérieur de l'individu devient objet de réflexion, de représentation et de valorisation morale, marquant le passage de la vie privée domestique à une véritable culture des sentiments et du moi.[566] Tout d'abord, la famille est considérée comme un espace devenu plus privé, moins ouvert. Avec l'avènement des lieux dédiés à l'hygiène,

[561] Clermont-Ferrand, *The home : the public use of a private space, from Antiquity to the present day*, journée d'étude, Maison des Sciences de l'Homme 2012. L'article montre cependant que, dans certains contextes, le logement (considéré comme un espace privé) devient un espace à usage public, pour des activités professionnelles, sociales, culturelles ou religieuses, qui se déroulent à l'intérieur.

[562] J.J. Courtine, G. Vigarello(dir.), *Histoire du corps*, Seuil, 2005.

[563] P. Ariès, G. Duby (dir.), *Histoire de la vie privée*, Seuil, 1985 – 1987. Il y a eu cinq tomes qui radiographient ce thème.

[564] J.J. Courtine, G. Vigarello(dir.), *Histoire du corps - Tome 1 - De la Renaissance aux Lumières*, Paris, Seuil, 2011.

[565] J.N. Biraben, Vénard Marc - Bourgeois et paysans au XVIIe siècle. Recherches sur le rôle des bourgeois parisiens dans la vie agricole au sud de Paris au XVIIe siècle. Population, vol. 14(3), 1959, p.579-579.

[566] J.-M. Goulemot, « Tensions et contradictions de l'intime dans les pratiques des Lumières », *Littérales*, « L'Invention de l'intimité au Siècle des Lumières », n° 17, Université Paris X-Nanterre, 1995, p.13. Le siècle des Lumières esquisse une nouvelle forme d'intimité, dans laquelle l'homme tente de concilier le désir d'introspection et le besoin de visibilité : « Le fait semble acquis : le XVIIIe siècle aurait inventé l'intimité ».

nous assistons donc à la constitution d'une intimité psychique et non pas seulement physique. Plus tard, ces pratiques sont devenues populaires parmi les paysans et les travailleurs.[567]

186. L'âge d'or de la vie privée. Le XIXe siècle est, selon de nombreux historiens, l'âge d'or de la vie privée, marquant le moment où l'intimité passe d'une valeur morale de l'intériorité à un espace esthétique et existentiel, dans lequel l'individu affirme sa sensibilité et son identité par l'écriture, la confession et la représentation.[568] Dans la bourgeoisie, la vie privée coïncide avec la cellule familiale qui tend à devenir une entité affective et un refuge pour les individus contre les agressions de la société. Parallèlement, le processus d'individualisation se poursuit grâce aux progrès de l'hygiène et de la médecine. Se déshabiller ou se laver en public devient peu à peu honteux, même parmi les classes ouvrières, et les premiers bains apparaissent à la fin du siècle. Ainsi, le XIXe siècle se caractérise par : l'invention de l'intimité, le désir d'intimité, la scénographie et la morale de l'intimité.[569] Cependant, d'importantes différences subsistent selon la classe sociale. Si dans les milieux bourgeois, le logement se caractérise par une séparation marquée entre les salles d'accueil et les autres, les conditions de vie des paysans ou ouvriers ne leur permettent pas de mettre à l'abri des regards une partie de la maison. L'Etat, puis les associations, ont progressivement traité certaines des questions liées à l'éducation, la santé, l'alimentation, l'hygiène, l'entretien physique, tous ces aspects de la vie personnelle qui étaient jusqu'alors l'apanage des choix individuels. Dans la vision de Hirschman, la vie privée n'est pas en opposition simple avec la vie publique, les deux étant reliées par l'alternance.[570] En d'autres termes, avec le XIXe siècle, la notion de vie privée s'est appréhendée par la possibilité d'entreprendre diverses activités loin des yeux des autres personnes[571].

187. La reconfiguration des frontières de la vie privée au XXe siècle. Le XXe siècle est la période au cours de laquelle des contributions notables ont été apportées à la définition du concept de « droit à la vie privée». Ainsi, Alan Westin définit ce concept comme le droit d'une personne physique, d'un groupe ou d'une institution de décider de manière autonome si et de

---

[567] J.C. Tournand, *Introduction à la vie littéraire du XVIIe siècle*. Paris : Bordas, 2005. L'ouvrage montre comment se dessinent les premières formes de l'intimité moderne : l'accent mis sur soi, sur l'introspection, sur l'individualité. À partir du XVIIe siècle, l'espace privé commence à prendre une forme plus claire, et n'est plus seulement le prolongement de la vie sociale, donnant naissance à l'idée de « retrait dans un espace privé », où la lecture, la conversation et l'écriture prennent de l'importance. À la fin du XVIIe siècle et au début du XVIIIe siècle, la vie privée se trouve dans une période de transition : elle n'est plus purement publique, mais pas non plus complètement séparée, devenant progressivement un espace de formation personnelle.

[568] D. Madelénat, *L'Intimisme*, Paris, PUF, coll. « Littératures modernes », 1989. Le terme « intime » devient, outre un principe moral, un concept fluide, chargé affectivement et variable en fonction des expériences individuelles.

[569] B. Diaz, J. L. Diaz, « Le siècle de l'intime », *Itinéraires. Littérature, textes, cultures*, n° 4, 2009, p. 117-146. À partir du XIXe siècle, l'intimité devient, outre un refuge de la vie privée, un espace de représentation, de création, où l'individu affirme son identité en explorant son propre univers intérieur : « Le XIXe siècle est bien, à plus d'un titre, le siècle de l'intime, celui où l'intériorité devient un objet de culture, un espace à explorer et à représenter ».

[570] A.O. Hirschman, *Bonheur privé, action publique*, L'espace du politique, Fayard, 1983.

[571] M. Ioniță-Niculescu, „Impactul modernității asupra vieții private", in Annales de l'Université Constantin Brâncuși de Târgu Jiu, série Lettres et Sciences sociales, Nr. 2, 2010.

quelle manière, ils communiqueront des renseignements personnels à autrui[572]. Dans le contexte de la vie urbaine moderne, l'espace privé — « chez-soi » — apparaît comme le lieu intime du choix et du retrait, en contrepoint de l'espace public, lieu de visibilité et de rencontres avec des catégories d'âge, de sexe, d'origine sociale et nationale très variées.[573] On constate donc sans équivoque que dans l'idée de vie privée et de son exposition, apparaît la discussion sur le consentement. L'acceptation ou le refus de fournir des renseignements sur les diverses questions liées à la protection de la vie privée commence à être la pierre angulaire du développement du concept de la protection de la vie privée.[574] Certes, donner le consentement d'un citoyen à une autorité pour prendre une décision ou pour établir un rapport juridique n'est pas une nouveauté dans la philosophie politique. Jean-Jacques Rousseau, dans le *Contrat social*[575], développe cette théorie et la soutient précisément afin de promouvoir un système démocratique dans lequel le citoyen est protégé des abus. Comme on le sait, au XXe siècle, l'humanité a pris conscience à grande échelle des façons dont un système politique totalitaire se manifeste par rapport à la vie privée, circonstance qui dénote la fragilité de ce concept. L'élaboration du concept juridique de vie privée ne saurait être dissociée du processus historique de sa mise en visibilité. La diffusion médiatique de l'intimité – d'abord par le livre et l'écrit, puis par la presse et les médias audiovisuels – a participé à la formation de l'intériorité moderne tout en redéfinissant, de manière fluctuante, les frontières du public et du privé. Dès lors, la protection normative de la vie privée au XXe siècle se construit dans une dialectique permanente entre l'exigence d'autonomie individuelle et la tendance sociétale à la médiatisation de la sphère intime.[576]

---

[572] A.F. Westin, *Privacy And Freedom*, Wash. & Lee L., vol.25, 1968. https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20, consulté le 20.08.2020.

[573] C. CALOGIROU, *L'espace du privé, l'espace du public. Frontières et rencontres*, Migrations Société, no. 107, 1996. La distinction entre l'espace privé et l'espace public ne reflète pas seulement une séparation physique, mais aussi une différenciation des rôles sociaux, de la visibilité et de l'interaction. Ainsi, « chez soi » est un lieu de retraite et de libre choix, tandis que « dehors » représente la visibilité, la socialisation, la diversité : « Le chez-soi, espace du privé, par définition espace intime, espace du caché où l'on fait ce que l'on veut, s'oppose la plupart du temps à l'extérieur, espace du public, espace du visible, où se rencontrent des catégories d'âge, de sexe, d'origine sociale et nationale fort variées ».

[574] B. Fauvarque-Cosson (dir.), *La sphère privée : IXe Journées Juridiques Franco-Japonaises*, Société de législation comparée, 2016. https://doi-org.docelec.u-bordeaux.fr/10.3917/slc.fauva.2016.01. L'auteur aborde le concept de vie privée comme un phénomène évolutif, dépendant du contexte culturel et historique de chaque système juridique. En droit français, la vie privée est considérée comme un droit consacré depuis le début du XXe siècle, s'étendant progressivement de la sphère familiale à de nouvelles dimensions, en mettant l'accent sur l'autonomie personnelle et le respect de l'intimité.

[575] J.J. Rousseau, *Du Contrat social, ou Principes du droit politique*, dans *Collection complète des œuvres*, Genève, 1780-1789, vol. 1, in-4.

[576] A. Walch, (dir.), *La Médiatisation de la vie privée, XVe-XXe siècle*, Arras, Artois Presses Université, coll. « Histoire », 2012, p. 264.

Enfin, le XXe siècle représente une période d'extrêmes.[577] D'une part, le droit à la vie privée des individus bénéficie d'un ensemble cohérent de règlements conçus pour assurer une plus grande protection. D'un autre côté, comme la technologie de l'information est en plein essor, les possibilités par lesquelles le droit à la vie privée peut être ignoré sont multiples et les risques que la vie privée d'une personne soit violée sont au plus haut niveau. Nous noterons, dans ce qui suit, le lien entre le développement de la technologie informatique et la mise en péril du droit à la vie privée.[578]

§2. PANOPTIQUE ET COERCITION PSYCHIQUE

188. L'architecture de la visibilité, l'invisibilité du pouvoir : le panoptique.[579] Avant d'aborder les questions liées à la législation relative à la vie privée, il convient de prêter attention à deux concepts qui ont analysé les questions relatives à l'intimité, au contrôle et à la surveillance, afin de mieux comprendre l'importance que la réglementation des ingérences dans la vie privée a sur la qualité de vie du citoyen. Au début, nous prêtons attention au concept de *panoptique*[580], créé et développé par le philosophe et juriste Jeremy Bentham. En réponse à la question qui lui a été posée (« *Qu'appelez-vous surveillance ?* »), Bentham a répondu : un moyen d'obtenir du pouvoir, un pouvoir de l'esprit sur l'esprit. L'auteur, philosophe anglais et fondateur de l'utilitarisme juridique, a consacré ses efforts à la réforme des pénitenciers afin d'obtenir le maximum de résultats grâce à une surveillance beaucoup plus étroite de la conduite des condamnés.[581] De cette façon, la fonction punitive du châtiment semble être plus prononcée que le reste de ses objectifs. Le Panoptique est une figure architecturale qui contient au centre une tour avec un seul superviseur qui peut observer tout le cercle des cellules de détention. En tant que forme d'organisation, le panoptique semble illustrer un projet de société sous la forme d'une utopie. De plus, le superviseur peut facilement observer tout le cercle des cellules, tandis que les détenus ne peuvent pas savoir exactement s'ils sont surveillés à un moment donné.

---

[577] E. Hobsbawm, *L'Âge des extrêmes. Histoire du court XXe siècle*, Bruxelles, Éditions Complexe / Le Monde diplomatique, 1999.
[578] R. Bénédicte, *La Vie privée à l'ère du numérique*, Cachan, Lavoisier, 2012.
[579] M. Porret, « Panoptique », de Jeremy Bentham, *Mensuel*, n° 468, 2020. Concept créé par Jeremy Bentham au XVIIIe siècle comme idée architecturale visant à permettre la surveillance totale des individus, grâce à un mécanisme centralisé, sans qu'ils sachent s'ils sont observés ou non. L'objectif n'est donc pas seulement de surveiller physiquement, mais aussi de créer un état psychologique conduisant à l'autodiscipline. En d'autres termes, le panoptique est l'imaginaire d'une société disciplinaire dans laquelle le pouvoir devient invisible, mais omniprésent.
[580] J. Bentham, *The Panopticon Writings*. Ed. Miran Bozovic, London: Verso, 1995. p.29 – 95.
[581] G. Tusseau, *Jeremy Bentham et le contrôle de constitutionnalité : du refus des formes fortes à l'anticipation des formes atténuées*, Droits, vol. 70(2), 2019, p.139-168. https://doi-org.docelec.u-bordeaux.fr/10.3917/droit.070.0139

Bentham a également déclaré que cette conformation architecturale peut être utilisée dans plusieurs formules, telles que l'école, l'hôpital, la caserne, l'usine, etc.[582]

189. La métaphorisation du panoptique par Foucault.[583] Le deuxième concept qui met en évidence le rôle de la surveillance dans la qualité de vie des individus est celui développé par Michel Foucault.[584] Il reprend le concept de panoptique de Bentham et va plus loin, arguant que dans ce processus de surveillance, la coercition psychique est l'élément essentiel du contrôle[585]. Même si personne n'était dans la tour de la prison circulaire, les prisonniers se comporteraient comme s'ils étaient surveillés directement.[586] Cette façon de contrôler l'individu représente un nouveau niveau d'intrusion dans sa sphère psychique. La simple impression qu'une personne est supervisée conduit à la modélisation de son comportement, et la liberté psychique (le dernier bastion entre l'univers de l'individu et le monde extérieur) disparaît effectivement. Foucault développe également dans son travail les manières dont la supervision a des effets sur l'éducation, le travail, la formation et l'acte médical.[587]

190. Genèse du cadre réglementaire français.[588] Le point de vue français sur ce concept a été exposé pour la première fois dans la loi de 1881 sur la liberté de la presse. Plus tard, la loi no 70 – 643 du 17 juillet 1970 a introduit dans le Code civil français l'article 9 : « chacun a droit au respect sa vie privée ». Cette loi promeut des éléments importants : elle consacre la notion de vie privée et le droit à la vie privée comme un droit subjectif, tente de délimiter la sphère personnelle et établit des mesures de protection appropriées à la disposition du tribunal. Grâce à une jurisprudence vaste et diversifiée générée par les tribunaux français sur la base de l'article 9 du code civil, la protection de la vie privée peut aujourd'hui être réalisée beaucoup

---

[582] M. Perrot, *Les ombres de l'histoire : Crime et châtiment au XIXe siècle*, Paris, Flammarion, 2001, pp. 65-100.

[583] A. Brunon-Ernst, « Les métamorphoses panoptiques : de Foucault à Bentham », *Cahiers critiques de philosophie*, 4(2), 2017, p.61-71. https://doi.org/10.3917/ccp.004.0061. Anne Brunon-Ernst retrace l'évolution et les interprétations données au fil du temps du Panoptique, en décrivant quatre visions successives de celui-ci :
- Panoptique des prisons – pour le contrôle et la discipline des détenus (1791)
- Panoptique des pauvres – une extension du précédent, pour le contrôle et la rééducation des pauvres (1795-1798)
- Panotique chrestomatique – appliqué à l'éducation des enfants des classes moyennes, (début des années 1800)
- Panoptique constitutionnel – proposé comme mécanisme de contrôle des citoyens d'une société (1820-1830).
La surveillance dépasse donc le cadre pénitentiaire et devient un instrument de rationalisation sociale.

[584] M. Foucault, *Théories et institutions pénales. Cours au Collège de France. 1971-1972*, Paris, Éd. EHESS/Gallimard/Seuil, coll. « Hautes études », 2015. Michel Foucault analyse la genèse des formes modernes du pouvoir punitif et la transformation des dispositifs de justice. Il met en lumière le passage d'une justice souveraine, fondée sur la vengeance publique et l'exemplarité du supplice, à une justice disciplinaire, centrée sur la normalisation des comportements. Les institutions pénales – tribunaux, maisons de correction, police, prisons – deviennent les instruments d'un nouveau savoir politico-juridique où la peine ne vise plus à punir le crime comme faute morale, mais à produire des sujets dociles et utiles à la société. Foucault montre ainsi que la rationalisation de la pénalité inaugure un régime inédit de pouvoir, fondé sur la surveillance continue et l'intériorisation de la norme, préludant à la théorie du panoptisme qu'il développera dans *Surveiller et punir* (1975).

[585] M. Foucault, *A supraveghea şi a pedepsi,* Ed. Humanitas, Bucureşti, 1997. p.279 – 315.

[586] O. Razac, *Avec Foucault , après Foucault : Disséquer la société de contrôle*, L'Harmattan, 2008.

[587] P. Poncela, *Avec Foucault, une analyse stratégique des pratiques pénales*, Paris, Dalloz, coll. « Les sens du droit », 2024.

[588] M. Foucault, *Pierre Boulez, l'écran traversé*, in Dits et écrits II. 1976-1988, 2e éd. (1994), Paris, Gallimard, « Quarto », 2001, vol. 2/2.

plus efficacement qu'en Roumanie. Cette jurisprudence a très clairement défini ce qui doit être protégé en matière de droit à la vie privée : résidence, image, voix, données personnelles, vie sentimentale, vie sexuelle, lieu de travail, correspondance, état de santé, etc.

Afin d'assurer une protection accrue du droit à la vie privée, le droit pénal français introduit dans le Code pénal entré en vigueur en 1994 le délit de l'atteinte à la vie privée (art. 368 – atteinte à la vie privée). Dans le Code en vigueur aujourd'hui, modifié, le délit de base, la forme type, se trouve à l'art. 226-1, et les délits assimilés sont définis par l'art. 226-2, 226-3, 226-8.[589]

191. L'émergence de la législation roumaine.[590] Dans la législation roumaine, la notion de vie privée apparaît pour la première fois dans la Constitution de 1991, qui prévoit à l'article 26 para (1er) : « les pouvoirs publics respectent et protègent la vie intime, familiale et privée ». Par la suite, la notion de vie privée est mieux définie par le Code civil entré en vigueur en 2011. Ainsi, l'art. 71, para 1er du Code civil stipule que « toute personne a droit au respect de sa vie privée». Le para (2) du même article stipule que « nul ne peut être soumis à aucune ingérence dans sa vie intime, personnelle ou familiale, ni dans son domicile, sa résidence ou sa correspondance, sans son consentement ou sans observer les limites prévues à l'article 75 ». Dans le même temps, le paragraphe 3 interdit l'utilisation sans consentement préalable, de quelque manière que ce soit, de toute information concernant la vie privée individuelle[591].

L'article 74 du Code civil est beaucoup plus clair en ce qui concerne l'établissement et la définition des atteintes à la vie privée[592], parmi lesquelles : l'entrée non autorisée dans un domicile ou le refuse de partir, l'espionnage auditif ou visuel effectué par la capture d'images ou l'interception de conversations, la surveillance de la vie privée d'une autre personne, la transmission dans l'espace public d'images qui ont été prises dans un espace privé, etc. L'Art.

[589] E. Dreyer, « Existe-t-il une conception pénale de la vie privée ? », in *Archives de politique criminelle*, n° 43, 2021/1, pp. 47-56. Dans cet article, l'auteur part de la construction de la protection de la vie privée autour du droit civil (art. 9 du Code civil) et de la jurisprudence de la CEDH (art. 8), tout en soulignant que le droit pénal joue un rôle déterminant dans la concrétisation de la garantie effective de cette valeur. Le législateur a transformé la vie privée en un bien juridique pénal, dont le contenu s'articule autour des notions d'autonomie de la personne et de liberté d'intimité.

[590] R. Bercea, *Droit privé – Journées italiennes et roumaines de l'Association Henri Capitant*, Fondation Henri Capitant, 2017. Le rapport analyse les décisions de la Haute Cour de cassation et de justice de Roumanie entre 2005 et 2015, afin d'évaluer la manière dont les principes constitutionnels sont invoqués dans les décisions civiles. Il indique que le système roumain de droit privé se trouve dans une phase d'adaptation et de transformation, où les influences et les normes européennes ont des effets tant sur la structure du code civil que sur la méthodologie d'interprétation juridique.

[591] Il est également interdit d'utiliser, de quelque manière que ce soit, la correspondance, les manuscrits ou autres documents personnels, ainsi que les informations de la vie privée d'une personne, sans son consentement ou sans observer les limites prévues à l'art. 75.

[592] F. A. Baias, E. Chelaru, R. Constantinovici, I. Macovei, *Noul Cod civil. Comentariu pe articole*, Bucarest, C.H. Beck, 2012.

74 du Code civil[593] définit très clairement les atteintes à la vie privée : « entrer ou demeurer sans autorisation dans le logement ou en retirer un objet sans le consentement de la personne qui l'occupe légalement ; l'interception illégale d'une conversation privée, commise par tout moyen technique, ou l'utilisation éclairée d'une telle interception; capter ou utiliser l'image ou la voix d'une personne dans un espace privé sans son consentement; diffuser des images montrant les intérieurs d'un espace privé, sans le consentement de la personne qui l'occupe légalement; la surveillance de la vie privée, par tout moyen sauf expressément prévu par la loi ; la diffusion de nouvelles, débats, enquêtes ou rapports écrits ou audiovisuels sur la vie intime, personnelle ou familiale, sans le consentement de l'intéressé ; la diffusion de matériel contenant des images d'une personne traitée dans les établissements de santé, ainsi que des données personnelles sur l'état de santé, les questions diagnostiques, le pronostic, le traitement, les circonstances liées à la maladie et divers autres faits, y compris le résultat de l'autopsie, sans le consentement de la personne concernée et si elle est décédée, sans le consentement de la famille ou des ayants droit; l'utilisation, de mauvaise foi, du nom, de l'image, de la voix ou de la ressemblance d'une autre personne; la diffusion ou l'utilisation de correspondance, des manuscrits ou d'autres documents personnels, y compris des données sur le domicile, la résidence ainsi que les numéros de téléphone d'une personne ou de membres de sa famille, sans le consentement de la personne à qui ils appartiennent ou qui a le droit de s'en disposer, le cas échéant ».[594]

Outre ces dispositions légales, le législateur roumain a également prévu des moyens spécifiques de protection de la vie privée par des moyens civils. La discussion est pertinente à la lumière du fait que certaines interventions dans la vie privée de l'individu ne bénéficient pas de la protection du droit pénal, de sorte qu'elles peuvent être sanctionnées selon le droit civil, par l'implication d'une responsabilité civile délictuelle. Par les dispositions de l'art. 252 du code civil roumain, le législateur a classé la vie privée parmi les valeurs intrinsèques à l'être humain. Selon ces dispositions, toute personne physique a droit à la protection des valeurs intrinsèques de l'être humain, telles que la vie, la santé, l'intégrité physique et mentale, la

[593] Code civil roumain, article 74 – Respect de la vie privée et de la dignité de la personne humaine – Atteintes à la vie privée, partie intégrante de la loi 287/2009.
Les dispositions de l'article 75 délimitent les limites en matière d'atteintes à la vie privée, à savoir :
« (1) Ne constituent pas une violation des droits prévus dans la présente section les atteintes qui sont autorisées par la loi ou par les conventions et pactes internationaux relatifs aux droits de l'homme auxquels la Roumanie est partie.
(2) L'exercice des droits et libertés constitutionnels de bonne foi et dans le respect des pactes et conventions internationaux auxquels la Roumanie est partie ne constitue pas une violation des droits prévus dans la présente section ».

[594] L'analyse des dispositions légales permet de conclure que les faits décrits ne doivent pas être commis en public ou portés à la connaissance du public pour être considérés comme des atteintes à la vie privée d'une personne, susceptibles d'engager la responsabilité civile délictuelle de leur auteur. Voir à cet égard *la décision civile n° 1521 du 12 novembre 2013*, section I civile, Cour d'appel de Timisoara.

dignité, le respect de la vie privée », la liberté de conscience, la création scientifique, artistique, littéraire ou technique. Le titre V du Code civil roumain, dans lequel l'article cité ci-dessus est encadré, établit des moyens efficaces de défense des droits non patrimoniaux, permettant aux justiciables de demander aux tribunaux de prendre des mesures pour protéger la vie privée, dans la mesure où elle est lésée de manière injustifiée. Il peut également être demandé une réparation morale pour le dommage causé par l'acte illicite. Un aspect qui mérite d'être mentionné est le fait que l'art. 255 du code civil roumain permet aux justiciables de saisir la justice en demandant l'adoption urgente de mesures provisoires pour protéger leurs droits non patrimoniaux, y compris le droit à la vie privée, ce qui reflète l'attention accrue du législateur à la protection de la personnalité humaine.

192. Le Code pénal roumain entré en vigueur en 2014 reprend une partie du contenu du délit d'atteinte à la vie privée dans le droit pénal français, trouvant sa définition et ses sanctions dans l'art. 226 du Code pénal.[595]

Comme nous le montrerons ci-dessous, la criminalisation du délit d'atteinte à la vie privée sous la forme que nous trouvons aujourd'hui aux dispositions de l'art. 226 du Code pénal[596], nous le devons à l'intention du législateur de s'aligner sur les rigueurs imposées par l'adhésion de la Roumanie à la « Convention européenne des droits de l'homme »[597]. Conformément à l'article 8 de la Convention, intitulé « *le droit au respect de la vie privée et familiale* » :

1. « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »

2. « L'ingérence d'une autorité publique dans l'exercice de ce droit n'est permise que si elle est prévue par la loi et constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et la prévention des faits pénaux, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui ».

---

[595] A. Boroi, *Drept penal. Partea specială*, Editura C.H. Beck, Bucarest, 2011, p. 145. L'infraction d'atteinte à la vie privée, consacrée par l'article 226 du nouveau code pénal, ne peut être commise, du point de vue subjectif, que de manière intentionnelle. L'aspect subjectif doit également être analysé par rapport à l'élément susmentionné — la commission de l'acte « sans droit » — qui constitue une condition de typicité de l'infraction.

[596] F., Streteanu, *Instituții și infracțiuni în Noul Cod penal*, Facultatea de Tranziție, Bucarest, 2010, p. 227. Dans la littérature spécialisée, il a été affirmé que la structure de l'article 226 du nouveau Code pénal pourrait être interprétée soit comme regroupant plusieurs infractions distinctes, soit comme réglementant plusieurs modalités alternatives de réalisation du même acte. Certaines perspectives qualifient l'infraction de violation de la vie privée d'infraction unique, caractérisée par la pluralité des contenus alternatifs.

[597] J. Callewaert, *L'adhésion de l'Union européenne à la Convention européenne des droits de l'homme*, ed. Du Conseil de l'Europe, 2013.

En outre, la doctrine roumaine a ajouté une troisième condition, tirée de la jurisprudence de la Cour, à savoir celle de la proportionnalité de la mesure restrictive par rapport à l'objectif légitime poursuivi par son instauration.[598]

193. La marge d'appréciation et les obligations positives dans la jurisprudence de la CEDH. Comme le montrent la structure et l'économie des dispositions de la Convention susmentionnée, la vie privée ne bénéficie pas d'une définition exacte, un aspect constaté par la CEDH elle-même dans les arrêts rendus dans les affaires concernant la violation de l'article 8 de la Convention[599]. Ce n'est pas là une lacune de la Convention, mais cela a permis à la Cour de Strasbourg d'élaborer, par sa jurisprudence, des orientations possibles quant au champ d'application du concept, augmentant ainsi l'efficacité de la protection conférée par l'article 8 de la Convention. Ainsi, il a été démontré que « la vie privée » ne peut être perçue uniquement par la notion de « cercle intime », dans lequel une personne vit comme bon lui semble, sans ingérence du monde extérieur. Le respect du droit à la vie privée doit également avoir pour effet de donner à l'individu le droit de se rapporter aux autres[600]. La notion de « vie privée » englobe aussi bien les activités professionnelles[601] que commerciales[602].

Section 2. ATTRIBUTS DE L'EXERCICE DU DROIT À LA VIE PRIVÉE AU MOYEN DE LA TECHNOLOGIE

[598] Corneliu Bîrsan, Convenția europeană a drepturilor omului. Comentariu pe articole, Vol. I Drepturi și libertăți, Éditions All Beck, Bucarest, 2005, p. 34-36.

[599] Voir en ce sens, *l'Affaire Niemietz v. Allemagne,* pt. 29 – „http://hudoc.echr.coe.int/eng?i=001 57887, consulté le 31.08.2021; *l'Affaire Pretty v. Royaume-Uni*, pt. 61 - http://hudoc.echr.coe.int/eng?i=001 60898, consulté le 31.08.2021".

[600] Voir *l'Affaire Von Hannover v. Allemagne,* pct. 95 - „http://hudoc.echr.coe.int/eng?i=001-109029: *l'Affaire Niemietz v. Allemagne*, pct. 29", susmentionnée.

[601] Voir *l'Affaire Fernandez Martinez v. Espagne,* ct. 110 – „According to the Court's case-law, there is no reason of principle why the notion of private life should be taken to exclude professional activities (see *Bigaeva v. Greece, no. 26713/05, § 23, 28 May 2009*, and *Oleksandr Volkov v. Ukraine, no. 21722/11, §§ 165-67, ECHR 2013*)". Restrictions on an individual's professional life may fall within Article 8 where they have repercussions on the manner in which he or she constructs his or her social identity by developing relationships with others. In addition, professional life is often intricately linked to private life, especially if factors relating to private life, in the strict sense of the term, are regarded as qualifying criteria for a given profession (see Özpınar v. Turkey, no. 20999/04, §§ 43-48, 19 October 2010). „Professional life is therefore part of the zone of interaction between a person and others which, even in a public context, may fall within the scope of private life (see Mółka v. Poland (dec.), no. 56550/00, ECHR 2006-IV)" - http://hudoc.echr.coe.int/eng?i=001-145068, consulté le 31.08.2021".

[602] Voir *l'Affaire Satakunnan Markkinaporssi Oy et Satamedia Oy v. Finlande*, pct. 130 –„Leaving aside the numerous cases in which the Court has held that the right to privacy in Article 8 covers the physical and psychological integrity of a person, private life has also been held to include activities of a professional or business nature" (see *Niemietz v. Germany*, 16 December 1992, § 29, Series A no. 251 B) „or the right to live privately, away from unwanted attention" (see *Smirnova v. Russia*, nos. 46133/99 and 48183/99, § 95, ECHR 2003 IX (extracts)". – „http://hudoc.echr.coe.int/eng?i=001-175121, consulté le 31.08.2021".

Cette section traite de l'impact de l'évolution technologique sur la vie privée, en examinant les différentes façons dont les changements et les technologies émergents ont influencé et modifié notre façon de comprendre et de protéger la vie privée.

194. Le processus kaléidoscopique de la définition de la vie privée. Nous vivons dans une société kaléidoscopique : les cultures, les vagues et les identités ont changé.[603] Cette société kaléidoscopique est fragmentée et pose un défi à la protection de l'individu, notamment dans le cas de problèmes globaux éphémères tels que ceux générés dans le domaine de la protection de la vie privée.[604] Cela se produit parce que des groupes de différentes cultures sont créés facilement et rapidement qui soutiennent des valeurs et des identités différentes et souvent conflictuelles. Il y a quelques générations, la culture au sein des sociétés était relativement statique, soutenant les identités collectives et les valeurs partagées par toutes les sociétés. Les identités sociales étaient généralement définies par la famille et le foyer[605], qui représentaient des questions telles que la classe sociale, la religion ou les croyances, et n'étaient généralement pas discutées. Aujourd'hui, cependant, la société a radicalement changé. Dans le monde développé, les sociétés sont devenues de plus en plus diversifiées et les éléments traditionnels qui créent une identité, comme la religion, les groupes socio-économiques, le mariage et le mode de vie, sont devenus beaucoup plus distincts. Cette société kaléidoscopique est interconnectée mais fragmentée en termes de culture, de valeurs et d'identités. Ainsi, si traditionnellement la culture peut être décrite par des catégories, des relations et des contextes bien définies qui permettent de traiter le sens et d'ordonner l'information[606], dans une société kaléidoscopique qui englobe différentes cultures[607], trouver des significations communes devient problématique.

---

[603] L. Fontaine, La pensée kaléidoscopique de Jacques Zylberberg, col. Thélème, Academia, 2021.

[604] M.T, Carlevaris, *Le Kaléidoscope de la vie,* Société des Écrivains, 2016.

[605] F. Guérin-Pace, et al., *En quête d'appartenances*. Ined Éditions, 2009, p. 107-124. https://doi.org/10.4000/books.ined.1013. Dans la société contemporaine, la famille continue d'être un cadre d'appartenance majeur pour l'identité, mais dans un contexte où l'autonomie individuelle s'affirme de plus en plus. La vie privée ne se limite plus au cadre familial, elle concerne également la manière dont l'individu se définit ou assume son identité, en fonction de son statut et de ses conditions sociales.

[606] E. B. Tylor, *Primitive Culture : Researches into the Development of Mythology, Philosophy, Religion, Art, and Custom. Vol. 1.* Londres : J. Murray, 1871. L'anthropologue britannique Edward Burnett Tylor formule l'une des premières définitions scientifiques de la culture.: „*that complex whole which includes knowledge, belief, art, morals, law, custom, and any other capabilities and habits acquired by man as a member of society".* Selon lui, les éléments essentiels de la culture sont les suivants :
- le caractère universel : toutes les sociétés, quel que soit leur niveau technologique ou leur degré de développement, ont une forme de culture.
- la culture s'apprend, elle n'est pas héréditaire : elle se transmet par l'éducation, l'imitation et la vie sociale.
- la culture est un système intégré : des domaines tels que l'art, la religion, l'éducation et la culture sont interconnectés.
- caractère évolutionniste : les sociétés humaines passent par des stades successifs de développement culturel, allant des formes primitives aux formes civilisées.

[607] B. Langlois, *Culture de l'information, culture de l'image et culture par l'image dans l'enseignement secondaire, thèse de doctorat*, l'université de Montpellier 3, 416 pages, 2019.

§1. SIGNES DE L'ÉMERGENCE DU DROIT À LA VIE PRIVÉE DANS LE CONTEXTE DE LA TECHNOLOGIE

195. L'hétérogénéité de l'ère numérique. Ce processus kaléidoscopique a été renforcé par cette technologie moderne qui n'a fourni que les outils qui ont permis aux individus de s'interconnecter au-delà des frontières territoriales et sociales traditionnelles pour former de nouveaux groupes d'intensités beaucoup plus élevées et d'intérêts bien plus profonds.[608] Ainsi, nous vivons dans une société où les gens sont plus que jamais susceptibles d'avoir des identités multiples, selon le contexte qu'ils préfèrent, et de soutenir des valeurs distinctives qui reflètent l'attitude prédominante du groupe spécifique avec lequel ils interagissent à ce moment-là.

Cette diversité est beaucoup plus évidente dans le monde virtuel, et ce n'est que lorsque les gens ont la capacité d'intervenir physiquement à volonté et de développer leur propre personnalité que nous nous posons la question profonde de savoir si le concept même d'identité[609] n'est pas affecté. Les frontières entre le monde physique et le monde virtuel pourraient devenir si froides que les frontières deviendraient floues alors que de plus en plus de gens adoptent cette transition continue et sans faille entre les réalités du monde physique et les réalités du monde virtuel numérique, nous nous demandons si les valeurs culturelles et les attitudes traditionnelles nécessaires sont restées les mêmes.[610]

196. Adaptabilité à l'évolution technologique. Les principes traditionnels tels que ceux spécifiques au droit à la vie privée sont-ils suffisamment flexibles pour être appliqués dans ce cadre d'évolution numérique et technologique ? Bien que la technologie soit bienvenue dans nos vies et nous aide efficacement, les questions restent ouvertes.[611]

---

[608] A. Dahmani, *Les technologies numériques dans les pays en développement. Quel paradigme ?,* Communication, technologies et développement vol. 6, 2018. L'article remet en question l'affirmation selon laquelle la numérisation serait un facteur automatique de progrès et de développement. La technologie n'est pas une solution universelle, son impact dépendant du contexte social, économique et culturel de chaque société. D'autre part, la numérisation risque d'accentuer les inégalités, l'auteur critiquant l'importation de modèles technologiques et économiques occidentaux sans adaptation locale.

[609] B. Gordijn (interview), *EPO Scenarios for the Future*, European Patent Office, EPO Interview, Radboud University Nijmegen, 2007.

[610] M. Hervé. *Décloisonner les identités: Essai sur les enjeux anthropologiques de l'altérité.* Paris : Le Cavalier Bleu, 2024. L'auteur soutient que toute réduction de l'identité diminue l'humanité, qui ne s'épanouit pleinement que dans la relation avec l'autre. Il esquisse le concept d'*homo alterus*, qui construit son identité à travers la relation, le dialogue et l'ouverture à la différence, et non à travers l'isolement, dont dépend un avenir véritablement humaniste.

[611] P. Türk, « L'État plateforme numérique », in *Revue du droit public*, p. 1189-1212, 2020. https://droit.cairn.info/revue-revue-du-droit-public-2020-5-page-1189?lang=fr. À l'ère numérique, un nouveau concept émerge, celui d'« État-plateforme ». Face aux transformations technologiques et numériques, l'État se métamorphose en une « plateforme » de services, de données et de réglementation numériques.

Selon l'époque dans laquelle nous vivons et la conception de l'État, ainsi que l'État dans lequel nous vivons, nous pouvons généralement apprécier que l'individu bénéficie d'une sphère privée dans laquelle il est protégé des intrusions et de la non-transparence.

Ainsi, dans la vision technologique, l'individu est représenté par un fichier informatique lors du traitement de ses données. On estime que la place de l'individu est prise par une « double informatique »[612], conception qui pourrait conduire à l'idée que les possibilités et opportunités offertes par le numérique sont en réalité une surveillance nominale individualisée ou de groupe. Depuis les années '70, la population a pris conscience des menaces que l'évolution de la technologie fait peser sur la vie privée des individus[613], conduisant ainsi à l'affirmation de nouveaux droits et à l'adaptation de ceux qui existaient déjà. En même temps que la sensibilisation, des principes pour une meilleure protection de la vie privée ont été définis dans l'ère technologique, qui ont ensuite été repris dans des textes législatifs comme « Informatique et libertés »[614], dans la directive européenne élaborée en octobre 1995 et dont la transposition aurait dû être votée en France avant octobre 1986[615]. À cette même fin, la France a institué le 6 janvier 1978 par la loi « Informatique, fichiers et libertés », une commission de contrôle et de régulation, appelée Commission nationale de l'informatique et des libertés, qui vise à trouver un compromis entre les différents intérêts contradictoires des administrations, des entreprises et des citoyens.

197. La redéfinition des limites de la vie privée. Le droit à la vie privée est l'un des plus touchés par les transformations technologiques que nous connaissons actuellement. D'origine fondamentale, le droit à la vie privée s'est étendu à un ensemble de facultés qui influencent les sphères patrimoniales et non patrimoniales dans l'espace physique et virtuel.

Au fil du temps, une vaste littérature s'est développée qui a examiné la valeur de la vie privée, avec diverses tentatives pour définir la place du droit à la vie privée.

Bennett, par exemple, fait remarquer que « les tentatives visant à définir le concept de vie privée n'ont généralement pas abouti »[616].

---

612. A. Vitalis, *Informatique, pouvoirs et libertés*, Paris, Économica, 1981. André Vitalis parle volontiers de double informationnel.

613 En octobre 1970, M. Poniatowski a fait une proposition de loi sur la création d'un comité de surveillance et un tribunal de l'informatique. En avril 1974, M. Caillavet en faisait une pour la création d'un directoire et un tribunal de l'informatique.

614 Au niveau juridique, en ce qui concerne la protection des données personnelles, plusieurs textes „*informatique et libertés existent*". Des lois nationales ont été votées dans une bonne trentaine de pays" (cf. www.cnil.fr). „Pour l'Europe, il y a la directive de 1995 mais aussi la Convention 108 du Conseil de l'Europe de 1981. Les lignes directrices de l'OCDE de 1980, les principes directeurs de l'ONU de 1989, les textes de l'OMC du 15 avril 1994 et de l'OIT de 1996 complètent l'arsenal juridique même si ces derniers textes sont peu connus et utilisés.

615 Le CREIS (Centre de coordination pour la recherche et l'enseignement en informatique et société) a fait une comparaison entre la loi de 1978 et l'avant-projet de loi de transposition de la directive européenne de 1995 (cf. www.creis.sgdg.org)

616 C. Bennett, „*Regulating privacy: data protection and public policy in Europe and the United States*", Cornell University Press, vol.25, 1992.

De même, Solove décrit la vie privée comme « un concept en désordre, un concept global qui comprend la liberté de pensée, le contrôle de son corps, la solitude dans son foyer, le contrôle sur les renseignements personnels, la liberté de surveillance, la protection de sa réputation et la protection contre les fouilles et les interrogatoires »[617]. Par conséquent, le concept de vie privée est considéré comme « un parapluie englobant une variété de choses connexes »[618].

Clarke fut le premier à développer une typologie de la notion de privé, en la ramifiant en plusieurs subdivisions : la confidentialité de la personne, la confidentialité du comportement, la confidentialité des données, la confidentialité de communication[619].

198. Les pensées et les sentiments, composantes de la vie privée. De plus, Finn et ses collaborateurs Raab et Wright ont étendu cette liste et ont ajouté comme subdivision du privé, celui des pensées et des sentiments, celui du foyer et de l'identité[620]. Même la Cour européenne des droits de l'homme a une approche pluraliste de la vie privée, soulignant constamment que « la vie privée » est un « terme large qui ne peut pas être défini de façon exhaustive »[621].

A. Naissance du droit à la vie privée dans un contexte numérique

199. La matrice doctrinale américaine. Mais il est incontestable que le berceau du droit à la vie privée à l'ère moderne se trouve aux États-Unis d'Amérique. Le père de l'initiative est Samuel Warren qui, avec Louis Brandeis, a exprimé la première opinion[622] ferme et innovante sur l'impact de la technologie sur la vie intime. Leurs références ont porté sur les questions de l'époque[623], à savoir le besoin de protection de la vie privée face à l'invasion des médias et aux photographies instantanées qui menaçaient de perturber la vie intime, en ce que les aspects personnels et intimes ont été exposés au public sans leur contrôle ni leur consentement.

---

[617] D. Solove, „*Understanding Privacy*", Harvard University Press, 2008. Dans le même ordre d'idées, vous pouvez consulter F. D. Schoeman, „*Philosophical dimensions of privacy: an anthology*", Cambridge University Press, 1984. p.444.

[618] N. Richards, „*Intellectual privacy: rethinking civil liberties in the digital age*", Oxford, 2015. p.9

[619] R. Clarke, „*Introduction to dataveillance and information privacy, and definition in terms*", Roger Clarke's homepage, www.rogerclarke.com

[620] R. Finn, D. Wright, M. Friedwald *Seven types of privacy* en S. Gutwirth, R. Leenes, P. de Hert, Y. Poullet *European data protection: coming of age*, Springer, 2013.

[621] *Niemietz v Germany,* 1996, 16 ECHR 97, para 29; *Peck v United Kingdom*, 2003, 36 ECHR 41, para 57; *Pretty v United Kingdom*, 2002, 35 ECHR 1, para 61.

[622] S.D. Warren, L.D. Brandeis, *The Right to Privacy,* Harvard Law Review, vol.4, no.5, 1890. p.193-220. L'opinion des auteurs sur la vie privée dans le contexte de l'émergence de la technologie est reproduite dans l'essai, qui peut être consultée à https://www.jstor.org/stable/1321160

[623] Les opinions de Samuel D. Warren et de Louis D. Brandeis sont émises en 1890.

Ses idées, perçues comme non-conformistes et novatrices, étaient fondées sur la jurisprudence de l'époque[624] à partir de laquelle S. Warren comprenait qu'avec l'évolution de la technologie, les individus doivent évoluer, militant ainsi pour une législation qui s'adapte au besoin des gens de protéger leur personne. En substance, S. Warren a été parmi les premiers à comprendre que ce n'est pas la technologie moderne elle-même qui pose problème, mais l'absence de législation adéquate qui donnerait aux individus les moyens de se protéger contre les intrusions indésirables.

200. Les thèses fondatrices de Warren sur le droit à la vie privée. S. Warren a aussi été influencé par la loi française[625]_bookmark69, en estimant que le droit à la vie privée, limité comme il devrait l'être, trouve son expression dans la loi française, mais il reste à considérer quelles sont les limites de ce droit à la vie privée, ainsi que les recours qui existent dans son application. S. Warren estime que ces principes devraient être établis à l'avance, de manière préventive, avant que des violations ne se produisent et que l'homme soit lésé, et de façon équitable, avant que la dignité et le confort de l'homme ne succombent aux exigences du bien-être public ou de la justice, sinon, le respect de la vie de l'individu deviendrait une tâche très difficile. Les orientations de S. Warren font partie des premières initiatives qui ont mis les bases de la législation actuelle.

Le premier principe[626] : le droit à la vie privée n'interdit pas la publication d'informations qui sont d'intérêt public ou d'intérêt général.

Le deuxième principe : le droit à la vie privée n'interdit pas la communication de toute information, même si la nature de l'information est privée, tant que sa publication se fait dans des circonstances conformes à la loi sur la diffamation et la calomnie[627].

---

[624] Dans son œuvre, *The Right of Privacy*, Samuel Warren renvoi à l'affaire Yates J. in Militar v. Taylor, 4 Burr. 2303, 2379 (1769), de laquelle il cite à titre de concept : „*It is certain every man has a right to keep his own sentiments, if he He has certainly a right to judge whether he will make them public, or commi only to the sight of his friends*". La citation pourrait se traduire en ce qu'il est certain que chaque homme a le droit de garder intimement ses propres sentiments, s'il veut, c'est certainement que chaque homme a le droit de décider si à eux les rendre publiques ou ne les garder que pour ses amis.

[625] Il s'agit de la loi nommée *Loi relative à la presse du 11 mai 1868*, Rivière, Code Français et Lois Usuelles. App. Code Pén., p. 20 : „*toute Dublication dans un écrit périodique relative à un fait de la vie privée constitue une contravention punie d'une amende de cinq cent francs. La poursuite ne pourra être exercée que sur la plainte de la partie intéressée*".

[626] Dans son essai, S. Warren argumente son principe comme suit : "*Celui-là seul a droit au silence absolu qui n'a pas expressement ou indirectement provoqué ou autorisé l'attention, l'approbation ou le blâme*" - Circ. Mins. Just., 4 Juin, 1868. Rivière Codes Français et Lois Usuelles, App. Code Pen. 20. La direction exprimée montre qu'à l'époque, il existait déjà un concept excluant les investigations agressives du passé de certains hommes populaire, qui jouissaient de publicité. S. Warren intervient et précise que, même si les hommes moins connus ne peuvent pas revendiquer le droit au « *silence absolu* », ils peuvent cependant exiger que tous les détails de leur vie privée (en sens le plus étroit de la notion) ne pas être mis en lumière dans le cas d'une enquête.

[627] S. Warren souligne que la limitation du droit d'empêcher la publication de lettres privées est reconnue depuis 1841, en ce sens l'auteur donne comme exemple l'affaire Story J. en Folsom v. Marsh, 2 Story, 100, 110, 111 (1841), qui la présente comme un argument pro de son principe. Ainsi, les destinataires des lettres privées ont le droit, voire l'obligation, de bénéficier de la possibilité de publier les lettres respectives qui leur étaient adressées, mais uniquement dans les situations où leur publication ou leur utilisation est nécessaire ou justifiée, comme dans

Le troisième principe : la loi ne pouvait accorder aucune compensation pour atteinte à la vie privée par la publication orale d'informations, en l'absence de dommages spéciaux[628].

Le quatrième principe : le droit à la vie privée cesse avec la publication de faits personnels par la personne concernée ou avec son consentement[629].

Le cinquième principe : la vérité des faits publiés ne constitue pas un moyen de défense[630].

Le sixième principe : l'absence de malveillance de la part de l'éditeur ne constitue pas une défense[631].

S. Warren estime que la loi sur la diffamation et la propriété littéraire et artistique est une loi efficace qui peut être donnée comme un exemple d'application, y compris en ce qui concerne une possible atteinte à la vie privée à travers les nouvelles technologies.

Par conséquent, lorsque le droit à la vie privée d'une personne a été violé, celle-ci devrait avoir la possibilité d'intenter des actions en dommages et intérêts dans absolument tous les cas, sans être limitée par un montant minimum de dommages-intérêts. Même dans les cas où il ne serait pas possible d'accorder des dommages spéciaux, une indemnisation substantielle pourrait être accordée pour avoir porté atteinte à ces sentiments. Une autre solution proposée par S. Warren consisterait à appliquer une interdiction, mais seulement dans une catégorie limitée de cas importants.

a). Impact de l'évolution de la technologie sur la vie privée

201. Les nouvelles frontières de la vie privée, dictées par l'évolution technologique. Ce sous-chapitre explore comment l'évolution de la technologie a influencé et modifié la vie

le but de maintenir ou de défendre leur propre droit dans un procès. De même, lorsque le destinataire des informations est publiquement accusé ou diffamé, il a le droit de publier seulement les parties des lettres qui sont nécessaires pour protéger sa réputation et son caractère, mais pas plus.

[628] Ce principe trouve ses racines dans la loi sur la diffamation, en vigueur à l'époque, qui prévoit une responsabilité limitée pour les diffamations faites par des publications orales par rapport à des publications écrites. Ainsi, les blessures résultant de communications orales sont si courantes qu'elles sont considérées comme insignifiantes, et la loi devrait les ignorer complètement dans l'intérêt de la liberté d'expression.

[629] Ce principe représentait, depuis cette époque, une application au droit de la propriété littéraire et artistique. S. Warren montre que cette loi déjà réglementée à l'époque détermine également les situations dans lesquelles une communication doit être considérée comme une publication, à cet égard illustrant qu'une communication ou une circulation privée à des fins limitées ne constitue pas une publication au sens de la loi.

[630] S. Warren motive son principe par le fait que lorsque la loi interdisait l'immixtion dans la vie privée, sans être nécessaire de prouver l'intention criminelle, en fait la loi visait à interdire tout débat de la part de la défense quant à la réalité des faits. L'argument est repris sur la base de l'avis émis par la Circ. Du Ministère de la Justice, le 4 juin 1868, Rivière Code Français et Lois Usuelles, App. Code Pén. 20 n(a).

[631] S. Warren défend son principe selon lequel tant que le délit n'a pas la mauvaise volonté personnelle comme élément criminel, la violation de la personne ou des biens ne l'inclut pas. Ainsi, aucune action en justice ne peut être engagée pour diffamation ou calomnie fondée sur la malveillance personnelle, cette « *attitude personnelle* » ne pouvant être invoquée qu'en réponse à la défense. Ainsi, une éventuelle atteinte à la vie privée doit être protégée peu importe que les raisons qui ont déterminé la personne ayant agi soient coupables ou non.

privée. Cela comprend des discussions sur les effets d'Internet, des médias sociaux, des appareils mobiles et d'autres technologies numériques sur la façon dont nous communiquons, interagissons et protégeons nos informations personnelles.[632]

Le droit à la vie privée est l'un des aspects fondamentaux de la protection des droits de l'homme[633], qui est garanti en Roumanie comme en France. Ce droit est réglementé au niveau des États par leurs constitutions, lois et codes pénaux respectifs. Dans les deux pays, la vie privée est reconnue comme un droit inaliénable, étant protégée par la loi, sa violation pouvant entraîner des sanctions pénales.[634]

202. Constructions législatives en Roumanie. En vertu de la Constitution roumaine, le droit au respect de la vie privée est prévu à l'article 26 : « Les pouvoirs publics respectent et protègent la vie intime, familiale et privée »[635]. Par cet article, la vie privée est consacrée comme un droit fondamental, selon lequel chaque citoyen de la Roumanie est protégé contre toute forme d'intervention qui pourrait être injustifiée des autorités ou d'autres personnes dans leur vie personnelle. La protection pénale de la vie privée est fondée sur l'art. 226 du Code pénal. Les deux dispositions présentées visent à protéger les citoyens roumains contre les intrusions non autorisées dans leur vie privée, telles que l'enregistrement vidéo ou audio, dans un espace privé, sans le consentement de la personne concernée.

203. Constructions législatives en France. En France, la Constitution ne mentionne pas explicitement le droit au respect de la vie privée, celui-ci découlant de la « Déclaration des droits de l'homme et du citoyen » de 1789, qui constitue la base de la Constitution de l'État français. L'article 2 de la Déclaration garantit les droits naturels et inaliénables de l'homme, y

---

[632] *Les nouvelles frontières de la vie privée Droits de la personnalité - Protection des données personnelles*, Actes du Forum Légipresse du 25 septembre 2008. (2009). LEGICOM, (43), https://droit.cairn.info/revue-legicom-2009-2?lang=fr.

[633] F. Crouzatier-Durand, *Fiche 7. Le droit à la vie privée (1) : la protection de la vie privée. Fiches de Libertés publiques et droits fondamentaux : Rappels de cours et exercices corrigés*, p. 63-74. Ellipses, 2017. https://droit.cairn.info/fiches-de-libertes-publiques-et-droits-fondamentaux-3e-edition--9782340016026-page-63?lang=fr. La vie privée est définie comme l'ensemble des relations, activités et éléments personnels qui ne relèvent pas de la sphère publique : intimité corporelle, domicile, correspondance, image, vie familiale, etc. Tant en France qu'en Roumanie, la protection juridique de la vie privée est assurée par :
- des dispositions constitutionnelles et statutaires
- la jurisprudence (Cour constitutionnelle, CEDH) qui clarifie les limites de l'intervention de l'État ou de tiers dans la sphère privée.

[634] *Le juge face aux mutations de la vie privée*, Revue justice actualités, 2025. https://droit.cairn.info/revue-justice-actualites-2025-1?lang=fr.

[635] *Constitution de la Roumanie*, Titre 2 (Article 26, f.a) https://www.cdep.ro/pls/dic/site2015.page?den=act2_1&par1=2#t2c2s0sba22"

compris la liberté, la propriété, la sécurité et la résistance à l'oppression[636]. De plus, en vertu du Code pénal français, le délit d'atteinte à la vie privée est réglementé à l'article 226[637].

La protection de la vie privée comprend également des sanctions pour publication non autorisée d'informations privées. Par exemple, la publication dans les médias ou l'environnement en ligne de données privées telles que des photos, des conversations ou des messages sans le consentement de la personne concernée est considérée comme un délit et est puni en conséquence. En matière de vie privée, la jurisprudence française est très riche et les tribunaux français appliquent souvent des sanctions sévères aux personnes ayant violé ce droit fondamental[638].

Cependant, dans le contexte des progrès technologiques rapides, le droit à la vie privée est confronté à des défis croissants.[639] L'Internet, les réseaux sociaux et les appareils mobiles[640] sont des moyens par lesquels des renseignements personnels peuvent être recueillis[641], souvent sans le consentement des utilisateurs, bien que certaines techniques puissent être illégales. Ainsi, le droit à la vie privée n'est plus seulement un concept juridique, devenant une préoccupation vitale pour les gens.[642]

---

[636] *Declaration of Human and Civic Rights Of 26 August 1*789, Conseil Constitutionnel. consulté le 26 novembre 2024, https://www.conseil-constitutionnel.fr/en/declaration-of-human-and-civic-rights-of-26-august 1789.

[637] *Partie législative (Articles 111-1 à 727-3), Légifrance*. consulté le 26 novembre 2024, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006089684/#LEGISCTA000006089684"

[638] Ibidem.

[639] P. Prokopios, « La règle de droit face aux défis de la technologie », in *Revue du droit public*, 2021. p.801-833. CAIRN.INFO, droit.cairn.info/revue-revue-du-droit-public-2021-3-page-801?lang=fr. Cet article explore les défis posés par les évolutions technologiques rapides, telles que l'intelligence artificielle, la numérisation, l'automatisation des décisions et la surveillance mondiale. Il identifie également les principaux risques, tels que la perte d'autonomie individuelle, l'opacité des décisions et la prolifération des défis transfrontaliers qui compliquent l'application des règles nationales. Il est nécessaire que le droit offre des garanties que la technologie n'érodera pas l'espace privé de l'individu, et la vie privée doit être replacée au centre de la réglementation technologique. En conclusion, l'idée est invoquée que le droit ne peut pas devenir passif face à la technologie : il doit se réinventer, créer des cadres adaptatifs, réagir rapidement, tout en conservant son essence protectrice.

[640] Avis 5/2009 sur les réseaux sociaux en ligne, Groupe de travail « Article 29 » sur la protection des données, WP 163, 2009, p. 4. Les services de réseaux sociaux sont définis comme des plateformes permettant aux utilisateurs de créer un profil public, de se connecter avec d'autres utilisateurs, d'interagir, de partager des informations, des images, etc. Cet avis souligne que la vie privée doit être activement protégée dans le contexte des réseaux sociaux : les utilisateurs ne doivent pas être exposés à des tiers inconnus sans leur consentement éclairé. Elle souligne également que les opérateurs ont des responsabilités claires, ce qui devient un élément important du droit moderne en matière de protection des données.

[641] J. P. Moiny, Facebook au regard des règles européennes concernant la protection des données, REDC, n° 2, 2010.

[642] J. Carbonnier, *Flexible Droit*, LGDJ, 1969. p. 273. Dès les années 60, Jean Carbonnier développait l'idée que le droit ne doit pas être perçu comme un système rigide, mais comme un organisme vivant, capable de s'adapter aux transformations sociales. La « flexibilité du droit » ne signifie pas l'absence de règles, mais la capacité à s'adapter aux réalités humaines. L'auteur affirme que la rigidité juridique rompt le lien entre la norme et la vie, tandis que la flexibilité permet de maintenir l'humanité dans la justice.

b). Protection juridique de la vie privée versus évolution de l'ordinateur[643]

204. L'impact de l'évolution technologique. La numérisation et l'interconnexion mondiale entraînent une multiplication exponentielle des méthodes par lesquelles la vie privée de l'individu subit des intrusions, et les positions géographiques de l'auteur et de la personne concernée deviennent insignifiantes. L'ère du numérique étant essentiellement fondée sur l'ordinateur et les fonctions qu'il remplit, nous nous concentrerons brièvement sur l'évolution de l'ordinateur[644] afin d'illustrer clairement la vitesse à laquelle il a évolué et les possibilités qu'il offre. En même temps, nous pensons qu'Internet joue également un rôle vital à l'époque actuelle et cet aspect ne sera pas négligé dans notre analyse.

De la création du bouclier[645], à l'invention de la première calculatrice mathématique[646] (1623) et à la construction du premier appareil capable de résoudre des opérations plus complexes, le chemin des inventions était relativement lent et ardu. La première génération d'ordinateurs, telle que nous les connaissons aujourd'hui, est apparue vers 1946. Ils traitaient l'information à une vitesse extrêmement lente, occupaient beaucoup d'espace physique et étaient coûteux[647]. Jusqu'en 1980, ces ordinateurs étaient utilisés pour résoudre des équations avec différents degrés de difficulté et pour stocker, dans la mesure du possible, les données saisies manuellement. Ce n'est qu'avec la cinquième génération d'ordinateurs que la véritable révolution technologique commence. Ainsi, grâce à l'invention et à la commercialisation à grande échelle des ordinateurs personnels, des ordinateurs portables et même des téléphones mobiles, les changements dans les technologies de l'information commencent à prendre de plus en plus d'ampleur, et les nouveautés se multiplient d'année en année[648].

205. Développement des réseaux informatiques. Dès 1950, les moyens par lesquels un ordinateur pouvait être relié à un autre ordinateur pour échanger des informations entre eux ont

---

[643] A. Jammet, *La Prise en Compte de la Vie Privée dans l'Innovation Technologique*, Droit, Université de Lille, 2018. Français. De nombreux articles sur ce sujet cherchent à répondre à la question suivante : « Quelle est l'efficacité réelle du régime de protection de la vie privée dans le contexte de l'innovation numérique ? » La protection juridique existante est importante, mais insuffisante pour garantir la vie privée dans le contexte de l'innovation rapide. L'un des points centraux de l'ouvrage cité est le décalage entre la confiance de la société dans la capacité de la technologie à respecter la vie privée et l'efficacité du cadre réglementaire. L'auteur suit le « parcours juridique » de la protection de la vie privée depuis sa conception initiale jusqu'aux adaptations législatives, en passant par sa mise en œuvre et les obstacles rencontrés.

[644] V. Fauchoux, J. M. Bruguière, P. Deprez, *Le droit de l'Internet, lois, contrats et usages*, 2e éd., LexisNexis, 2013, p. 7.

[645] C. Gîrbea, *Le bouclier dans l'imaginaire médiéval : Les fonctions symboliques du bouclier,* Paris : Classiques Garnier, 2024. En plus d'être une pièce d'armure, le bouclier est un symbole culturel complexe qui représente la protection, l'identité, la frontière entre la vie et la mort, entre le public et le privé.

[646] Encyclopædia Britannica. (s.d.). Pascaline, Encyclopædia Britannica en ligne. La Pascaline est la première machine à calculer commercialisée et largement utilisée, conçue par Blaise Pascal entre 1642 et 1644. Elle marque le début de l'ère des machines à calculer mécaniques et est à l'origine de l'évolution des ordinateurs modernes.

[647] D. Pianeta, *Histoire de l'informatique : Tome 1 – Les histoires.* Édition 2020.

[648] *History of Computer*, T point Tech, 2020. https://www.javatpoint.com/history-of-computer. consulté le 24.08.2020

été mis en œuvre. Les premières entités à bénéficier de tels réseaux étaient sous l'égide du gouvernement américain, notamment dans le domaine de la défense nationale. À partie des années 1980, les réseaux informatiques sont devenus accessibles au grand public et la commercialisation de l'Internet ne tarde pas apparaître.[649] Le développement des réseaux informatiques a inévitablement conduit au développement de la technologie avec laquelle les ordinateurs ont été équipés, devenant d'année en année plus rapides, plus puissants et plus complets dans la mémoire. Partant des réseaux locaux, Internet s'est développé en réseaux régionaux, nationaux puis internationaux, réduisant ainsi la distance entre les individus. Depuis les premiers sites dédiés au dialogue à Facebook, Twitter ou Instagram, l'évolution de la connexion des ordinateurs aux réseaux internet a connu une vitesse fulgurante, et actuellement, tout individu peut être connecté à un réseau haut débit tant qu'il a un ordinateur dans sa main, que ce soit sous la forme d'un smartphone[650].

L'évolution technologique particulièrement soudaine et complexe a inévitablement donné aux droits de l'homme une valence moderne.[651] Le droit à la vie privée était aussi nécessairement soumis à cette modernisation, et les risques que des erreurs ou abus potentiels peuvent présenter à l'interconnectivité atteinte ont conduit à l'adoption des premières formes de réglementation établissant les garanties de protection juridique du droit à la vie privée[652]. Le développement continu des techniques par lesquelles l'information est reçue, récupérée, stockée et transmise a créé la nécessité de réglementer de nouvelles situations qui donneraient inévitablement lieu à des relations juridiques pour lesquelles les anciennes règles ne suffisaient plus.

c). Convention pour la protection des données personnelles

206. Reconfiguration du cadre législatif relatif à la vie privée. Dans le contexte de la nouvelle ère, il a été jugé impératif d'adopter des règles internationales qui régissent notamment les relations juridiques découlant de l'utilisation de l'information par ordinateur. Ainsi,

---

[649] P. Le Tourneau, *Contrats du numérique : informatiques et électroniques 2025-2026,* 13e éd., Dalloz, 2025. La commercialisation de l'Internet impose une redéfinition des concepts contractuels, exigeant une attention accrue à la protection de la vie privée. Bien que le droit commun des contrats reste le fondement, la spécificité technique de l'environnement numérique impose des adaptations significatives des règles juridiques. La vie privée, les données personnelles, le profilage et les services en ligne sont intrinsèquement liés aux contrats numériques, leur compréhension est donc essentielle pour la protection de la vie privée à l'ère numérique.

[650]K. Robert, D. M. Aaron, "*Internet"*, Encyclopedia Britannica, 2020. https://www.britannica.com/technology/Internet/Foundation-of-the-Internet consulté le 24.08.2020

[651] M. Atias, D. Linotte, *Le mythe de l'adaptation du droit au fait*, Recueil Dalloz, Chronique et législation, 1977, chron. XXXIV, p. 254. La capacité des normes juridiques à refléter les faits et les besoins sociaux est remise en question.

[652] S. Șandru, *Protecția datelor personale și viața privată*, Ed. Hamangiu, Bucarest, 2016. p.117

l'Organisation de coopération et de développement économiques (OCDE) a adopté en 1980 une série de pratiques sous la forme d'un guide pour la protection des données à caractère personnel et, implicitement, de la vie privée[653]. Sur la base de ce guide, le Conseil de l'Europe a élaboré et adopté, au cours de l'année suivante, « la Convention sur la protection des données à caractère personnel »[654]. Compte tenu de ces nouveaux actes élaborés spécifiquement pour régir les situations survenant lors du traitement des données à caractère personnel, la CEDH a développé une pratique particulière, appliquant les principes qui sous-tendent la protection de la vie privée dans les cas ayant pour objet le traitement de données à caractère personnel dans la nouvelle ère numérique.

En adoptant, pour la première fois, un acte normatif contragnant pour les États membres de l'Union Européenne[655], la protection de la vie privée devient de plus en plus importante dans l'espace européen. La directive 95/46/CE établit, à titre indicatif, un ensemble de règles que les États membres doivent mettre en œuvre pour réglementer le traitement des données à caractère personnel au niveau national et interétatique.[656] Inévitablement, la mondialisation a conduit à un élargissement des horizons de communication, mais aussi à un « aplatissement » de la Terre, situations qui ont eu des conséquences directes sur la façon dont la vie privée des individus est engagée en diverses relations juridiques. En référence à l'actuel règlement européen sur « la protection des données personnelles », actuellement en vigueur, nous renvoyons au « Règlement 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 » (RGPD) « relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE ». Cette fois-ci, compte tenu des différences dans le caractère contraignant des différents actes normatifs européens, les données personnelles des personnes physiques sont protégées au moyen de l'acte législatif ayant le plus grand pouvoir coercitif – le règlement.[657]

d). Datafication, les algorithmes influencent de manière décisive la liberté de choix

[653] *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OCDE, 1980. Disponible https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm consulté le 25.08.2020

[654] *Convention du 28 janvier 1981, de protection des personnes face au traitement automatique des données à caractère personnel*, Conseil de l'Europe, Strasbourg, 1981.

[655] J. Tricot, « Droit de l'Union européenne », in *Revue de science criminelle et de droit pénal comparé*, vol. 4(4), p. 909-945, 2019. https://doi.org/10.3917/rsc.1904.0909.

[656] J. Frayssinet, « La régulation des données personnelles », in *LEGICOM*, vol. 42, 2009. https://droit.cairn.info/revue-legicom-2009-1?lang=fr.

[657] B. Haftel, « Protection des données personnelles : autorité de contrôle compétente et loi applicable », in *Revue critique de droit international privé*, vol. 2(2), 2016, p. 377-387. https://doi.org/10.3917/rcdip.162.0377.

207. Modélisation de la réalité et des interactions sociales. La datafication[658] est un concept par lequel divers aspects de la vie quotidienne sont transformés en données quantifiables, générant une grande quantité d'informations[659] qui peuvent être collectées, analysées et utilisées par les organisations et les entreprises. Le terme a été introduit par Viktor Mayer-Schonberger et Kenneth Cukier dans l'œuvre "*Big Data : A Revolution That Will Transform How We Live, Work and Think"*. Selon les auteurs, grâce au processus de collecte et d'analyse, toute action sociale est transformée en données quantifiées qui aident au suivi et à l'analyse prédictive en temps réel[660]. Dans le contexte technologique actuel, chaque interaction que l'homme a avec l'environnement numérique génère des données.[661] Il s'agit notamment de la navigation sur Internet, de l'utilisation d'applications mobiles ou de toute activité physique impliquant l'utilisation d'un appareil. Ce concept est également discuté par Mirko Tobias Schafer et Karin Van Es, dans l'œuvre « *The Datafied Society : Studying Culture through Data* », les auteurs analysant comment le datafication influence la culture et la société, ce concept affectant à la fois les entreprises et les individus, en transformant la façon dont les gens interagissent avec la technologie[662].

En tant que pratique, la datafication a un impact majeur sur la vie privée et les interactions sociales, par la façon dont chaque individu traite ses données personnelles et comment elles peuvent être utilisées. L'un des effets les plus négatifs du processus de datafication est l'augmentation des risques liés à la vie privée des utilisateurs. Dans le livre « The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power », Shoshana Zuboff explique comment les entreprises technologiques travaillent, non seulement en recueillant un volume de données pertinent, mais aussi en les analysant pour créer un profil spécifique pour chaque utilisateur. En ce sens, les entreprises ont la capacité de prédire le comportement et les préférences d'un utilisateur, influençant indirectement ses choix sans qu'il soit conscient de la manipulation. Zuboff souligne que cette pratique crée « une économie

---

[658] M. Lycett, *'Datafication': Making sense of (big) data in a complex world*, European Journal of Information Systems, vol. 22, 2013.

[659] I. Aimé, F. Berger-Remy, M.E. Laporte, *The brand, the persona and the algorithm : How datafication is reconfiguring marketing work*, Journal of Business Research, vol. 145, 2022, pp. 814-827. La datafication n'est pas une simple collecte de données, mais une reconfiguration socio-matérielle des activités quotidiennes. Dans ce contexte, la notion d'individu peut perdre de sa pertinence, remplacée par des unités d'analyse – groupes, profils, métadonnées – qui réduisent la singularité de la personne.

[660] V. Mayer-Schönberger, K. Cukier, *Big Data: A Revolution That Will Transform How We Live*, *Work, and Think*", Houghton Mifflin Harcourt, 2013.

[661] J. Ortiz-Freuler, *Datafication, Identity, and the Reorganization of the Category Individual*, Temple Law Review, Vol. 65, No. 4, 2023. Available at SSRN: https://ssrn.com/abstract=4501828. Cet article analyse comment les processus de numérisation et de datafication mettent sous pression l'individu et ses droits fondamentaux. L'auteur soutient que, à mesure que les données deviennent un moyen de segmentation, de regroupement et d'analyse, les concepts traditionnels d'identité individuelle deviennent vulnérables.

[662].M.T. Schäfer, E. Karin, *The Datafied Society. Studying Culture through Data.,* Amsterdam University Press, 2017.

de surveillance », dans laquelle toutes les entreprises ont la possibilité de profiter des données d'un utilisateur afin de maximiser leurs revenus, sans tenir compte des aspects éthiques et juridiques de la vie privée et du contrôle personnel[663].

e). La collecte de données personnelles influence le comportement humain

208. Effets comportementaux de la collecte de données personnelles.[664] En outre, comme mentionné précédemment, la datafication implique indirectement la manipulation du comportement humain, ce qui est également abordé par Kate Crawford et Meredith Whittaker dans le rapport *AI Now Report 2018*. Les auteurs expliquent comment des algorithmes basés sur des données collectées auprès des utilisateurs peuvent influencer ce même utilisateur[665]. Par exemple, les algorithmes peuvent identifier le type de contenu médiatique qu'un utilisateur consomme quotidiennement, de sorte que le même type de contenu lui est davantage promu, étant exposé uniquement à un certain type d'information, en fonction des convictions existantes. Cette pratique est également connue sous le nom de « bulle de filtre » et limite la perspective et la diversité d'opinion de chaque utilisateur. Ainsi, la polarisation sociale peut être atteinte, chaque personne ayant une opinion bien établie sur un certain sujet qui peut être débattu et controversé. La datafication peut également contribuer à perpétuer l'inégalité sociale, un fait analysé par Cathy O'Neil dans son livre « *Weapons of Math Destruction : How Big Data Increases Inequality and Threatens Democracy* » (2016), illustrant comment les algorithmes sont utilisés dans divers domaines, tels que l'éducation, la santé et la justice, peuvent amplifier de façon significative les préjugés sociaux existants ou développer certains préjugés. L'autrice fait valoir que les modèles basés sur des données peuvent discriminer certains groupes sociaux, par exemple les minorités raciales, en appliquant des critères qui ne tiennent pas compte du contexte social actuel[666]. Par exemple, les algorithmes qui évaluent le risque de récidive peuvent

---

[663] S. Zuboff - *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Social Forces, vol.98, issue2, 2019.
https://www.academia.edu/43229446/Shoshana_Zuboff_The_Age_of_Surveillance_Capitalism_The_Fight_for_a_Human_Future_at_the_New_Frontier_of_Power.

[664] J. A. Castañeda, F.J. Montoro, *The effect of Internet general privacy concern on customer behavior*, Electron Commerce Res vol. 7, p. 117–141, 2007.

[665] AI Now Institute, „*AI Now 2018 Report*", AI Now Institute (blog), 2018. https://ainowinstitute.org/publication/ai-now-2018-report-2. Le rapport présente une analyse interdisciplinaire des implications sociales, économiques et politiques de l'intelligence artificielle. Il examine également la vulnérabilité de la vie privée face aux outils numériques d'automatisation : collecte de données personnelles, profilage, décisions automatisées, extension de la reconnaissance faciale.

[666] C. O'Neil, "*Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*", Crown, 2016.

utiliser des données historiques qui reflètent des préjugés sociaux généralement acceptés par un certain modèle de population.[667]

f). Les réseaux sociaux ont créé une extension virtuelle du soi

209. Les réseaux sociaux, moyen de collecte de données personnelles. Facebook, Instagram et X(Twitter) sont quelques-uns des plus grands réseaux sociaux actuels, mais aussi certains où la datafication est activement utilisée.[668] Ces plateformes recueillent un large éventail d'informations sur les utilisateurs, y compris des renseignements personnels, des interactions sociales et des comportements de navigation et de recherche des utilisateurs. Tarleton Gillspie, dans le livre « Custodians of the Internet : Platforms, Content Moderation and the Hidden Decisions That Shape Social Media » (2018), discute à la fois des avantages que les plateformes de médias sociaux apportent, ainsi que de la quantité de données qui sont collectées pour personnaliser le contenu et la publicité de chaque utilisateur[669]. De plus, les plateformes de commerce électronique comme Emag ou Amazon utilisent le processus de datafication pour améliorer l'expérience d'achat en ligne de chaque utilisateur. Ils utilisent la datafication afin de collecter des données sur l'historique des commandes et les préférences des utilisateurs. De cette façon, les entreprises de e-commerce utilisent des données pertinentes pour personnaliser leurs offres et anticiper les besoins de chaque client utilisant la plateforme[670].

---

[667] D. Kaplan, *Informatique, libertés, identités.* Paris : FYP Éditions, 2010. Daniel Kaplan est le fondateur de la Fondation Internet Nouvelle Génération (FING) et fait partie de la première génération de penseurs français à avoir abordé le sujet de l'impact d'Internet sur la société d'un point de vue éthique, juridique et sociologique. L'ouvrage cité met en évidence la tension entre deux réalités : d'une part, la liberté des individus de s'exprimer et de se projeter dans l'environnement numérique, d'autre part, les risques de surveillance, de profilage, de perte de contrôle sur les images et les données personnelles. Kaplan observe que, bien que les utilisateurs exposent activement leurs données personnelles et s'« auto-exposent » dans l'espace numérique, ils ne contrôlent pas la manière dont ces données sont utilisées par les utilisateurs commerciaux ou administratifs, ce qui les rend vulnérables. En d'autres termes, l'auteur remplace l'ancienne question de savoir comment protéger le citoyen contre l'État surveillant par une question contemporaine : comment protéger l'individu contre sa propre exposition numérique ? L'auteur propose ensuite une approche qui met l'accent sur la compétence individuelle : l'utilisateur doit protéger sa propre identité numérique en s'impliquant activement dans sa gestion.

[668] M. Vanvlasselaer, *Un avenir commun au sein de la société numérique,* Mémoire de Master 2, 2025. L'auteur analyse les transformations apportées par les nouvelles technologies et la manière dont les données personnelles sont devenues des ressources informationnelles abondantes, que l'homme ne peut traiter dans leur intégralité. Des plateformes telles que Facebook, YouTube ou Google agissent comme des filtres, sélectionnant et suggérant des contenus, prenant ainsi le contrôle des flux informationnels et influençant les préférences et les comportements des utilisateurs.

[669] T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*, Yale University Press, 2018. consulté 26 noiembrie 2024, https://www.researchgate.net/publication/327186182_Custodians_of_the_internet_Platforms_content_moderation_and_the_hidden_decisions_that_shape_social_media.

[670] F. Provost, T. Fawcett, "*Data Science and its Relationship to Big Data and Data-Driven Decision Making*", Big Data 1, nr.1, 2013. p.51–59 https://doi.org/10.1089/big.2013.1508.

Ainsi, la datafication est un processus complexe qui a redéfini comment chaque personne interagit avec la technologie, mais aussi comment il gère ses données personnelles. En fait, le datafication apporte à la fois des aspects positifs et négatifs, étant très important de savoir comment ce phénomène croissant est utilisé. En ce sens, le principal défi qui reste à relever est de trouver un équilibre entre les avantages offerts et la protection des droits individuels concernant les informations personnelles de chaque utilisateur. Il est essentiel que les utilisateurs et les autorités prennent conscience de l'impact des données collectées, et qu'une culture de responsabilité et de transparence dans leur utilisation soit principalement promue.

210. L'exposition numérique selon Harcourt. L'œuvre « Generalogy du Doppelganger numérique » analyse comment le développement technologique a généré un double numérique de chaque personne, une construction numérique qui évolue et développe sa présence parallèlement à notre identité physique. Ce « double » est alimenté par des données personnelles collectées lors de nos interactions numériques, telles que l'utilisation des réseaux sociaux, les transactions en ligne ou les recherches sur Internet. Au fur et à mesure que la technologie progresse, ce double devient de plus en plus autonome, représentant une extension virtuelle du soi qui peut être utilisée à des fins diverses, parfois sans le consentement de l'individu[671]. Cette situation change profondément la perception de la vie privée, en changeant les frontières entre ce qui est personnel et ce qui est public.

g). « Double numérique » – la vie privée devient une ressource exploitable

211. Prédiction des comportements et influence sur les décisions.[672] Un aspect essentiel abordé par l'auteur est le manque de contrôle des individus sur leur propre « double numérique. » Les données collectées sont souvent traitées et utilisées par des tiers, tels que des entreprises technologiques, des agences gouvernementales ou même des pirates informatiques. Ce phénomène met la confidentialité en danger, car le double numérique peut être utilisé pour prédire des comportements, influencer des décisions ou créer des profils qui ne reflètent pas

[671] B. Harcourt, *5.Généalogie du Doppelgänger numérique. La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.125-149. shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-125?lang=fr.

[672] J. Cestac, T. Meyer, *Des attitudes à la prédiction du comportement : le modèle du comportement planifié, La psychologie sociale : applicabilité et applications*, édité par Pascal Morchain et Alain Somat, Presses universitaires de Rennes, 2010. Les auteurs proposent de présenter le « modèle de comportement planifié », un modèle cognitivo-social de prédiction des comportements basé sur des données psychosociales. Dans l'environnement numérique, ces variables sont manipulées ou modélisées en analysant les préférences extraites de l'activité en ligne des individus. Ainsi, dans l'environnement en ligne, les algorithmes peuvent personnaliser le contenu en fonction de nos données (clics, recherches, historiques de visionnage, etc.). Les données collectées servent de matrice psychologique pour prédire les attitudes futures et influencer les décisions.

toujours la réalité.[673] L'évolution de cette technologie a transformé la protection de la vie privée en un défi[674], dans lequel les individus se sentent souvent impuissants face aux entités qui contrôlent leurs données[675].

212. Symbiose entre le matériel et l'idéel. De même, dans son ouvrage anthropologique, Maurice Godelier montre qu'il n'y a pas de rupture entre le plan matériel et le plan idéel, mais un lien de co-création : les instruments et les technologies produits par l'homme ne sont pas neutres, mais portent l'empreinte des conceptions et des valeurs qui les ont générés, devenant ainsi des supports à travers lesquels ces idées se perpétuent et se transforment.[676]

Dans ce contexte, le document met en évidence comment les technologies modernes, bien qu'elles offrent des avantages importants tels que l'accès rapide à l'information ou la personnalisation des services, créent un déséquilibre entre les utilisateurs et les entités qui gèrent leurs données.[677] L'émergence du double numérique illustre un changement fondamental dans la relation entre l'individu et la technologie[678], faisant de la vie privée une ressource exploitable.[679] Cette dynamique souligne le besoin de certaines réglementations claires et efficaces qui protègent l'identité numérique et assurent un meilleur contrôle sur l'utilisation des données personnelles[680].

§2. EFFET DES CHANGEMENTS TECHNOLOGIQUES SUR LA VIE PRIVÉE

[673] A. Deslée, *La vie privée en ligne: utopie ou réalité ? Comprendre la vulnérabilité perçue relative aux données personnelles,* Décisions Marketing, vol. 111(3), 2023. p.11-37. https://doi.org/10.3917/dm.111.0011. Cet article examine la vulnérabilité des utilisateurs en matière de données personnelles et ses conséquences sur leur comportement en ligne. Sur la base d'entretiens avec des consommateurs et de discussions avec des professionnels du marketing numérique, l'auteur identifie les principales causes de cette vulnérabilité : méconnaissance des risques, absence de contrôle effectif et transparence limitée du processus de collecte des données.

[674] T. Bizet, *Vers La Fin De La Vie Privée? Les Données Personnelles à l'Ère Des Big Data*, Privacy law, Academia.edu.

[675] Ibidem

[676] M. Godelier, *L'Idéel et le matériel, Pensée, économies, sociétés,* Paris, LGF, 1992. Maurice Godelier explore la relation entre le monde des idées (ce qui touche au symbole, à la croyance, à la représentation) et celui des réalités matérielles (production, économie, organisation sociale). Il montre que ces deux dimensions ne peuvent être séparées, mais fonctionnent dans une interdépendance contraignante. Dans les sociétés contemporaines, ce lien se manifeste également dans l'univers numérique, où les données, les algorithmes et les flux d'informations sont à la fois des constructions techniques et des projections des valeurs et des idéologies humaines.

[677] Y. El Yahyaoui, *Chapitre troisième. Les plateformes numériques « globales » : puissance et abus de position. Économie des plateformes numériques : Captation de la valeur, pouvoir de marché et communs collaboratifs*, L'Harmattan, 2021, p. 149-201. https://shs.cairn.info/economie-des-plateformes-numeriques--9782343231280-page-149?lang=fr.

[678] L. Matosas- Lopez, *The Impact of Digitalization on Current Marketing Strategies,* Emerald Publishing Limited, 2024.

[679] N. Hassani, *Le Paradoxe De La Protection Des Données Personnelles à l'Heure De La Libre Circulation Des Informations*, Terminal, OpenEdition, 2019.

[680] Ibidem ref. 666.

Cette section traite des effets directs du changement technologique sur la vie privée.[681] Il examine des questions telles que l'impact de l'automatisation, de l'intelligence artificielle et de big data sur la confidentialité et la sécurité des données, et comment ces technologies modifient l'équilibre entre les droits individuels et l'intérêt public ou commercial.

213. Apparition des algorithmes, impact sur la manière de collecter les données. Ces dernières années, les progrès technologiques ont facilité le traitement des données collectées, analysées et utilisées à diverses fins. Cukier et Mayer-Schonberger appellent cette période « Big Data », chose qui marque un changement fondamental dans la façon dont les organisations et les gouvernements gèrent leurs données personnelles. L'émergence des algorithmes et le développement de l'infrastructure numérique ont permis la collecte et l'analyse de données à un niveau majeur[682]. Cette collection ne se limite pas uniquement aux interactions en ligne, telles que les réseaux sociaux ou les moteurs de recherche. Étant un environnement numérique interconnecté, tout appareil connecté à Internet contribue continuellement à cette collecte de données. Les données de navigation, la location GPS et les comportements d'utilisation des applications sont enregistrés, analysés et souvent vendus ou distribués à des tiers[683].

214. Capacité à créer un profil numérique. En outre, le processus de numérisation continu a donné aux entreprises la possibilité de créer un profil numérique détaillé de chaque utilisateur à travers les données obtenues. Mark Andrejevic illustre la façon dont les données obtenues par les entreprises aident à créer un profil d'utilisateur, mais aussi à effectuer une analyse comportementale de l'utilisateur dans l'environnement en ligne. Grâce à ces profils, les entreprises peuvent personnaliser les expériences numériques et les publicités que chaque utilisateur voit[684]. Par exemple, les réseaux sociaux peuvent afficher du contenu en fonction des intérêts ou des comportements passés d'un utilisateur, ou recommander des personnes susceptibles d'être connues en fonction de leurs abonnés communs.[685] En outre, les plateformes commerciales peuvent suggérer des publicités pertinentes en fonction de l'historique de recherche précédent ou des achats antérieurs. La prolifération comportementale peut apporter des avantages, compte tenu de la fourniture de contenus pertinents, ainsi que des inconvénients, du fait des abus que peuvent commettre certaines entreprises. L'un des exemples les plus

---

[681] B. REY, *La vie privée à l'ère du numérique*, Paris, Hermès-Lavoisier, coll. « Traitement de l'information », 2012.
[682] V. Mayer-Schönberger, K. Cukier, *Big Data : A Revolution that Will Transform how we live, work and think*, Houghton Mifflin Harcourt, 2012.
[683] Ibidem
[684] M. Andrejevic, "*Infoglut: How Too Much Information Is Changing the Way We Think and Know*", Routledge, 2013. https://doi.org/10.4324/9780203075319.
[685] C. Gallic, R. Marrone, *Chapitre 18. La publicité sur les réseaux sociaux. Le Grand Livre du Marketing digital*, Dunod, 2023, p. 425-446. https://shs.cairn.info/le-grand-livre-du-marketing-digital--9782100851133-page-425?lang=fr.

notables est le scandale entre Facebook et Cambridge Analytica en 2018[686], lorsque la société Facebook a été accusée de collecter des données à l'insu des utilisateurs[687].

A. Conséquences sociales et juridiques du développement technologique[688]

Cette section traite des conséquences sociales et juridiques du développement technologique sur la vie privée.[689] Il comprend l'analyse de l'impact sur la législation en matière de protection des données, le besoin d'équilibrer l'innovation technologique avec les droits à la vie privée et les effets sur la société dans son ensemble, y compris sur des questions telles que la liberté d'expression, la démocratie et l'égalité.

a). Surveillance omniprésente[690] - concurrence entre l'État et les entreprises

215. La vulnérabilité de la confidentialité face à l'évolution technologique. Le développement technologique accéléré a créé des conséquences importantes pour la protection de la vie privée, au-delà de la simple vulnérabilité de la confidentialité. Le chapitre souligne

[686] C. Pérez Lagos, « Rendre visibles les conséquences de la surveillance numérique : Le cas du "scandale" Cambridge Analytica », in *Communication*, vol. 37, n° 2, 2020. https://doi.org/10.4000/communication.13252. Le scandale Cambridge Analytica a mis en lumière, dans les médias, les mécanismes invisibles de la surveillance numérique et de la collecte massive de données personnelles. Bien que les utilisateurs aient été perçus comme les victimes d'une trahison de confiance, cela n'a pas entraîné de véritable transformation des pratiques numériques. L'enjeu n'est donc pas seulement de révéler ces pratiques, mais aussi la capacité démocratique à les interpréter, à les réglementer et à limiter leurs effets sur l'autonomie individuelle.

[687] „*Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, The New York Times, 2018. consulté 27 novembre 2024, "https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal fallout.html

[688] J. Guilhem (dir.), *Sciences et sens de l'intelligence artificielle*, Paris, Dalloz, coll. « Thèmes & commentaires », 2020. Cet ouvrage est le résultat d'un colloque scientifique organisé en 2019, dont le thème principal était l'intelligence artificielle et sa signification. Les conclusions soulignent qu'une approche purement technique du développement technologique n'est pas suffisante, celui-ci devant être considéré sous trois angles : social, juridique et économique. Dans le domaine juridique, les thèmes abordés sont la réglementation des algorithmes, l'éthique de l'IA, le rôle du juge et l'autonomie décisionnelle dans le contexte de l'IA.

[689] F. G'sell, (dir.), *Le Big Data et le Droit*, Paris, Dalloz, « Thèmes & commentaires – Actes », 2020. Selon Florence G'Sell, spécialiste du droit numérique et de la protection des données, le Big Data n'est pas seulement un problème technologique, mais aussi une rupture épistémologique pour le droit, avec des conséquences sur toutes les branches juridiques : droit civil, pénal, public et administratif, droit de la concurrence. Les données sont passées du statut de simples informations isolées à celui de « matière première » pour l'économie, conférant un avantage concurrentiel. L'auteure soulève également la question de savoir à qui appartiennent ces données, puisqu'il n'existe pas de droit de propriété classique, mais une multitude de régimes juridiques (protection de la vie privée, secret commercial). Elle attire en outre l'attention sur la collecte de données par les plateformes numériques (données qui ont une valeur équivalente) et sur le déséquilibre entre les individus et les géants technologiques.

[690] G. Berthoud, *L'horizon d'une surveillance omniprésente?,* Revue européenne des sciences sociales, XL(2), 2002. https://doi.org/10.4000/ress.623. En 2002, Gérald Berthouda affirmait que le monde entier allait être engagé dans un vaste mouvement de transformation et que la seule voie privilégiée pour inventer un monde nouveau semblait être celle offerte par le développement illimité de la technologie. Si l'on en croit les experts, les grands décideurs économiques et les représentants du pouvoir politique, nous serons tous entraînés dans une « mutation informationnelle ».

que la surveillance omniprésente n'est plus exclusivement l'attribut de l'État, mais aussi des entreprises qui exploitent les données personnelles à des fins lucratives. Par exemple, les algorithmes qui permettent de personnaliser des flux d'actualités ou des recommandations de produits que chaque utilisateur reçoit en partie sont alimentés par un grand nombre de données recueillies auprès des utilisateurs, ce qui remet constamment en question l'éthique de ces types de pratiques, ainsi que la protection juridique des données personnelles[691].

216. Vulnérabilité sociale. D'un point de vue social, les utilisateurs sont de plus en plus disposés à faire des compromis sur la protection de leur vie privée, acceptant indirectement la surveillance en échange d'un accès aux avantages numériques[692]. Ce phénomène actuel montre l'évolution de la relation entre l'individu et la technologie, faisant de la confidentialité et de l'intégrité de l'information une monnaie d'échange. George Orwell souligne dans son œuvre que cette exposition est alimentée par les désirs d'interaction et de connectivité, des mécanismes qui rendent les utilisateurs vulnérables à la surveillance des entreprises et de l'État[693].

217. Vulnérabilité juridique. D'un point de vue juridique, les réglementations juridiques actuelles, par exemple le règlement RGPD dans l'Union Européenne, tentent d'équilibrer cette dynamique, mais elles sont souvent dépassées par l'avancée technologique rapide de l'innovation technologique[694]. La vulnérabilité de la vie privée nécessite une réévaluation constante du cadre juridique et une prise de conscience accrue de la part des utilisateurs des risques inhérents à un monde qui se définit par l'interconnectivité.[695]

218. De l'État surveillant à la société exposée. Le chapitre « L'État de surveillance » met en évidence l'intégration des technologies de surveillance dans l'infrastructure numérique mondiale et la façon dont elle a fait de la vie privée une ressource accessible aux États et aux entreprises. Ce changement redéfinit non seulement le concept de confidentialité, mais aussi le rôle de la législation dans la réglementation d'un environnement qui évolue plus rapidement que les autorités judiciaires peuvent suivre[696]. Par exemple, les collaborations entre les agences

---

[691] G. Crewe, „*How Algorithms Shape Our Online World I Oxford Open Learning*", 2024. consulté le 28 novembre 2024, https://www.ool.co.uk/blog/how-algorithms-shape-our-online-world/.

[692] Publicis Sapient, „*Privacy or Convenience: What's the Tradeoff*, Insights. consulté le 28 novembre 2024, https://www.publicissapient.com/insights/privacy-or-convenience--what-s-the-tradeoff.

[693] J.A Dilmaç, O. Kocadal, *Exchanging Glances With Big Brother: Diffuse Surveillance in Orwell's Nineteen Eighty-Four and Today*, Sciences & Actions Sociales, vol.12(2), 2019. p.10-32 https://doi.org/10.3917/sas.012.0010.

[694] Y. Smirnova, V. Travieso-Morales, *Understanding challenges of GDPR implementation in business enterprises: a systematic literature review,* International Journal of Law and Management, vol.66(3), 2024. p.326–344.

[695] L. Urban, « La vie privée révélée et la vulnérabilité exploitée – une approche comparée du piratage informatique en tant que méthode occulte d'enquête policière », in *Archives de politique criminelle*, vol. 43(1), 2021, p. 207-219. https://doi.org/10.3917/apc.043.0207.

[696] B.E. Harcourt, *« 2.L'État de surveillance ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.59-76. shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-59?lang=fr.Harcourt.

de renseignements et les entreprises privées, telles que les partenariats entre la NSA et les géants de la technologie, démontrent à quel point les normes juridiques traditionnelles sont souvent insuffisantes pour faire face à la complexité de la surveillance moderne[697].

b). « Société d'exposition » - les utilisateurs acceptent volontairement le contrôle

Socialement, les nouvelles technologies influencent la façon dont les individus perçoivent l'intimité et la sécurité.[698] Au fur et à mesure que les utilisateurs acceptent des avantages tels que la personnalisation du contenu, l'accès rapide aux informations et une connectivité accrue, ils deviennent de plus en plus tolérants aux compromis sur la vie privée[699]. Ce changement culturel, surnommé par Harcourt « la société d'exposition », souligne que les individus jouent souvent un rôle actif en rendant leurs renseignements personnels vulnérables[700]. En acceptant les conditions imposées par les plateformes numériques, les utilisateurs renoncent au contrôle de leurs données[701], ce qui a des implications profondes sur la notion de vie privée comme droit fondamental.

219. L'impact de l'exposition publique sur la vie privée. L'impact de ces transformations ne se limite pas à la confidentialité, mais touche également les droits fondamentaux tels que la liberté d'expression et d'association.[702] Dans un contexte où chaque activité en ligne peut être surveillée, les individus peuvent finir par autocensurer leurs comportements par crainte d'être supervisés ou analysés[703]. Cet « effet paralysant » sur les libertés personnelles est l'un des plus

---

[697] *Developments in the Law: More Data, More Problems*, Harvard. Law. Review, vol.131, no.6, 2018. p.1714-811. https://harvardlawreview.org/print/vol-131/cooperation-or-resistance-the-role-of-tech-companies-in-government-surveillance/

[698] X. Leonetti, *Smartsécurité et Cyberjustice*. Presses Universitaires de France, 2021. https://doi.org/10.3917/puf.leone.2021.01. Magistrat et docteur en droit, intéressé par le droit numérique et la protection des données, Xavier Leonetti part du principe que la nouvelle ère technologique, basée sur la collecte massive de données, les algorithmes et l'intelligence artificielle, modifie profondément la compréhension et le fonctionnement de la sécurité et du système juridique.

[699]R. Lippert, *David Lyon, Surveillance Studies: An Overview*, Canadian Journal of Sociology, vol.33, no.2, 2008. https://doi.org/10.29173/cjs2004

[700] Ibidem

[701] J. Richard, *Le numérique et les données personnelles : quels risques, quelles potentialités?,* Revue du droit public, Janvier(1), 2016, p. 87-100. https://droit.cairn.info/revue-revue-du-droit-public-2016-1-page-87?lang=fr.

[702] C. Vallet, *Le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs*, Droit et société, vol. 80(1), 2012, p. 163-188. https://doi.org/10.3917/drs.080.0163. Les réseaux sociaux (Facebook, MySpace) ont modifié l'espace privé de l'individu, non seulement en termes d'exposition volontaire, mais aussi en changeant les normes sociales et la perception de l'intimité. Ce changement est significatif car :
- la perception de la « vie privée » devient plus flexible
- le contrôle des données personnelles est réduit (en grande partie à cause des plateformes numériques qui réduisent la différence entre « privé » et « public »)
- les contextes sociaux normatifs concernant ce qui est divulgué et ce qui reste privé évoluent rapidement.
Le présent ouvrage invite à réfléchir aux implications : que signifie la vie privée à l'ère numérique, quels droits méritent d'être protégés, quelles règles doivent être adaptées.

[703] Unesco, „*Global Survey on Internet Privacy and Freedom of Expression*", 2012. consulté le 28 novembre 2024, https://www.unesco.org/en/articles/global-survey-internet-privacy-and-freedom-expression.

grands défis sociaux et juridiques de l'ère numérique[704]. Dans un tel environnement, le rôle de l'État n'est plus seulement de protéger les citoyens contre la surveillance, mais aussi de réglementer la collaboration entre le secteur privé et le public afin de maintenir un équilibre entre sécurité, innovation et respect des droits fondamentaux[705].

L'impact des technologies modernes sur la vie privée va au-delà des limites de la surveillance évidente et s'étend à des domaines plus subtils et difficiles à réglementer. Dans l'œuvre « Panoptique » de Bentham, réinterprété par Foucault, il a été utilisé à l'origine pour comprendre comment l'architecture peut organiser les relations de pouvoir, mais à l'ère numérique, ce modèle devient plus complexe[706]. La surveillance ne se limite plus aux espaces physiques, mais pénètre profondément dans tous les aspects de la vie à travers les données personnelles[707]. Dans ce contexte, les conséquences juridiques sont particulièrement problématiques, car les structures juridiques traditionnelles n'ont pas été conçues pour répondre à de telles formes invisibles et omniprésentes de surveillance[708].

220. Concept/statut de surveillance. La législation actuelle vise à protéger la vie privée par le biais de réglementations strictes sur la collecte et l'utilisation des données personnelles.[709] Cependant, ces mesures sont insuffisantes lorsque le pouvoir de supervision n'appartient plus exclusivement à l'État, mais est réparti entre les gouvernements et les entreprises privées[710]. Par exemple, le modèle de « date-panoptisme », mentionné dans l'œuvre, montre comment la surveillance par algorithmes[711] peut être justifiée par l'efficacité ou la transparence, mais en

---

[704] B.E. Harcourt, « *3. Le Panoptique de Jeremy Bentham* ». *La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.77-97. shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.

[705] D. Lyon, „*The Culture of Surveillance: Watching as a Way of Life*, Polity Press, 2018. consulté le 28 novembre 2024,https://www.researchgate.net/publication/324547017_The_Culture_of_Surveillance_Watching_as_a_Way_of_Life.

[706] B.E. Harcourt, « *3.Le Panoptique de Jeremy Bentham* ». *La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.77-97. shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.

[707] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* NY, Public Affairs*, 2019.*

[708] O. Reis et all., *Privacy law challenges in the digital age: a global review of legislation and enforcement,* International Journal of Applied Research in Social Sciences, vol.6, no.1, 2024. https://doi.org/10.51594/ijarss.v6i1.733.

[709] C. Féral-Schuhl, *Protection des données personnelles*, Paris, Dalloz, 2021. Cet ouvrage passe en revue l'évolution de la législation : de la loi « Informatique et Libertés » de 1978 à l'application du Règlement général sur la protection des données (RGPD) et à la législation nationale de mise en œuvre. Il aborde également les nouvelles tendances : réglementation de l'IA, transparence algorithmique, responsabilité organisationnelle.

[710] *Le Règlement 2016/679 du Parlement Européen et du Conseil du 27 avril 2016* « concernant la protection des personnes physiques relative au traitement des données à caractère personnel et la libre circulation de ces données et d'abrogation de la Directive 95/46/CE » http://data.europa.eu/eli/reg/2016/679/oj/ron.

[711] *Le juge face aux mutations de la vie privée,* Revue justice actualités, vol. 30, 2025. https://droit.cairn.info/revue-justice-actualites-2025-1?lang=fr.

même temps elle peut conduire à la discrimination ou à la violation des droits fondamentaux[712]. Les algorithmes, bien qu'apparemment neutres, peuvent reproduire et amplifier des préjugés préexistants, comme dans le cas de systèmes automatisés de sélection de candidats pour des emplois ou des systèmes de crédit[713].

221. La société de l'auto-exposition . Au-delà de la dimension juridique, les effets sociaux de la surveillance numérique sont profondément transformateurs.[714] Harcourt met l'accent sur la façon dont les individus internalisent leur statut de « sujets exposés », ce qui les amène à s'autocensurer et à accepter des règles qui auraient autrefois été perçues comme envahissantes[715]. Par exemple, l'utilisation de caméras de surveillance dans les espaces publics[716] ou d'outils numériques de suivi des contacts pendant la pandémie de COVID-19 a été justifiée comme une mesure temporaire, mais elle a créé des précédents dangereux[717]. Bien que ces pratiques puissent être efficaces pour protéger la santé publique, elles soulèvent de sérieuses questions sur la façon dont ces technologies peuvent être utilisées plus tard à des fins moins bienveillantes[718]. Cet effet secondaire démontre que le développement technologique engendre souvent des dilemmes éthiques et juridiques qui nécessitent une réévaluation constante.[719]

c). Nécessité d'un équilibre entre la protection de la vie privée, la sécurité et la transparence

222. Créer un équilibre entre surveillance et confidentialité. Dans ce contexte, le principal défi juridique est de trouver un équilibre entre la protection de la vie privée et le besoin de sécurité et de transparence. Foucault disait que « la surveillance devient efficace lorsque

---

[712] B.E. Harcourt, « *3.Le Panoptique de Jeremy Bentham*». *La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.77-97. shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.
[713] Ibidem
[714] B. Benhamou, *Les conséquences démocratiques des mutations de la surveillance numérique*, Cahiers français, vol. 439(3), 2024, p. 62-69. https://doi.org/10.3917/cafr.439.0062.
[715] Ibidem
[716] L. Bachmaier Winter, *Section III – Procédure pénale. Societé de l'information et droit pénal Rapport Général*, Revue internationale de droit pénal, vol. 85(1), 2014, p. 15-74. https://doi.org/10.3917/ridp.851.0013.
[717] A.Dubov, *Ethics of Digital Contact Tracing to Contain the COVID-19 Pandemic,* Institute for Health Policy Leadership, 2021. consulté le 28 novembre 2024, https://ihpl.llu.edu/blog/ethics-digital-contact-tracing-contain-covid-19-pandemic
[718] M. Kapila, „*The Long Shadow of COVID-19*", en S. Pachauri, A. Pachauri, *Global Perspectives of COVID-19 Pandemic on Health, Education, and Role of Media*, Springer Nature, Singapore, 2023. p.177–192 https://doi.org/10.1007/978-981-99-1106-6_8
[719] J. Hamet, S. Michel, *Les questionnements éthiques en systèmes d'information*, Revue française de gestion, vol. 271(2), 2018, p. 99-129. https://doi.org/10.3166/rfg.2018.00221.

l'individu internalise le regard du superviseur »[720], et à l'ère numérique, ce principe est amplifié par la technologie. La législation doit évoluer non seulement pour sanctionner les abus évidents, mais aussi pour empêcher que des individus ne soient transformés en produits d'une économie axée sur les données.[721] Une telle réglementation n'est pas seulement une question de droit, mais une nécessité sociale pour protéger les valeurs fondamentales dans un monde où le pouvoir s'exerce de manière plus subtile et omniprésente.[722]

223. Le désir d'exposition conduit à la création d'une éclipse de l'humanisme. Le chapitre « L'éclipse de l'humanisme » met en évidence la façon dont les technologies numériques ont fondamentalement transformé la relation entre les individus et la vie privée, générant de profondes implications sociales et juridiques. Au fur et à mesure que les données deviennent une ressource clé de l'économie numérique, les frontières traditionnelles de la vie privée sont érodées et la vie privée se transforme en valeur commerciale[723]. Bernard E. Harcourt souligne que cette transition n'est pas seulement technologique, mais aussi culturelle, reflétant un changement des valeurs de la société, où l'exposition et la transparence sont souvent célébrées au détriment de la confidentialité.[724]

L'une des conséquences sociales remarquables est la création d'une « société d'exposition »[725], dans laquelle les individus internalisent les règles de supervision et participent activement à leur propre surveillance[726]. Les plateformes numériques et les réseaux sociaux fonctionnent comme des espaces d'interaction, mais aussi comme des mécanismes de collecte de données[727]. Harcourt souligne comment cette dynamique réduit la confiance des utilisateurs dans leur propre contrôle sur la vie privée, les conduisant à accepter une surveillance

[720] B.E. Harcourt, «*3. Le Panoptique de Jeremy Bentham ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.77-97. shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.

[721] T. Slingeneyer, *La surveillance électronique selon le Conseil de l'Europe : entre un contrôle de la réinsertion et une réinsertion par le contrôle*, en R. Lévy, L. Dumoulin, A. Kensey, C. Licoppe, *Le bracelet électronique : action publique, pénalité et connectivité*, Médecine & Hygiène, 2019, p.63-85. https://doi.org/10.3917/mh.dumou.2019.01.0063.

[722] P. Adam, *Vie personnelle/vie professionnelle : une distinction en voie de dissolution ? (petit exercice de jardinage juridique),* Le Droit Ouvrier, vol. 780(7), 2013, p. 431-444. https://doi.org/10.3917/drou.780.0431. L'auteur montre que la jurisprudence a ouvert la voie à l'intervention dans un domaine auparavant considéré comme protégé, et que la distinction entre vie privée et vie professionnelle semble perdre de son utilité.

[723] B.E. Harcourt, 6. *L'éclipse de l'humanisme ». La Société d'exposition Désir et désobéissance à l'ère numérique,* Le Seuil, 2020. p.150-160. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-150?lang=fr.

[724] Ibidem.

[725] Ibidem.

[726] D. Lyon, „*The Culture of Surveillance: Watching as a Way of Life*, Polity Press, 2018. consulté le 28 novembre 2024.https://www.researchgate.net/publication/324547017_The_Culture_of_Surveillance_Watching_as_a_Way_of_Life.

[727] J. van Dijck, *The Culture of Connectivity: A Critical History of Social Media*, Oxford Academic, 2013.

étendue comme norme sociale[728]. Dans ce contexte, la vie privée devient un privilège réservé uniquement à ceux qui peuvent se permettre d'investir dans des mesures de protection avancées, amplifiant les inégalités sociales[729].

d). Redéfinir la relation entre le droit, l'humanité et la technologie

224. Approche interdisciplinaire de la protection de la vie privée. D'un point de vue juridique, le chapitre attire l'attention sur le fait que la législation existante, bien qu'avancée dans certains domaines, reste insuffisante pour faire face aux défis de l'ère numérique[730]. Par exemple, les règlements sur la protection des données sont souvent limités à certaines juridictions[731], laissant des vides juridiques qui permettent aux sociétés mondiales d'exploiter ces lacunes[732]. En outre, les technologies émergentes comme l'intelligence artificielle et les algorithmes de décision automatisée créent des scénarios complexes où la responsabilité juridique est difficile à attribuer[733]. L'œuvre souligne la nécessité d'une approche holistique qui intègre la législation, l'éducation publique et l'innovation technologique pour protéger les droits fondamentaux des individus dans un environnement numérique de plus en plus difficile.[734]

Équilibre entre innovation et confidentialité. Cette transformation comporte un défi philosophique : redéfinir la relation entre l'humanité et la technologie. Par cette œuvre, Harcourt se demande si la protection de la vie privée peut encore être considérée comme un droit fondamental ou si elle devient une ressource négociable, sacrifiée au nom du progrès.[735]

---

[728] B.E. Harcourt, «*6. L'éclipse de l'humanisme ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-150?lang=fr.

[729] M. Madden, „*Privacy, Security, and Digital Inequality*", Data & Society Research Institute, 2017. https://datasociety.net/library/privacy-security-and-digital-inequality/.

[730] B.E. Harcourt, «*6. L'éclipse de l'humanisme* ». *La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-150?lang=fr.

[731] „*Navigating the Jurisdictional Chaos: An International Law Perspective on the Extraterritorial Application of Data Protection Laws",* DPO Europe, 2024. consulté le 28 novembre 2024, https://data-privacy office.eu/navigating-the-jurisdictional-chaos-an-international-law-perspective-on-the-extraterritorial-application of-data-protection-laws/.

[732]C. Alvaro et all., *Multinationals misbehavior*, Journal of World Business, vol. 56, issue 5, 2021.

[733] „*Liability Rules for Artificial Intelligence",* European Commission, consulté le 28 novembre 2024, https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/digital contracts/liability-rules-artificial-intelligence_en.

[734] F. Dubuisson, *La Cour européenne des droits de l'homme face à la surveillance de masse (obs. sous Cour eur. dr. h., Gde Ch., arrêt Big Brother Watch et autres c. Royaume-Uni, 25 mai 2021),* Revue trimestrielle des droits de l'Homme, vol.129(1), 2022, p. 123-141. https://doi.org/10.3917/rtdh.129.0123.

[735] B.E. Harcourt, *«6. L'éclipse de l'humanisme»*, *La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.150-160. shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-150?lang=fr.

Pour répondre à ces questions, il faut une collaboration entre tous les secteurs de la société, des législateurs et éducateurs aux développeurs de technologies, afin de rétablir l'équilibre entre innovation et la confidentialité.

Sur certains de ces points, la CEDH a exprimé un avis assez ferme dans son arrêt Big Brother Watch and Others c. Royaume-Uni de 2021.[736] Dans cet arrêt, la Cour reconnaît que la surveillance de masse peut viser des objectifs légitimes, tels que la sécurité nationale, mais souligne que les mécanismes de surveillance peuvent être extrêmement intrusifs, car ils permettent de suivre les réseaux sociaux, les déplacements et les interactions, ce qui équivaut à une surveillance systémique.[737] La visibilité de la technologie n'équivaut pas à son contrôle, et il subsiste des vulnérabilités importantes dans la protection des droits individuels.

225. Convergence de la surveillance : État, plateformes numériques, opérateurs privés. Le chapitre « La disparition des frontières entre l'État, l'économie et la société »[738] explore les effets profonds de la dissolution des frontières traditionnelles entre l'État, l'économie et la société à l'ère numérique. Cette transformation redéfinit la façon dont les technologies influencent la vie privée, renforçant la surveillance et la collecte de données en tant que normes sociales.[739] Après avoir analysé plusieurs décisions de la CEDH, certaines opinions doctrinales concluent que la jurisprudence commence à reconnaître la nécessité de protéger la vie privée dans le contexte des technologies numériques, et ont identifié certaines zones d'incertitude : normes nationales inadaptées, normes de surveillance encore floues, déséquilibre persistant entre les intérêts économiques de l'employeur et la protection de l'employé, etc.

Harcourt souligne que ces changements ont de profondes implications juridiques et sociales, car les responsabilités et les limites des acteurs impliqués – gouvernements, entreprises et citoyens – sont de plus en plus difficiles à identifier.[740]

e). Collecte de données sur les réseaux sociaux, réglementation inégale

[736] Affaire de *Big Brother Watch et autres v. Royaume-Uni*, requêtes nos. 58170/13, 62322/14 et 24960/15, https ://hudoc.echr.coe.int/fre#{"itemid":["001-210077"]}
[737] F. Dubuisson, *op. cit.*, p.124.
[738] B.E. Harcourt, « 7. La disparition des frontières entre l'État, l'économie et la société ». *La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.163-184
[739] M. D'Aponte, *Les nouvelles technologies et le respect de la vie privée du travailleur dans la jurisprudence de la CEDH*, Revue de droit comparé du travail et de la sécurité sociale, n° 2, 2021.
[740]. B.E. Harcourt, *« 7. La disparition des frontières entre l'État, l'économie et la société ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.163-184. shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-163?lang=fr.

226. État – privé : partenariat de surveillance.[741] D'un point de vue juridique, Harcourt met en lumière la façon dont l'État et les entreprises privées collaborent dans le cadre « d'un partenariat de surveillance », ce qui porte atteinte à la vie privée des individus[742]. Cette collaboration permet l'utilisation de technologies avancées pour une surveillance massive, souvent justifiée par le besoin de sécurité nationale ou d'efficacité économique[743]. Cependant, ces pratiques mettent en danger les droits fondamentaux, car la législation actuelle est insuffisante pour protéger les utilisateurs contre les abus. Par exemple, la collecte de données via les réseaux sociaux ou les applications de suivi n'est pas uniformément réglementée, ce qui permet d'exploiter des lacunes juridiques au détriment de la confidentialité.[744]

D'un point de vue social, cette dissolution des frontières contribue au changement culturel, où l'exposition devient la norme.[745] Le paradoxe fondamental de la société numérique est que, d'une part, elle promet l'affirmation de la liberté individuelle (liberté d'expression, accès à l'information, participation à la vie sociale), mais, d'autre part, elle introduit de nouveaux mécanismes de surveillance qui peuvent éroder l'autonomie personnelle.[746]

L'autonomie des citoyens. En même temps, la littérature juridique souligne que les individus, souvent sans s'en rendre compte, participent activement à leur propre supervision, partagent des données personnelles et acceptent des conditions qui réduisent leur vie privée.[747] Cette « société de la transparence »[748] renforce le pouvoir de l'État et de l'économie privée, mais réduit l'autonomie des citoyens, qui subissent une perte progressive de contrôle sur leurs propres informations. Dans ce contexte, la confidentialité devient un privilège plutôt qu'un droit universel, créant des inégalités et des vulnérabilités accrues.[749]

Harcourt propose la nécessité de repenser fondamentalement le rapport entre la technologie, l'État et les citoyens. La législation doit être adaptée afin de garantir la

---

[741] I. Compiègne, *Chapitre VI. Société de liberté ou de surveillance ? La société numérique en question(s)*, Éditions Sciences Humaines, 2010, p. 71-84. https://shs.cairn.info/la-societe-numerique-en-questions--9782361060077-page-71?lang=fr.

[742] Ibidem

[743] D. Lyon, „*Surveillance After Snowden",* Polity, 2015. consulté le 28 novembre 2024, https://www.politybooks.com/bookdetail?book_slug=surveillance-after-snowden--9780745690841

[744] C. Kumar, „*Government Surveillance and the Erosion of the Right to Privacy*, LinkedIn, 2023. consulté le 28 novembre 2024, https://www.linkedin.com/pulse/government-surveillance-erosion-right-privacy-chetan-kumar/.

[745] D. Encaoua, *Repenser les politiques d'innovation en France?,* Revue française d'économie, XXXII(3), 2017, p. 90-135. https://doi.org/10.3917/rfe.173.0090.

[746] Idem, p. 90 – 135.

[747] B.E. Harcourt, *« 7. La disparition des frontières entre l'État, l'économie et la société ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.163-184, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-163?lang=fr.

[748] B.E. Harcourt, *La Société d'Exposition: Désir et Désobéissance à l'Ère Numérique*, Le Seuil, 2020. https://shs-cairn-info.docelec.u-bordeaux.fr/la-societe-dexposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page39?lang=fr.

[749] TechTarget and Informa „*The Role of Transparency in Digital Trust"*, Search Security, 2022. consulté le 28 novembre 2024, https://www.techtarget.com/searchsecurity/post/The-role-of-transparency-in-digital-trust.

transparence et la responsabilisation des gouvernements et des entreprises, et l'éducation numérique doit devenir une priorité pour sensibiliser le public à leurs droits.[750] Enfin, les conséquences du développement technologique sur la vie privée ne sont pas seulement techniques, mais aussi profondément politiques, nécessitant des réponses intégrées pour protéger la dignité et la liberté individuelles dans un monde numérisé.[751]

B. Principes de l'exercice du droit à la vie privée grâce à la technologie

227. Systèmes de protection des droits de l'homme, nouveaux risques. L'approche généreuse de la définition du droit à la vie privée a permis le développement de la jurisprudence au fur et à mesure de l'évolution des technologies.[752] En analysant la jurisprudence récente de la CEDH, on constate qu'elle fait référence aux défis posés par les technologies numériques en matière de droits et libertés fondamentaux. La numérisation – qui inclut ici l'internet, les algorithmes, le profilage et la surveillance – soulève des questions liées à l'interprétation et à l'application des droits de l'homme à l'ère nouvelle. Bien que la Convention ait été adoptée en 1950, elle a prouvé sa capacité à s'adapter à l'ère numérique, mais des défis subsistent : des normes claires concernant les algorithmes, le profilage, la surveillance automatisée.[753]

Lorsque nous faisons référence à l'exercice du droit privé grâce à la technologie, nous identifions inévitablement « le droit au respect de la vie privée et le droit à la protection des données personnelles »[754]. Bien qu'étroitement liés, les deux droits sont distincts.[755] Le droit au respect de la vie privée est inscrit dans le droit international par « la Déclaration universelle des droits de l'homme » (DUDH) en 1948, adoptée en Europe par la Convention européenne des droits de l'homme (CEDH) en 1950.

Redéfinition du droit de propriété : les données privées deviennent des biens publics. Étant donné que ces actes de grande importance ont été adoptés bien avant l'avènement de la société de l'information, respectivement avant l'avènement des ordinateurs et d'Internet, de nouveaux risques pour la vie privée sont apparus avec l'évolution

---

[750] M. Saritepeci et all., „*The Role of Digital Literacy and Digital Data Security Awareness in Online Privacy Concerns: A Multi-Group Analysis with Gender",* Online Information Review, vol.48, nr.5, 2024. p.983–1001, https://doi.org/10.1108/OIR-03-2023-0122

[751] A. Lewis, „*Balancing Technological Advancements with Privacy Risks*", DMNews (blog), 2024, https://www.dmnews.com/balancing-technological-advancements-with-privacy-risks/.

[752] S. Turgis, *La Convention européenne des droits de l'homme et la protection des droits et libertés à l'ère du numérique*, Civitas Europa, vol 49(2), 2022, p. 263-272. https://doi.org/10.3917/civit.049.0263.

[753] S. Turgis, *op. cit*.

[754] A. Ménard, *La garantie des droits fondamentaux dans les états d'exception sous la Ve République*, Revue française de droit constitutionnel, 128(4), 2021, e1-e29. https://doi.org/10.3917/rfdc.128.e0001.

[755] P. Bourdon, *Introduction. Les indispensables du droit public*, Ellipses, 2021, p.9-12. https://droit.cairn.info/les-indispensables-du-droit-public-2e-edition--9782340040113-page-9?lang=fr.

technologique.[756] Dans ce contexte, certains auteurs[757] explorent la notion traditionnelle de droit de propriété et les nouveaux types de biens, tels que les données personnelles et les données publiques, en partant de l'idée que la propriété – le droit de posséder, d'utiliser, de disposer – est déstabilisée lorsque l'objet de la propriété devient un flux d'informations ou de données, qui ne se prête pas facilement à l'exclusivité ou à la rivalité. Les droits relatifs à la personne (préférences, comportements, données biométriques) sont considérés comme des biens propres, mais, bien que la personne puisse avoir un droit de contrôle, celui-ci est limité, car les données peuvent être multipliées, reproduites et utilisées simultanément par plusieurs individus. Les données dites « publiques » (provenant des autorités, des sondages, des données ouvertes) sont présentées comme des ressources appartenant à la collectivité ou ayant un potentiel utilitaire commun. En conséquence, le droit de propriété doit être réinterprété pour répondre à ces dilemmes : il ne s'agit pas seulement d'adapter la législation existante, mais aussi d'envisager un régime hybride dans lequel les données peuvent être utilisées, protégées et valorisées correctement.

Ainsi, « afin de répondre aux besoins engendrés par la nouvelle technologie, des règlements juridiques spéciaux ont été élaborés pour garantir la protection des informations à caractère personnel. La protection des données en Europe a commencé dans les années 1970, lorsque certains États ont adopté une législation visant à gérer le traitement des informations personnelles par les autorités publiques et les grandes entreprises ».[758]

228. Protection des données à caractère personnel, partie intégrante du droit à la vie privée.[759] L'Union Européenne reconnaît officiellement pour la première fois la protection des données à caractère personnel comme une valeur nécessaire à réglementer de façon distincte de la vie privée, en 1981 par la Convention 108[760]_bookmark88, et en 1995 elle assure une double protection des données par la directive 95/46/CE.[761]

---

[756] É. Chevalier, « *Leçon 5. Propriété, données personnelles et publiques* », in M. Boudot, D. Veillon (dir.), *Les propriétés*, Presses universitaires juridiques de Poitiers, 2016, p. 67-81. https://doi.org/10.3917/puj.boudo.2016.01.0068

[757] É. Chevalier, *op. cit.*

[758] Il s'agit de la première loi se référant à la protection des données, adoptée en 1970 et appliquée d'une façon limitée, uniquement sur le territoire du Land de Hessa. La Suède est celle ayant adopté la première loi nationale concernant la protection des données en 1973. Ensuite, plusieurs pays européens ont pris courage et se sont intéressés à ce domaine, dont la France, le Royaume-Uni et les Pays-Bas, régissant jusqu'à la fin des années 1980 la protection des données.

[759] *Big data : quelle protection des données personnelles ?,* LEGICOM, (59), 2017. https://droit.cairn.info/revue-legicom-2017-2?lang=fr.

[760] L'Union Européenne adopte en 1981 la *Convention du Conseil d'Europe de protection des personnes face au traitement automatique des données à caractère personnel* ». (*Convention 108*).

[761] « Il s'agit de la *Directive 95/46/CE concernant la protection des personnes physiques relative au traitement des données à caractère personnel et la libre circulation de ces données » (Convention 108*), adoptée en 1995 et reconnue par l'UE comme étant sont premier outil global de protection des données.

La protection des données et la protection de la vie privée sont considérées dans l'ordre juridique européen comme deux droits fondamentaux distincts mais étroitement liés, puisque tous deux protègent des valeurs similaires et garantissent aux individus un environnement sûr dans lequel ils peuvent se développer, penser et s'exprimer librement.[762] Les deux droits se distinguent par leur formulation et leur portée. Ainsi, si le droit à la vie privée concerne la sanction générale[763] de l'ingérence, le droit à la protection des données se réfère au côté spécifique, moderne[764] et actif du traitement des données. De plus, « le droit à la protection des données personnelles » couvre un domaine plus large que le droit au respect de la vie, dans le sens où le premier ne se limite pas à la protection des données liées à la vie privée, mais fait référence à tous les types et traitements de données personnelles.

229. Articulation du droit à la vie privée et du droit à la protection des données à caractère personnel, émergence d'un droit hybride. Notre étude examine les principes spécifiques des deux droits distincts qui se rapportent à la protection de la valeur privée de l'individu, ce qui permet même d'apprécier l'identification d'un « nouveau » droit hybride, à savoir la protection de la vie privée par le biais de la technologie.[765]

Ce « nouveau » droit revêt un caractère hybride, en ce sens qu'il protège à la fois la vie privée en général et la vie privée surtout à l'ère de la technologie, ayant pour objet la protection de la personne dans le cadre d'une atteinte à un intérêt privé consécutive au traitement de données à caractère personnel par voie numérique. Le droit hybride protège les spécificités des deux droits distincts en combinant le droit physique (hors ligne) avec le droit numérique (en ligne).[766]

Les données des utilisateurs de technologies, « le pétrole du XXIe siècle ». À cet égard, « le nouveau » présente des caractéristiques, des attributs spécifiques, identifiés dans cette recherche comme principes du droit de la protection de la vie privée de la personne par le biais de la technologie numérique, à savoir : le principe de la sécurité des données numériques, le principe du consentement numérique, le principe des données massives, des algorithmes[767]

---

[762] N. Hassani, *Le paradoxe de la protection des données personnelles à l'heure de la libre circulation des informations*, Terminal, 2019, p. 124.
[763] Sous réserve de certaines affaires pouvant justifier l'intervention de certains critères d'intérêt public.
[764] En date de 17 juin 2010, dans les Conclusions de l'avocat général Sharpston, au point 71, l'avocat général Eleanor Sharpson apprécier que la protection de la vie privée appartient au droit « *classique* », tandis que la protection des données appartient au droit « *moderne* ». Voir les Conclusions.
[765] A. Rabagny-Lagoa, *Fiches de Droit du traitement et de la protection des données personnelles : Rappels de cours et exercices corrigés.* Ellipses, 2022. https://doi.org/10.3917/elli.rabag.2022.01.
[766] *La protection des données dans une économie globalisée*, Annales des Mines - Réalités industrielles, 2022. https://stm.cairn.info/revue-realites-industrielles-2022-3?lang=fr.
[767] D. Bourcier, P. De Filippi, *Transparence des algorithmes face à l'open data : quel statut pour les données d'apprentissage?,* Revue française d'administration publique, 167(3), 2018, p. 525-537. https://doi.org/10.3917/rfap.167.0525.

et de l'intelligence artificielle (IA), le principe du web 3.0 (Internet des objets - IoT)[768]. Les principes servent de règles de base dans la protection de la vie privée par le biais de la technologie et de référence pour interpréter une situation de violation du droit.[769] La collecte de grandes quantités de données sur les utilisateurs de technologies est devenue un sujet très actuel, non seulement pour l'économie, le marketing ou la sociologie, mais aussi pour le droit : « alors que la donnée est considérée comme « le pétrole du 21e siècle », […] l'exploitation des données massives représente actuellement l'un des piliers d'une économie numérique mondialisée et largement dominée par les Big tech ».[770]

a). Sécurité des données

230. Définition du concept de sécurité des données à caractère personnel.[771] Le respect des données à caractère personnel est essentiel pour prévenir et combattre les effets négatifs sur les données du titulaire, identifiant en ce sens la sécurité des données comme un principe essentiel de la protection de la vie privée par la technologie.[772]

La sécurité des données est assurée par la confidentialité, l'intégrité, la disponibilité, le contrôle et l'autonomie, ainsi que l'information du titulaire.[773] Ce sont des attributs du principe de la sécurité des données, et étant donné leur importance primordiale pour garantir la protection de l'individu, on peut y ajouter la qualité des sous-principes de la sécurité des données.[774] L'utilisation de données personnelles au moyen de la technologie peut très

---

[768] L. Vuarin, P. Gomes Lopes, D. Massé, *L'intelligence artificielle peut-elle être une innovation responsable ?* Innovations, 72(3), 2023, p.103-147. https://doi.org/10.3917/inno.pr2.0153.

[769] R. Daneshjou, M.P. Smith, M.D. Sun, V. Rotemberg, J. Zou, *Lack of Transparency and Potential Bias in Artificial Intelligence Data Sets and Algorithms: A Scoping Review*, JAMA Dermatol, 157(11), 2021, p.1362–1369.

[770] N. Hassani, *op. cit*.

[771] J.L. Sauron, L. Paravano, P. Céspedes, *S'y retrouver au sein du droit de la protection des données : Boussole pour DPO et autres usagers de la donnée*, Legitech, 2022. https://droit.cairn.info/s-y-retrouver-au-sein-du-droit-de-la-protection-des-donnees--9782919814350?lang=fr.

[772] A. Bensoussan, *Vers un droit de propriété des données personnelles*, Annales des Mines - Réalités industrielles, vol. 3, 2022, p. 18-19. https://doi.org/10.3917/rindu1.223.0018. L'apparition constante de nouvelles technologies et l'omniprésence du traitement des données à caractère personnel dans tous les domaines de la vie placent les données au centre de l'attention. Dans ce contexte, la question se pose de savoir si les données à caractère personnel ne devraient pas être traitées non seulement comme un objet de protection, mais aussi comme un bien sur lequel il est possible de revendiquer un droit de propriété.

[773] Inforeg, *Sécurité des données personnelles. Le nouvel audit cybersécurité*, Cahiers de droit de l'entreprise, n° 3, 2022, p. 65. Cet article explique la nouvelle obligation légale d'audit de cybersécurité introduite par la loi n° 2022-309 du 3 mars 2022, applicable aux grandes plateformes numériques à compter du 1er octobre 2023. Elle vise à rétablir la confiance du public et à faire de la protection des données un objectif stratégique des entreprises. L'audit doit être réalisé par des organismes tiers qualifiés et accrédités par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) et a pour but d'informer le public sur le niveau de sécurité informatique des plateformes et la localisation des données stockées.

[774] M. Séjean, (dir.), *Code de la cybersécurité 2026 annoté et commenté*, 3e éd., Paris, Éditions Dalloz, collection « Codes Dalloz », 2025.

facilement conduire, par négligence, intentionnellement ou non, à l'atteinte au droit à la vie privée du propriétaire des données personnelles.[775]

Afin de prévenir ou de combattre une telle ingérence, le titulaire des données personnelles a le droit de faire valoir son choix – droit de sécuriser ses données, cette possibilité étant un principe essentiel de l'exercice du droit à la vie privée dans l'environnement numérique.[776]

231. Normes et exigences en matière d'intégrité et de confidentialité des données. Le principe de sécurité des données vise à offrir au titulaire la garantie de la sécurité de l'utilisation de ses propres données contre tout accès non autorisé, divulgation ou utilisation externe. Le caractère de garantie de ce principe repose sur la mise en œuvre de mesures et de technologies qui garantissent que les données du titulaire restent privées, intégrales et accessibles uniquement à la personne autorisée à les utiliser.[777]

Le principe de la sécurité des données est distinct de la façon dont le droit traditionnel à la vie privée est exercé.[778] Les données, initialement considérées comme de simples éléments d'information, sont devenues des ressources stratégiques, avec des conséquences sur la propriété, la vie privée et la concurrence. L'expansion des données comporte des risques : perte du contrôle individuel sur ses propres données, apparition d'acteurs économiques disposant d'un pouvoir disproportionné d'exploitation, fragilisation de l'autonomie de la personne. Pour répondre à ces défis, il est nécessaire de repenser le cadre juridique : non seulement la protection des données, mais aussi leur régime de circulation, de valorisation, de propriété et d'accès.[779]

Processus de gestion continu. Si les données personnelles d'une personne pouvaient être obtenues avec plus de difficulté et implicitement le droit à la vie privée pourrait être plus difficile à violer, avec l'évolution de la technologie, le non-respect du droit à la vie privée est devenu une occasion négative plus courante et plus facile à obtenir, et les conséquences sont dévastatrices car elles touchent plusieurs aspects de la vie de l'individu.[780]

---

[775] V. Bullich, V. Clavier, *Production des données, « Production de la société ». Les Big Data et algorithmes au regard des Sciences de l'information et de la communication*, Les Enjeux de l'information et de la communication, vol. 19/2(2), 2018, p. 5-14. https://doi.org/10.3917/enic.025.0005.

[776] N. Mallet-Poujol, *Protection des données personnelles et droit à l'information*, LEGICOM, 59(2), 2017, p. 49-59. https://doi.org/10.3917/legi.059.0049.

[777] C. Zolynski, M. Le Roy, *La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée,* LEGICOM, 59(2), 2017, p. 105-113. https://doi.org/10.3917/legi.059.0105.

[778] V.L. Benabou, *L'extension du domaine de la donnée,* LEGICOM, 59(2), 2017, p. 3-17. https://doi.org/10.3917/legi.059.0003.

[779] V.L. Benabou, *op. cit.*

[780] A. Latil, *Le droit du numérique: une approche par les risques*, Paris, Dalloz, coll. « Droit numérique », 2023. La numérisation de la société (données, algorithmes, intelligence artificielle) crée des vulnérabilités et des préjudices potentiels, et le droit doit s'adapter par des interdictions générales, mais aussi par des instruments permettant d'anticiper, d'évaluer et de gérer les risques.

Le principe de la sécurité des données assigne un rôle actif au détenteur des données en lui confiant la responsabilité de veiller à ce que des mesures techniques et/ou organisationnelles appropriées soient prises afin de protéger contre l'accès non autorisé, l'utilisation, la perte, la divulgation, la destruction ou le dommage non autorisé ou même illégal.[781] La protection des données personnelles ne peut plus être considérée uniquement comme un ensemble d'obligations administratives, mais comme un processus continu de gestion responsable de l'information. Le respect de ces principes devient un exercice d'équilibre entre sécurité, transparence et liberté individuelle.[782] On peut donc comprendre que le principe de la sécurité des données dépend, dans un premier temps, du libre arbitre du détenteur.[783]

232. Le cryptage, un moyen de sécuriser les données à caractère personnel. Les mesures techniques et organisationnelles que la législation actuelle[784] juge comme appropriées sont, par exemple, le cryptage des données personnelles. L'évaluation et la mise à l'essai réguliers de l'efficacité de ces mesures est une mesure de sécurité visant à assurer le respect du principe de la sécurité des données. Les mesures sont flexibles et s'adaptent à la situation concrète de l'individu.[785]

b). Confidentialité

233. La confidentialité, élément fondamental de la sécurité des données à caractère personnel. Une caractéristique essentielle de la sécurité des données privées concerne la confidentialité. La confidentialité n'est pas seulement une dimension technique de la protection des données, mais un principe essentiel de l'autonomie individuelle, car elle permet à la personne de garder le contrôle sur les informations qui la définissent et de décider librement quelle partie d'elle-même devient visible dans l'espace numérique.[786] La confidentialité est le

[781] J.L. Sauron, A. Vitard, *Vos données personnelles : Que savoir et comment faire pour qu'elles le restent !*, Paris, Legitech, 1er éd., 2021. Les auteurs attirent également l'attention sur le fait que les normes juridiques ne suffisent pas toujours à garantir pleinement la confidentialité et l'autonomie individuelle. La sécurité des données doit être une démarche active et continue, et chaque individu doit devenir le « gardien » de ses propres informations.
[782] P. Cespedes Arteaga, L. Paravano, J.L. Sauron, *S'y retrouver au sein du droit de la protection des données : boussole pour DPO et autres usagers de la donnée*, Luxembourg/Paris, Éd. Legitech, 4e éd., 2022.
[783] M. Brogli et all., *Droit des données personnelles*, Paris, Dalloz, coll. « Décryptage », 1re éd., 2019.
[784] Nous faisons référence à titre général à la législation européenne qui influence spécifiquement la législation intérieure des États membres, respectivement le Règlement général de protection des données et la Convention 108 modernisée.
[785] CNIL, *La Sécurité des données personnellles*, Les Guides de la CNIL, 2018. Ce guide de la CNIL préconise la sécurisation des équipements mobiles par des mécanismes de cryptage afin de prévenir la perte ou le vol de données. De même, dans le contexte de la protection de la transmission ou du transfert de données sensibles, le guide mentionne l'importance du cryptage du canal de transmission. La CNIL considère le cryptage comme une mesure technique essentielle pour la protection des données à caractère personnel, tant au niveau du stockage qu'au niveau de la transmission ou de la collaboration.
[786] B. Wintrebert, *Innovation confidentielle : L'avantage secret*, Paris, Éditions EMS, coll. « Questions de société », 2024. Le concept d'« innovation confidentielle » est une stratégie basée sur la confidentialité des projets, des

fondement même du principe de sécurité des données utilisé par la technologie, son rôle étant de s'assurer que les seules personnes ou parties qui peuvent accéder à ces données sont celles autorisées.[787]

Par exemple, le droit de naviguer en privé dans le Navigateur est une caractéristique de la sécurité des données, en ce sens que la plupart des navigateurs web modernes fournissent la fonctionnalité permettant de naviguer en mode privé ou incognito. Ce mode de navigation privée est destiné à empêcher le stockage de l'historique de navigation, des cookies et autres données d'identification de la personne sur cet appareil.[788]

Toujours pour des raisons de sécurité des données, l'utilisateur et le propriétaire des données privées ont la possibilité d'opter pour le droit de configurer ses paramètres de confidentialité concernant le contrôle des informations qu'ils partagent, cette option - droit incluant la possibilité d'établir les niveaux d'accès à leurs données, ainsi que les communications que le titulaire fait.[789]

234. Stockage des données sur des appareils personnels.[790] Dans le même sens, un autre outil qui protège la confidentialité des données personnelles et qui représente ainsi une

---

idées ou des informations, ce qui est considéré comme un réel avantage concurrentiel, alors que le monde numérique a tendance à exagérer la transparence et le partage public. Le livre donne des exemples concrets pour illustrer ce concept. Par exemple, Steve Jobs a utilisé la confidentialité comme partie intégrante de sa stratégie disruptive.

[787] F. Tréguer, « *Anonymat et chiffrement, composantes essentielles de la liberté de communication* », in Q. Van Enis, C. De Terwangne, *L'Europe des droits de l'homme à l'heure d'Internet*, Bruxelles, Bruylant, inPress, 2019.

[788] CNIL, *La navigation privée pour limiter les risques de piratage de vos comptes en ligne* , 2016. Outre les avantages de ce mode de navigation, la CNIL souligne que celui-ci présente également des limites :
- il ne garantit pas l'anonymat total : l'adresse IP, le fournisseur d'accès à Internet et les sites visités peuvent toujours suivre l'activité de l'utilisateur.
- cette méthode est utilisée pour la protection locale (par exemple lorsque plusieurs personnes utilisent le même ordinateur), mais elle ne protège pas complètement contre les attaques externes (phishing, malware, interceptions réseau).
En conclusion, la navigation privée doit être complétée par d'autres mesures de sécurité, telles que : des mots de passe forts, une authentification en deux étapes, la mise à jour des logiciels, l'utilisation de connexions cryptées, l'évitement des réseaux Wi-Fi publics pour les opérations sensibles.

[789] S. Ghernaouti, Cybersécurité : Analyser les risques, mettre en oeuvre les solutions, 7e éd., Dunod, 2022. https://stm.cairn.info/cybersecurite--9782100841493?lang=fr.

[790] G. Pigeon, *Sécurisez votre ordinateur et vos données : déjouer les pièges et user des bonnes pratiques*, Éditions ENI, 2021. À l'ère numérique, les données personnelles et les informations numériques des utilisateurs deviennent extrêmement précieuses, en particulier pour les entités qui cherchent à exploiter le comportement en ligne. Les experts recommandent donc :
- la sécurisation des équipements matériels : cryptage des données sur clé USB ou smartphone, maintenance, utilisation de différentes méthodes de protection
- sécuriser les logiciels : mise à jour, utilisation d'un antivirus ou d'un pare-feu, reconnaissance des programmes malveillants.
- gérer ses propres données : contrôle de la diffusion des données personnelles, conformité avec le RGPD, sauvegarde régulière des données, récupération de celles-ci en cas d'incident.
- bonnes pratiques quotidiennes : création de mots de passe sécurisés, authentification en deux étapes, séparation des domaines personnel/professionnel, navigation sécurisée sur Internet, sensibilisation aux risques.
L'idée centrale de l'ouvrage cité est que le maintien du contrôle sur ses propres données implique, outre les technologies, une attitude et un comportement organisés. De plus, elle souligne le fait que la suppression d'une information ne garantit pas qu'elle n'existe pas dans d'autres copies ou sur des serveurs inconnus.

caractéristique du principe de sécurité des données, se réfère au stockage local des données.[791] Ainsi, la possibilité de stocker des données personnelles sur des appareils personnels, des ordinateurs ou des appareils mobiles, au lieu de les garder en cloud, peut aider le titulaire du droit personnel à obtenir un plus grand contrôle sur les informations personnelles et implicitement sur sa propre vie.[792]

La possibilité volontaire et appropriée de se protéger contre les cyberattaques, telles que le piratage, le hameçonnage ou les logiciels malveillants, est également une caractéristique de la sécurité des données. La mise en œuvre de solutions de sécurité, telles que firewalls, des logiciels antivirus et des mises à jour régulières de sécurité, est essentielle à cet égard.[793]

c). Le cryptage, une mesure essentielle pour la protection des données[794]

235. Cryptage.[795] La protection de la vie privée se manifeste par le cryptage et d'autres techniques spécifiques. À cet égard, nous rappelons qu'il existe de nombreuses applications et outils logiciels spécifiques créés aux fins de la protection de la vie privée, à savoir les VPN (Réseaux Privés Virtuels) qui ont pour rôle de cacher l'adresse IP du titulaire des données et de protéger ses données lors de l'utilisation d'outils numériques, ainsi que les services qui gèrent les mots de passe du titulaire, respectivement pour stocker et contrôler en toute sécurité les informations d'authentification du propriétaire.[796]

Une étude réalisée en 2015[797] a mis en évidence le fait que, dans le contexte actuel des volumes massifs de données, même les informations apparemment anonymisées, telles que les métadonnées des transactions bancaires, peuvent permettre de réidentifier des personnes par la simple corrélation de quelques éléments comportementaux, démontrant ainsi les limites réelles de l'anonymisation traditionnelle. L'étude citée identifie le risque de réidentification des

---

[791] M. Maciel-Hibbard, *Protection des données personnelles et cyber(in)sécurité*, Politique étrangère, Été(2), 2018, p. 55-66. https://doi.org/10.3917/pe.182.0055.

[792] P. Le Galèze, W. Isabelle Westeel, *« Conserver les documents numérisés », Numériser et mettre en ligne*, édité par T. Claerr et I. Westeel, Presses de l'enssib, 2010, https://doi.org/10.4000/books.pressesenssib.439.

[793] H. Champenois, *L'Internet des Objets modifie la cybersécurité : l'exemple de Linky,* Annales des Mines - Enjeux numériques, 8(4), 2019, 106-109. https://stm.cairn.info/revue-enjeux-numeriques-2019-4-page-106?lang=fr La cybersécurité traditionnelle, basée sur la protection périmétrique, de type firewall ou antivirus, devient insuffisante face au développement numérique actuel. Il faut une sécurité avancée, un cryptage au niveau des appareils, une transparence sur les flux de données.

[794] J. M. MANACH, *En attendant la « cryptocalypse »*, Vacarme, n° 69/4, 2014, pp. 100-109. La technologie de cryptage se trouve à la croisée des chemins entre la liberté individuelle et le contrôle social, devenant ainsi un symbole de la rupture entre le privé et le public, entre les individus et les systèmes de contrôle. Face à l'évolution numérique et aux données massives, le cryptage offre une résistance, un refuge pour l'autonomie individuelle.

[795] O. Eymard, *Questions de cryptologie*, Délibérée, 3(1), 2018, p. 60-63. https://doi.org/10.3917/delib.003.0060.

[796] L. Blisson, *Petits vices et grandes vertus du chiffrement*, Délibérée, 7(2), 2019, p.56-59. https://doi.org/10.3917/delib.007.0056.

[797] Y. A. De Montjoye, L. Radaelli, V. K. Singh et al., *Unique in the Shopping Mall : On the Reidentifiability of Credit Card Metadata,* Science, nº 347, 2015.

personnes sur la base des métadonnées des transactions par carte de crédit, même lorsque ces données sont anonymisées. Les auteurs[798] ont démontré que certaines données (telles que le lieu et la date d'achat) sont suffisantes pour identifier 90 % des individus. Les résultats montrent que l'anonymisation traditionnelle des données n'est plus efficace à l'ère du Big Data, car les modèles de comportement financier sont très distinctifs.

236. Le cryptage *end to end*. Par exemple, les applications de messagerie telles que WhatsApp, Signal et Telegram offrent à l'utilisateur des données la possibilité du cryptage de bout en bout (end-to-end) pour toutes les conversations texte ou les appels vocaux. La confidentialité de la communication des données se manifeste par le fait que seuls l'expéditeur et le destinataire peuvent entrer en contact avec les informations utilisées.

237. Double authentification, méthode de sécurisation des données. Une autre caractéristique pourrait être considérée comme essentielle pour la sécurité des données, à savoir le droit d'authentification à deux facteurs 2F, cette possibilité étant accordée aux personnes sous la forme d'un droit d'utiliser deux méthodes différentes pour vérifier l'identité d'une personne, telles qu'un mot de passe et un code généré par une application mobile ou envoyé par SMS, en accordant ainsi au titulaire du droit un niveau de sécurité supplémentaire et empêchant ainsi l'accès non autorisé à ses données.[799]

d). Pseudonymisation

238. Bonnes pratiques en matière de pseudonymisation. La mesure de pseudonymisation des données suppose que les informations personnelles réelles du propriétaire, telles que le sexe, la date de naissance, l'adresse, le nom et d'autres éléments personnels qui sont susceptibles de conduire à son identification, subissent un processus de remplacement par un pseudonyme.[800] La pseudonymisation est une forme intermédiaire de protection des données qui ne les rend pas complètement anonymes, mais les sépare de l'identité directe de la personne, tout en permettant leur utilisation à des fins analytiques ou statistiques sans exposer directement l'individu[801]. Les

[798] Y. A. De Montjoye, L. Radaelli, V. K. Singh et al,. *Op. cit.*
[799] L. Bertrand, M. De Freitas Pereira, J. Y. Marion, *Les capacités offensives de l'intelligence artificielle dans le cyberespace,* Études françaises de renseignement et de cyber, 4(1), 2025, p. 217-233. https://doi.org/10.3917/efrc.243.0218.
[800] B. Texier, *Anonymisation et pseudonymisation au cœur de l'open data judiciaire*, Archimag, 368(8), 2023, p. 26-27. https://doi.org/10.3917/arma.368.0026.
[801] M. Arnaud, *Authentification, identification et tiers de confiance*, Hermès, La Revue, 53(1), 2009, p. 127-136. https://doi.org/10.4267/2042/31488. Avec la prolifération des services en ligne, les frontières entre l'espace privé et l'espace public deviennent de plus en plus floues, et l'authentification (confirmation de l'identité de l'utilisateur) et l'identification (association de l'identité à une personne) nécessitent des mécanismes juridiques, techniques et de confiance sociale. Ainsi, des entités telles que les autorités, les fournisseurs de services numériques et les

actes juridiques européens définissent la « pseudonymisation » comme « le traitement des données à caractère personnel de telle sorte qu'elles ne puissent plus être attribuées à une personne donnée spécifique sans l'utilisation d'informations supplémentaires, à condition que ces informations supplémentaires soient stockées séparément et soient soumises à des mesures techniques et organisationnelles garantissant que ces données personnelles ne sont pas attribuées à une personne physique identifiée ou identifiable ».[802]

Le processus par lequel les données d'une personne sont pseudonymisées suppose que le titulaire des données utilise un pseudonyme ou tout autre identifiant numérique, toute autre identité numérique.[803] En conséquence, les données de l'utilisateur restent des données personnelles, avec la possibilité pour l'utilisateur de les utiliser quand il le souhaite. Ainsi, une connexion appropriée est créée entre l'identité réelle de l'utilisateur et l'identité pseudonymisée, à travers laquelle ses données sont sécurisées.[804]

Seuils de risque vs normes fixes. La pseudonymisation ne doit pas être considérée uniquement comme une obligation technique, mais comme un processus stratégique qui implique la cartographie des flux d'informations, l'application des principes de confidentialité dès la phase de conception et la prise en charge d'une responsabilité continue en matière de protection de la vie privée.[805] Le point de vue européen[806] garantit que la pseudonymisation ne doit pas être confondue avec l'anonymisation, qui implique le processus de suppression de tous « les éléments d'identification d'un ensemble de données personnelles afin que la personne concernée ne soit plus identifiable ».[807] Si les données, une fois anonymisées, ne sont plus des données personnelles, le processus d'anonymisation détruisant tout lien qui permettrait

---

certifications numériques deviennent les pivots de la nouvelle infrastructure d'identité, mais leur rôle doit être réglementé et contrôlé.

[802] Extrait du *Règlement général concernant la protection des données*, article 4, point 5, http://data.europa.eu/eli/reg/2016/679/oj

[803] J. Domingo-Ferrer, J. Soria-Comas, *Anonymization in the Time of Big Data*, in Domingo-Ferrer J. et Pejié-Bach M. (éd.), *Privacy in Statistical Databases*, PSD, coll. « Lecture Notes in Computer Science », vol. 9867, 2016. L'anonymisation se heurte à deux obstacles majeurs : l'augmentation du nombre de données pouvant identifier indirectement une personne et la prolifération de sources de données indépendantes permettant de réassocier les informations, soulignant que l'anonymisation reste utile, mais nécessite des adaptations contextuelles.

[804] De nombreux articles spécialisés abordent la question de l'« anonymisation » des données personnelles à l'ère du Big Data. Bien que l'anonymisation soit souvent présentée comme une solution pour protéger les données, elle comporte des risques sérieux, notamment celui de la réidentification de la personne concernée, en raison de la puissance croissante des algorithmes et de l'interconnexion des bases de données. Voir Information Commissioner's Office, *Anonymisation : managing data protection risk code of practice*, 2012.

[805] B. Texier, *Données personnelles : méthode et outils pour les gérer*, Archimag, 340(10), 2020, p. 26-27. https://doi.org/10.3917/arma.340.0026.

[806] Il s'agit du *Rapport explicatif concernant la Convention 108 modernisée*, où le point 18 mentionne que « *l'utilisation d'un pseudonyme ou d'un identifiant numérique d'une identité numérique ne conduit pas à l'anonymisation des données, car la personne visée reste identifiable ou individualisée* ». Pour le rapport complet, veuillez consulter : J.P.Moiny, C. De Terwangne, J.M. Van Gyseghem, Y. Poullet, *Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques (Partie II)*. Conseil de l'Europe, 2010.

[807] Extrait du *Règlement général concernant la protection des données*, considération 26.

l'identification du titulaire, les données pseudonymisées restent sous la protection de la loi, car elles n'ont pas perdu leur « personnalité », celle-ci étant juste cachée sous un autre nom (pseudonyme).[808] La littérature[809] souligne clairement la nécessité d'une définition juridique du terme « données anonymes », car une qualification incorrecte peut affaiblir la protection des données. Elle propose également que l'anonymisation soit évaluée à l'aide de seuils de risque adaptés au contexte d'utilisation, plutôt qu'à l'aide de normes fixes et restrictives.

239. Critique des approches européennes en matière d'anonymisation des données. Dans une étude publiée dans International Data Privacy Law (2015), C. Álvarez et K. El Emam examinent de manière critique la position du groupe de travail « Article 29 » sur les techniques d'anonymisation. Les auteurs estiment que les recommandations émises par cet organisme européen sont souvent trop rigides et ne tiennent pas compte de l'évolution technologique des méthodes modernes de protection des données. Ils soulignent qu'une application trop prudente du principe d'anonymisation risque de réduire considérablement le potentiel d'utilisation légitime des données dans des domaines tels que la recherche scientifique, l'analyse statistique ou l'innovation numérique. Selon eux, la protection de la vie privée doit s'accompagner d'une approche pragmatique, fondée sur une évaluation contextuelle des risques, et non sur des interdictions généralisées.[810]

e). Disponibilité et intégrité des données

240. Disponibilité des données, principe de sécurité des données. Un autre trait caractéristique du principe de sécurité des données est représenté par la capacité des données à être toujours disponibles pour le titulaire qui est assuré que ses données personnelles sont toujours accessibles et utilisables, à tout moment qu'il souhaite les avoir. L'importance de cette fonctionnalité dans le respect de la vie privée peut être mise en évidence par un exemple opposé, à savoir par des attaques de Déni de service que le titulaire pourrait supporter, risquant ainsi de ne plus avoir accès à ses données personnelles.[811]

---

[808] H. Tanghe, P. O. Gibert, *L'enjeu de l'anonymisation à l'heure du big data*, Revue française des affaires sociales,2017, p. 79-93. https://doi.org/10.3917/rfas.174.0079.
[809] H. Tanghe, P. O. Gibert, *op. cit*.
[810] C. Álvarez, K. El Emam, « *A Critical Appraisal of the Article 29 Working Party Opinion 05/2014 on Data Anonymization Techniques* », International Data Privacy Law, vol. 5, nº 1, 2015, p. 73-87. doi.org/10.1093/idpl/ipu033.
[811] M. Bergeat, D. Blum, N. Cuppens, et al., *Comment anonymiser les données : un panorama non exhaustif des méthodes d'anonymisation*, Dossiers Solidarité et Santé. Données de santé : anonymat et risque de ré-identification, n° 64, 2015.

241. Intégrité des données, principe de sécurité des données. Le principe de sécurité des données se caractérise également par son intégrité, qui garantit à la personne concernée que ses données personnelles ne peuvent être ni modifiées ni altérées sans l'autorisation ou le consentement de la personne concernée.[812] Une approche « tout ou rien » en matière d'anonymisation des données est considérée comme dépassée à l'ère numérique actuelle. Certains auteurs[813] soutiennent qu'il existe une zone intermédiaire, dans laquelle les données sont suffisamment protégées pour réduire les risques d'identification, sans les priver complètement de leur valeur analytique. Ainsi, une protection efficace de la vie privée ne devrait pas reposer sur l'exclusion totale des données, mais sur une gestion intelligente des risques et l'utilisation de techniques de sécurité permettant d'équilibrer innovation et confidentialité.

242. Caractéristiques. L'apparition et la structure des communautés virtuelles transforment les relations sociales, la culture et la manière dont l'identité se construit, reconstruisant le sentiment d'appartenance et redéfinissant l'intimité. C'est pourquoi le maintien de l'intégrité des données personnelles représente une méthode très importante pour la protection de la vie privée.[814] La caractéristique de l'intégrité des données est essentielle pour l'ébauche d'un principe solide en ce qui concerne la protection de la vie privée humaine au moyen de la technologie, dans le cas où la possibilité de modification ou d'altération des données serait autorisée en l'absence du consentement du titulaire des données, nous serions en présence d'un droit d'exercice limité, qui ne correspondrait pas aux valeurs fondamentales des droits et des libertés de l'homme.[815]

243. « Si vous n'avez rien à cacher, vous n'avez pas à vous inquiéter ».[816] Il existe une littérature juridique assez vaste qui contredit ce type d'expression simpliste, que l'on rencontre fréquemment dans le langage courant, et qui exprime l'idée que la surveillance et la collecte de données ne poseraient pas de problème si les personnes concernées ne commettaient pas d'actes illégaux. Dans leur ouvrage intitulé Nothing to Hide: The False Tradeoff between Privacy and Security, les auteurs soutiennent que ce type d'argumentation repose sur une compréhension limitée du concept de vie privée et ignore les multiples façons dont la collecte et l'analyse des données personnelles peuvent affecter l'autonomie, la dignité et la liberté des individus. Le

[812] S. Y. Esayas, *The Role of Anonymisation and Pseudonymisation under the EU Data Privacy Rules : Beyond the "all or nothing" Approach*, European Journal of Law and Technology, vol. 6, nº 2, 2015.
[813] S. Y. Esayas, *op. cit.*
[814] H. Rheingold, *Les Communautés virtuelles. Autoroutes de l'information : pour le meilleur ou pour le pire ?*, Paris, Addison Wesley France, 1995
[815] R. A. Posner, D. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven, Yale University Press, 2011.
[816] R. A. Posner, D. Solove, opt. cit., p. 21

principe de sécurité des données ne doit pas être considéré comme un luxe ou une option passive, mais comme un élément actif d'une société démocratique, et une surveillance étendue, même justifiée par des raisons de sécurité, peut saper les fondements de ce principe si elle n'est pas accompagnée de garanties, de transparence et de contrôle démocratique.[817]

f). Le contrôle, l'information et l'autonomie relatifs aux données

244. Possession, accès et contrôle de vos propres données. Le sentiment d'autorité et d'autonomie du propriétaire sur ses propres données représente, en essence, son droit de contrôler et de gérer ses propres données grâce à la technologie, le caractère de responsabilité sur ses propres actions selon le principe juridique que l'homme est responsable de ses actions et de ses actes. En conclusion, nous sommes dans l'hypothèse de l'exercice équitable du droit à la vie privée dans le contexte de l'évolution de la technologie, seulement si l'utilisateur se voit accorder le droit préexistant inconditionnel de gérer et d'octroyer ou de retirer, le cas échéant, son consentement à la collecte et au traitement de ses propres données.

Une autre caractéristique propre au principe de la sécurité des données est que la personne qui veut sécuriser ses données dispose de lois et règlements clairs et prévisibles dans le pays d'origine. Ainsi, le titulaire des données peut exercer son droit à la vie privée dans un cadre juridique sécurisé, en bénéficiant du droit d'être informé par les autorités et par la législation sur l'élaboration de politiques et procédures appropriées.[818]

245. La propriété absolue de ses propres données, impossible à obtenir ?! Le propriétaire des données privées a le droit de recevoir des informations sur l'utilisation des données, ayant ainsi la possibilité de recevoir une éducation adéquate sur l'exercice même du droit à la vie privée.[819] À mesure que les données deviennent plus utiles pour l'analyse et l'innovation, le risque de réidentification augmente, ce qui rend impossible la propriété absolue dans le contexte des technologies actuelles.[820] À cet égard, nous pouvons mentionner que les détenteurs de données ont le droit que les autorités, les organisations, les institutions, les personnes avec lesquelles ils collaborent reçoivent une éducation sur les risques et les

---

[817] *Idem*, p. 21 – 38.
[818] Organisation des États Américains, Département du Droit International, *Principes actualisés relatifs à la vie privée et à la protection des données personnelles*, Washington, D.C., 2022.
[819] Conseil de l'Europe*, Partie 1. Les opérations de surveillance massive. Surveillance de masse : Quel contrôle démocratique ?* 2016, p. 5-62. Conseil de l'Europe. https://shs.cairn.info/surveillance-de-masse--9789287181039-page-5?lang=fr. Le document explique comment les opérations de surveillance massive, telles que la collecte, le stockage et l'analyse à grande échelle des données de communication, des métadonnées et de la géolocalisation, mettent en danger les droits fondamentaux de l'homme, en particulier le droit à la vie privée et la liberté d'information et d'expression.
[820] L. Maisnier-Boché**,** *Données personnelles. Anonymisation : que faire pour sortir de l'impasse ?*, Expertises, 2016, p. 296-30.

meilleures pratiques, afin de réduire les erreurs humaines et les comportements inappropriés qui pourraient compromettre les données personnelles du propriétaire, mais surtout l'exercice même du droit à la vie privée.[821]

g). Droit à l'image et la protection des photos

246. Image et photographie, données à caractère personnel. Le droit à l'image et à la protection des photographies comprend le droit du titulaire de publier des données personnelles au moyen de photographies, d'images et d'articles.[822] En ce qui concerne cet aspect, la Cour estime que l'image d'une personne est l'une des caractéristiques les plus importantes de sa personnalité, dans le sens où elle exprime ces caractéristiques uniques qui distinguent une personne de ses autres.[823] La Cour suprême a établi que l'atteinte à la vie privée et celle à l'image d'une personne constituent des formes distinctes de préjudice, chacune engendrant une responsabilité propre.[824] Compte tenu de la valeur intime et personnelle de l'image, la jurisprudence européenne considère que le droit d'une personne à bénéficier de la protection de son image est l'un des éléments essentiels liés au développement personnel de cette personne.[825]

Ainsi, puisque « les photographies peuvent contenir des informations très personnelles ou même intimes sur une certaine personne ou sa famille », la Cour estime que la protection des droits et de la réputation de certaines personnes est supérieure à la liberté d'expression[826]

---

[821] S. Wojcik, *La démocratie numérique : illusion ou réalité ?,* Cahiers français, vol. 420-421(2), 2021, p. 88-96. https://doi.org/10.3917/cafr.420.0088.

[822] N. Mallet-Poujol, *Vie privée et droit à l'image: les franchises de l'histoire*, Legicom, n° 20, 1999/4, pp. 51-68. Cet article traite de la relation entre la vie privée et le droit à l'image, ce dernier s'étant progressivement développé comme une branche spécifique du droit de la personnalité. Si, au départ, la vie privée se limitait à la sphère intime (famille, domicile, correspondance), avec l'évolution technologique et médiatique, la notion s'est étendue à la vie sociale et à l'image publique de l'individu. Dans le contexte moderne, la protection de la vie privée par rapport à l'image et à l'information publique devient encore plus complexe, et la jurisprudence doit trouver un équilibre entre l'autonomie de la personne et l'intérêt social à l'information.

[823] C. Berthier, *Droit à l'image et la protection des photos*, fiche pratique no FP-628046, Lexis 360 Intelligence, 2024.

[824] Voir les arrêts de la Cour de cassation : Cass. 1re civ. n° 98-21.161 du 12 décembre 2000, Cass. 1re civ., n° 02-14.730 du 10 mai 2005.

[825] Selon les décisions susmentionnées, le respect dû à la vie privée et la protection de l'image ne se confondent pas, mais se complètent dans le cadre des droits de la personnalité.

[826] Dans la jurisprudence de la Cour, le droit à la liberté d'expression est souvent mis en balance avec le droit à la sécurité des données en termes de protection du droit à la vie privée de la personne concernée. À cet égard, la Cour énonce les critères essentiels à prendre en compte pour la protection de la personne : la contribution à un débat sur l'intérêt général, la notoriété de la personne concernée et le sujet du reportage, sa conduite antérieure, le contenu/la forme/les conséquences de la publication, les circonstances dans lesquelles les photos ont été prises, le degré de sévérité de la sanction imposée.
Sur cela, la jurisprudence est riche : *affaire Axel Springer Af vs. Allemagne (GC),* 2012, pt.89 95, http://hudoc.echr.coe.int/fre?i=001-109035 ; *affaire Couderc et Hachette Filipacchi Associes contra France (GC),* 2015, pt. 90-93, http://hudoc.echr.coe.int/fre?i=001-158855 ; affaire *Dupate contra Letoniei*, 2011, pt. 49-76, http://hudoc.echr.coe.int/fre?i=001-153893

d'autres personnes de publier des photographies[827], même lorsqu'il s'agit de la publication d'une photographie neutre, mais qui est accompagnée d'un commentaire négatif.[828]

247. Le droit à l'image et la protection des photographies : entre vie privée et liberté d'expression.[829] Le droit à la liberté d'expression est souvent mis en balance dans la jurisprudence de la Cour avec le droit à la sécurité des données à la lumière de la protection du droit à la vie privée de la personne concernée.[830] La jurisprudence française et européenne cherche à harmoniser ces deux droits, en soulignant qu'aucun des deux n'est absolu et que la liberté d'expression ne peut justifier une atteinte disproportionnée à la vie privée.[831] À cet égard, la Cour énonce les critères essentiels à prendre en compte pour la protection de la personne.[832]

h). Droit à la protection de la réputation d'une personne

248. La réputation, élément de la vie privée. Le droit à la protection de la réputation d'une personne comprend le droit de ne pas être victime de diffamation. La Cour constate que des millions d'utilisateurs de technologie publient quotidiennement des commentaires qui sont exprimés d'une manière qui pourrait être considérée comme offensante ou, pourquoi pas, diffamatoire. Bien qu'il soit probable que la plupart des commentaires soient de nature moins significative et que leur publication ne prenne pas l'ampleur négative qui affectera la réputation d'une autre personne dans certains cas[833], la Cour a eu tendance à être d'accord avec les juridictions nationales qui ont jugé qu'elle représentait « des insultes vulgaires » dans un registre familier qui est souvent utilisé dans les communications sur de nombreux portails internet. D'autant plus que les commentaires prétendus offensants ont très probablement été interprétés par les lecteurs comme de simples soupçons, qui ne devraient pas être pris au sérieux.

249. La réputation, protégée dans la jurisprudence de la CEDH. Dans une autre affaire[834], la Cour est allée plus loin et a souligné qu'en ce qui concerne les commentaires postés

---

[827] Voir *l'affaire Con Hannover vs Allemagne (nr. 2) (MC),* pt.103, „http://hudoc.echr.coe.int/eng? i=001-109029"
[828] Voir *l'affaire Rodina vs Lettonie*, 2020, pt.131, „http://hudoc.echr.coe.int/fre?i=001-202437"
[829] A. Heymann-Doat, *50 libertés et droits fondamentaux*, 3e éd., Dalloz, coll. « Savoir », 2022. Le droit à la vie privée et le droit à la liberté d'expression sont tous deux des droits fondamentaux dans une société démocratique. Cependant, dans certaines situations, ces deux droits peuvent entrer en contradiction : la liberté de communiquer des idées et des opinions peut porter atteinte à la vie privée.
[830] A. Vignon-Barrault, *JurisClasseur – Responsabilité civile et Assurances, Fasc. 133-10 : Droit à Réparation. – Responsabilité fondée sur la faute. – Atteintes aux droits de la personnalité. Droit à la vie privée. – Droits susceptibles d'atteinte*, Lexis 360 Intelligence, 2022.
[831] Voir la décision de la Cour de cassation, Cass. 1re civ., n° 19-24.780, din 17 februarie 2021. P
[832] A. Lepage, *Droit au respect de la vie privée - Quand la balance entre le droit au respect de la vie privée et la liberté d'expression penche en faveur du premier -,* Communication Commerce électronique, n° 10, comm. 72, Lexis 360 Intelligence, 2023.
[833] Voir *l'affaire Tamiz vs Royaume-Uni* (dec.), pt. 80-81, „http://hudoc.echr.coe.int/eng? i=001-178106"
[834] Voir *l'affaire Pihl vs Suède* (dec.), pt.28, „http://hudoc.echr.coe.int/eng?i=001-172145"

sur un bloc par des tiers, l'article 8 de la Convention protégeant le droit à la vie privée impose aux États contractants une obligation positive d'assurer une protection effective du droit au respect de la réputation des personnes relevant de leur juridiction. Ainsi, les juridictions nationales ont considéré que les réclamations diffamatoires publiées sur internet étaient nulles et non avenues mais, compte tenu des circonstances de l'affaire[835], elles ont refusé d'accorder une indemnisation ou un remboursement des frais de justice au demandeur. La Cour est intervenue et a déclaré que la décision des tribunaux nationaux de ne pas accorder d'indemnisation ne constitue pas en soi une violation de l'article 8 de la Convention, d'autant plus que les déclarations diffamatoires ont été publiées sous forme de commentaires parmi des centaines ou des milliers d'autres commentaires, et le fait qu'elles ont été supprimées par leur auteur dès que le demandeur en a fait la demande, a été pris en compte pour déterminer si le droit à la réputation du demandeur était suffisamment protégé.

Dans le même esprit, la Cour a constaté que l'État dispose d'une large marge d'appréciation en ce qui concerne la liberté d'expression des prestataires de services de la société de l'information, tel que Google Inc., et a souligné que les fournisseurs de services en ligne sont ceux qui ont le rôle important de faciliter l'accès à l'information et au débat sur de multiples questions politiques, sociales et culturelles.[836]

i). Confidentialité des communications électroniques

250. La confidentialité, dimension essentielle du droit à la vie privée. La confidentialité des communications électroniques est un principe essentiel pour garantir la protection de la vie privée grâce à la technologie numérique. Interprété comme l'un des attributs de ce droit, le principe bénéficie de règles européennes spéciales de protection dans le domaine des communications électroniques, à savoir la Directive de la confidentialité et des communications électroniques[837], la Convention 108 modernisée, la Recommandation sur les services de

[835] Voir *l'affaire Egill Einarsson vs Islande* (nr.2), pt. 38-39, http://hudoc.echr.coe.int/eng? i=001-184672
[836] Voir *l'affaire Tamiz vs Royaume-Uni* (dec.), pt. 83-84, http://hudoc.echr.coe.int/eng? i=001-178106
[837] La directive réglemente le traitement des données à caractère personnel dans le cadre de la fourniture de services de communications au niveau de l'UE. Après une première tentative infructueuse en 1997, la directive est adoptée en 2002, modifiée en 2009 pour compléter et adapter les dispositions relatives au secteur des télécommunications . *Directive 2002/58/CE du Parlement Européen et du Conseil du 12 juillet 2002 relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications publiques* (Directive sur la vie privée et les communications électroniques*), JO 2002 L 201, modifié par la directive 2009/136/CE du Parlement Européen et du Conseil du 25 novembre 2009 modifiant la directive 2/22/CE relative au service universel et aux droits des utilisateurs en ce qui concerne les réseaux et services de communications électroniques, Directive 2002/58/CE relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications publiques et règlement no 2006/2004 relatif à la coopération entre les autorités nationales chargées de l'application de la législation en matière de protection des consommateurs, JO 2009 L 337* .

télécommunications [838]et d'autres actes européens.[839] La nécessité d'une réglementation spécifique est née des problèmes posés par l'évolution de l'internet, de la téléphonie mobile et fixe.

251. Principes de confidentialité. Le principe de confidentialité des communications électroniques fait référence à trois catégories principales de données qui sont générées au cours d'une communication :

a) les données contenant le contenu des messages envoyés au cours de la communication ; ces données sont confidentielles.

b) les données appelées « métadonnées » ou « données de transfert », qui comprennent des renseignements sur les participants à la communication (heure et durée de la communication) et qui sont nécessaires pour établir et maintenir la communication.

c) données intitulées « données de localisation », qui comprennent des informations sur l'emplacement spécifique du dispositif de communication et qui sont nécessaires pour indiquer l'emplacement spécifique de tels dispositifs de communication (en particulier les dispositifs de communication mobiles).

252. Nécessité du consentement pour la violation de la confidentialité. Les seules utilisations de données autorisées par le prestataire sont celles effectuées exclusivement à des fins de facturation et de fourniture effective du service. Si le titulaire des données exprime expressément son consentement, ses données peuvent être communiquées par le prestataire de services exclusivement à d'autres prestataires de services à valeur ajoutée, telles que les données sur l'emplacement de l'utilisateur : où se trouve l'arrêt de tramway suivant, la pharmacie la plus proche, les prévisions météorologiques pour la localité où se trouve l'utilisateur, etc.

Tout autre type d'accès aux données relatives aux communications sur les réseaux électroniques doit satisfaire à la condition qu'il s'agisse d'une atteinte justifiée au droit à la protection de la vie privée au moyen de données à caractère personnel.[840]

---

[838] *Recommandation Rec(95)4 du 7 février 1995 du Comité des Ministres du Conseil de l'Europe sur la protection des données à caractère personnel dans le domaine des services de télécommunications*. La recommandation du Conseil de l'Europe réglemente des règles spécifiques en matière de protection des données dans le domaine des télécommunications, avec une référence particulière aux services téléphoniques. Selon cet acte, la collecte et le traitement des données personnelles dans le domaine des télécommunications se fait uniquement dans le but de connecter l'utilisateur au réseau, en mettant à disposition le service spécifique des télécommunications, facturation, vérification, assurance d'un fonctionnement technique optimal et le développement du réseau et du service. La recommandation concerne également les règles d'envoi des messages marketing direct, en précisant que si l'abonné a expressément renoncé à recevoir des messages publicitaires, les messages de marketing direct ne peuvent être adressés à cet abonné. De plus, les appareils d'appel automatisés ne peuvent être utilisés pour envoyer des messages publicitaires préenregistrés que si l'abonné a donné son consentement exprès. Dans ce domaine, le droit national prévoit des règles détaillées.

[839] Des règles importantes concernant le secteur de la confidentialité et des communications électroniques se trouvent également dans le *Règlement général sur la protection des données*, acte de l'Union Européenne.

[840] Un exemple d'ingérence justifiée est l'accès aux données à des fins d'enquête des infractions.

253. Garanties de protection de la confidentialité. À l'heure actuelle, lorsqu'elle se manifeste par des communications électroniques, la vie privée de la personne est protégée par plusieurs mesures appropriées. Ainsi, dans le but de respecter la vie privée de l'individu, il est limité à l'envoi de messages à des fins de marketing direct par courriel, SMS, services de messagerie multimédia et autres applications similaires. En outre, il est expressément interdit d'envoyer des courriels de marketing si le consentement du titulaire n'a pas été obtenu au préalable. En l'absence d'un tel consentement, les messages de marketing ne peuvent être envoyés qu'aux clients existants qui ont mis leur adresse à disposition et n'ont aucune objection.

Une autre garantie de protection, imposée au niveau européen, est le fait que les cookies[841] ne peuvent être installés qu'avec le consentement[842] de l'utilisateur.

En outre, comme mesure de protection appropriée, chaque État a l'obligation d'assurer par le droit national des recours judiciaires concernant la violation de l'interdiction des communications non sollicitées.

Le parcours de l'exercice des garanties a connu différentes situations, comme par exemple, le fait qu'à un moment donné les fournisseurs de services de communication étaient tenus[843] de conserver les métadonnées. Cette mesure n'était pas conforme au droit à la vie privée et, en tant que telle, elle a fait l'objet d'une dérogation.[844]

254. La protection de la confidentialité protège la vie privée. En termes généraux, le principe de confidentialité des communications électroniques vise à protéger la vie privée en obligeant les opérateurs de services de communications électroniques à veiller à ce que l'accès aux données personnelles du titulaire soit limité uniquement aux personnes autorisées, et de prendre des mesures pour prévenir la destruction accidentelle, la perte ou l'endommagement des données à caractère personnel. La protection de la vie privée du titulaire est également assurée par le fait que, lorsque les garanties offertes ont néanmoins entraîné une atteinte à la sécurité du droit, les opérateurs sont tenus dans tous les cas d'en informer l'autorité compétente. En ce qui concerne les personnes physiques, la protection ne s'applique que lorsque cette interférence est susceptible de porter atteinte aux données à caractère personnel et à la vie privée

[841] Les modules cookies sont les logiciels qui surveillent et enregistrent les actions d'un utilisateur d'ordinateur.
[842] Afin de garantir un niveau optimal de protection, la loi nationale de chaque État membre est tenue de réglementer en détail la modalité dont le consentement du titulaire est exprimé et obtenu.
[843] Il s'agit de la *Directive 2006/24/CE du Parlement Européen et du Conseil du 15 mars 2006 concernant la conservation des données générées ou traitées en lien à la fourniture des services de communications électroniques* accessibles ou public ou des réseaux publics de communication ; ainsi que sur la *Directive 2002/58/CE, JO 2006 L 105 qui visait à modifier la première Directive* .
[844] En particulier, la *directive 2006/24/CE* a été déclarée nulle par la CJUE le 8 avril 2014 dans *l'affaire Digital Right Ireland* au motif que l'atteinte à la vie privée n'est pas justifiée, ce qui a été confirmé par plusieurs États à la suite d'une analyse dans des procédures judiciaires.
Il s'agit de la *Cour constitutionnelle fédérale d'Allemagne (Bundesverfassungsgericht*), 1 *BvR 256/08,* 2 mars 2010; de la *Cour constitutionnelle de Roumanie*, *no 1258, 8 octobre 2009*; de la *Cour constitutionnelle de la République Chèque (Ustavni soud Ceske republiky), 94/2011* Coll., 22 mars 2011.

du titulaire. Le principe de confidentialité des communications électroniques se caractérise par le fait qu'il est interdit, en principe, d'écouter, de stocker, d'intercepter tout type de surveillance, de communication et de métadonnées.

C. Les traits essentiels du consentement à l'ère numérique

255. Le consentement, garantie de la protection de la vie privée. Comme nous l'avons vu, l'exercice du droit à la protection de la vie privée dans le contexte de la technologie numérique est assuré par l'application d'attributs qui sont, en fait, les principes d'assurance de la protection de la vie privée de l'individu. Le consentement[845] est un autre principe spécifique pour assurer cette protection[846].

Le consentement est la base juridique même du traitement des données personnelles, car lesdites données doivent être « traitées légalement, équitablement et de manière transparente »[847]. Pour être légalement traitées, les données doivent être obtenues légitimement.

Le consentement fait référence au consentement donné par le titulaire des données pour l'utilisation de ses données. L'accord a la nature d'une action sans équivoque, c'est une manifestation libre, claire, spécifique, exprimée sciemment. S'il s'agit de catégories particulières de données, le consentement doit être principalement explicite.

256. Droit de retirer son consentement. En tant que directive européenne, le titulaire a le droit de retirer son consentement à tout moment[848] et doit être informé à l'avance de la possibilité d'exercer ce droit. Il n'est en aucun cas permis de demander la justification du retrait du consentement et aucun risque de conséquences négatives pour le titulaire des données en cas de retrait, l'action de retrait du consentement doit être aussi simple que l'action de l'accorder[849]. Il est considéré comme un consentement qui n'a pas été donné librement, si le titulaire n'a pas

---

[845] Sur le degré de consentement dans l'exercice de la protection du droit à la vie privée par la technologie numérique, voir les arrêts importants qui ont contribué à l'application de la législation actuelle : arrêt CJEU dans *l'affaire C-543/09 Deutsche Telekom AG/Bundesrepublik Deutschland, 2011* ; arrêt CEDH dans *l'affaire Elberte/Lettonie, no 61243/08, 2015*; arrêt CJUE dans *l'affaire C-536/15 In Tele2 (Pays-Bas) BV et Others/Autroteit Consumer en Markt (ACM), 2017*.

[846] Le consentement de la personne est une base juridique pour la protection de la personne, ce qui ressort de l'arrêt Peck/Royaume-Uni, où il est démontré que *« le demandeur a tenté de se suicider dans la rue en se coupant les veines des mains, ne pas sachant qu'une caméra TVCI l'avait filmé lors de la tentative. Après que la police, qui surveillait les caméras de la TVCI, l'a secouru, ils ont envoyé l'enregistrement de la caméra de la TVCI aux médias, qui l'ont publié sans cacher le visage du plaignant. La CEDH a conclu qu'il n'y avait pas de motifs pertinents ou suffisants pour justifier la divulgation directe au public de l'enregistrement des autorités sans obtenir le consentement du plaignant ou dissimuler son identité* ». La Cour a conclu à une violation de l'article 8 de la convention européenne des droits de l'homme. Plus de détails dans l'affaire Peck/Royaume-Uni dans l'arrêt CEDH du 28 janvier 2003 no 44647/98, p. 85

[847] Cité de l'article 5 du *Règlement général de protection des données*.

[848] Conclusion sortant du *Règlement général de protection des données*, *art. 7 para (3).* Le rapport explicatif concernant la Convention 108 modernisée, point 45

[849] Conclusion sortant du *Règlement général de protection des données, art. 7 para (3).*

la possibilité de retirer son consentement sans subir de préjudice, ou si le retrait du consentement n'est pas aussi simple que de l'accorder[850].

a). Consentement librement exprimé

257. Validité du consentement : conditions, effets, garanties. Un consentement est librement exprimé uniquement « lorsque la personne concernée peut réellement exercer sa liberté de choix et qu'il n'y a aucun risque de tromperie, d'intimidation, de coercition ou de conséquences négatives importantes s'il ne donne pas son consentement »[851].

L'appréciation d'un consentement librement donné s'effectue en analysant l'existence d'un acte conditionnel lié à la conclusion d'un contrat ou même à la fourniture d'un service.

Aussi, en cas de relations de subordination, lorsqu'il peut y avoir un déséquilibre important entre les parties, de quelque nature que ce soit, le consentement peut être remis en question, puisque « les employés ne sont presque jamais en mesure d'accorder librement, de refuser ou de retirer leur consentement, étant donné la dépendance découlant de la relation employeur/employé. Compte tenu du déséquilibre des pouvoirs, les employés ne peuvent donner librement leur consentement que dans des circonstances exceptionnelles, lorsque l'acceptation ou le rejet d'une offre n'a aucune conséquence »[852].

b). Consentement éclairé

258. Information et compréhension, caractéristiques essentielles du consentement. Avant d'exercer une option, le titulaire des données doit disposer de suffisamment « d'informations claires, compréhensibles, exactes et complètes sur toutes les questions pertinentes (…) telles que la nature des données traitées, les finalités du traitement, les destinataires éventuels des données et les droits de la personne concernée »[853]. Le titulaire « devrait être au courant au moins de l'identité du responsable du traitement et des finalités du

[850] Conclusion sortant du *Règlement général de protection des données*, considération 42 ; Le rapport explicatif concernant la Convention 108 modernisée, point 42

[851] Citation tirée du rapport explicatif sur la mise à niveau de la *Convention 108, paragraphe 42*. Voir également *l'avis 15/2011 du 13 juillet 2011 du Groupe de travail « Article 29 »* sur la notion de consentement, WP 187, Bruxelles, 13 juillet 2011, p. 12.

[852] Citation tirée des Conclusions du *Groupe de travail « Article 29 »* qui peuvent être consultées dans l'Avis 2/2017 du 8 juin 2017 du Groupe de travail « Article 29 » concernant le traitement des données au lieu de travail, AWP 249, Bruxelles, le 8 juin 2017.

[853] Citation tirée du Document de travail du 15 février 2007 du *Groupe de travail « Article 29 »* concernant le traitement des données à caractère personnel médicales du dossier de santé électronique (DES), WP 131, Bruxelles.

traitement auquel les données à caractère personnel sont destinées »[854], ainsi que ce qui « implique l'octroi du consentement et la mesure dans laquelle le consentement est accordé »[855].

La langue dans laquelle les informations sont fournies doit être adaptée au niveau prévisible des bénéficiaires, un langage clair et simple sans jargon doit être utilisé, compréhensible par l'utilisateur régulier[856]. Les informations doivent être facilement accessibles, clairement visibles, bien en évidence, exprimées par écrit ou verbalement.

c). Consentement spécifique

259. L'objectif du consentement doit être présenté de manière rigoureuse. Un consentement valable implique également le consentement donné spécifiquement à la finalité pour laquelle les données doivent être traitées. L'objectif doit être décrit clairement et sans équivoque. Le niveau de compréhension du but doit être adapté aux attentes d'une personne ordinaire, et s'il y a plusieurs buts[857] pour tous ces buts[858].

d). Consentement manquant d'ambiguïté

260. La validité du consentement suppose l'absence d'ambiguïté. Dans ce cas, le consentement est obtenu par une déclaration qui est incluse dans la politique de confidentialité, de type « en utilisant notre service, vous consentez au traitement de vos données personnelles »,

---

[854] Citation tirée du *Règlement général de protection des données*, *considération 42.*
[855] Citation tirée du *Rapport explicatif sur la Convention 108 modernisée, point 42.*
[856] Conclusions tirées de *l'avis 15/2001 du 13 juillet 2011 du Groupe de travail « Article 29 » concernant la définition du consentement, WP 187*, Bruxelles, p. 19.
[857] Conclusions tirées du *Règlement général concernant la protection des données, considération 32*
[858] Voir l'arrêt de la CJUE du 15 mars 2017 dans *l'affaire C-536/15, Tele2 (Pays-Bas) BV, Ziggo BV, Vodafone Libertel BV/Autroteit Consumer en Markt (ACM)*, qui concernait la demande de l'entreprise belge tendant à ce que les services d'information téléphonique et les listes d'abonnés exploités par les entreprises attribuant des numéros de téléphone aux Pays-Bas lui permettent d'accéder aux données relatives à leurs abonnés. L'entreprise belge a invoqué une obligation au titre de la directive sur le service universel. Elle obligeait les entreprises qui attribuaient des numéros de téléphone à mettre ces numéros à la disposition des services d'information téléphonique qui en font la demande, lorsque les abonnés ont donné leur consentement à la publication de leurs numéros. Les sociétés néerlandaises ont refusé de le faire, déclarant qu'elles n'étaient pas tenues de fournir les données en question à une entreprise établie dans un autre État membre. Ils ont prétendu que les utilisateurs avaient donné leur consentement à la publication de leurs numéros, étant entendu que ces numéros seraient publiés dans une liste d'abonnés aux Pays-Bas. La CJUE a montré que toutes les demandes émanant de sociétés fournissant des listes d'abonnés sont incluses dans le champ d'application de la directive sur le service universel, quel que soit l'État membre dans lequel elles sont établies. La CJUE a également établi que la transmission des mêmes données à une autre entreprise ayant l'intention de publier une liste d'abonnés sans obtenir le consentement renouvelé des abonnés n'est pas susceptible d'affecter substantiellement le droit à la protection des données à caractère personnel. Par conséquent, il n'est pas nécessaire que l'entreprise qui attribue des numéros de téléphone à ses abonnés inclue, dans la demande de consentement adressée à l'abonné, des informations différenciées selon l'Etat membre auquel les données de l'abonné peuvent être envoyées ».

par laquelle l'utilisateur exprime manuellement et individuellement son consentement. Le consentement est manquant d'ambiguïté lorsqu'il n'existe aucun doute raisonnable quant au fait que la personne concernée souhaitait consentir à l'éventuel traitement de ses données[859].

Lorsque le consentement est donné sous une forme écrite qui fait partie d'un contrat, il doit être individualisé et « les garanties doivent assurer que la personne concernée sait qu'elle a donné son consentement et dans quelle mesure elle l'a fait »[860].

e). Consentement donné pour le compte des enfants

261. Information compréhensible pour les enfants et validité du consentement. La législation européenne prévoit des garanties spéciales pour l'exercice de la vie privée des enfants grâce aux technologies numériques, à savoir une protection spécifique dans le contexte de la fourniture de services de la société de l'information. La garantie spécifique supplémentaire repose sur le fait « qu'ils peuvent être moins conscients des risques, conséquences, garanties en question et de leurs droits en relation avec le traitement des données personnelles »[861]. Dans le cas des enfants, les données à caractère personnel sont légalement traitées dans des conditions respectant la limite d'âge imposée par la législation nationale de l'État.

En droit européen, les données personnelles d'un enfant de moins de 16 ans ne sont légalement traitées sur la base du consentement « que si et dans la mesure où ce consentement est accordé ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant »[862].

Les États membres peuvent prévoir dans leur législation nationale un âge inférieur à 16 ans pour le traitement des données relatives aux enfants sur la base du consentement, mais celui-ci ne peut être inférieur à 13 ans[863]. En ce qui concerne les services de prévention et de conseil fournis directement aux enfants, le consentement du titulaire de la responsabilité parentale à l'égard de l'enfant n'est pas requis[864].

La protection spécifique à l'enfant se manifeste également au niveau de langage, qui doit être clair et simple, compréhensible pour l'enfant[865].

---

[859] Conclusions tirées du *Règlement général concernant la protection des données, article 4 point 11*
[860] Ibidem, considération 42
[861] Citation tirée du *Règlement général concernant la protection des données, considération 38*
[862] Citation tirée du *Règlement général concernant la protection des données, article 8 alinéa (1er) premier paragraphe*
[863] Conclusion extraite du *Règlement général concernant la protection des données, article 8 alinéa (1er) deuxième paragraphe*
[864] Ibidem, considération 38
[865] Tel qu'il apparaît du *Règlement général concernant la protection des données, considération 58.* Voir également la *Convention 108 modernisée, art. 15 alinéa (2) lettre (e*), *Le rapport explicatif concernant la Convention 108 modernisée, points 68 et 125.*

Conclusions du chapitre 1

Le chapitre 1 met en évidence, de manière diachronique, le passage de la définition de la vie privée en tant que notion philosophique à sa configuration en tant que droit fondamental, puis à l'explicitation de la manière dont ce droit est exercé et affecté dans le contexte technologique. La première partie souligne que la vie privée n'est pas un produit exclusif de la modernité, mais le résultat d'une évolution conceptuelle qui distingue progressivement la sphère intime de la sphère publique, offrant une définition opérationnelle capable de soutenir la construction juridique ultérieure. L'analyse du rapport entre le panoptisme et la contrainte psychique fixe le cadre dans lequel la technologie devient un instrument de surveillance et d'intériorisation du contrôle.

La section consacrée à l'émergence du droit à la vie privée dans le contexte technologique montre que le développement des environnements numériques ne génère pas de rupture, mais amplifie les exigences de protection : l'évolution de la technologie et de l'informatique, l'apparition des conventions sur les données personnelles, la datafication, l'influence des algorithmes sur la liberté de choix, le rôle des réseaux sociaux et la configuration du « double numérique » convergent vers l'idée que l'identité de la personne se projette dans un espace virtuel persistant, qui doit être intégré dans la sphère de la vie privée protégée juridiquement.

L'analyse des effets des changements technologiques sur la vie privée met en évidence des conséquences sociales et juridiques directes : la surveillance omniprésente exercée tant par les autorités que par les acteurs privés, l'acceptation volontaire de l'exposition, la nécessité d'un équilibre entre vie privée, sécurité et transparence, ainsi que la nécessité de redéfinir le rapport entre le droit, l'humain et la technologie. Dans ce cadre, des principes précis d'exercice du droit à la vie privée par le biais de la technologie sont identifiés : sécurité et confidentialité des données, utilisation du cryptage, pseudonymisation, garantie de la disponibilité et de l'intégrité des informations, garantie du contrôle et de l'information de la personne, protection de l'image, de la réputation et des communications électroniques.

Enfin, ce chapitre analyse les caractéristiques du consentement à l'ère numérique – caractère libre, éclairé, spécifique, sans ambiguïté, ainsi que les particularités du consentement accordé pour les mineurs – et fixe les critères matériels permettant à l'utilisation de la technologie de rester compatible avec le respect de la vie privée.

Chapitre 2
LES INGÉRENCES DANS LE DROIT À LA VIE PRIVÉE DANS LE CONTEXTE DE L'ÉVOLUTION NUMÉRIQUE

262. Défis émergents: l'ère numérique. À l'ère du numérique, la technologie fait désormais partie intégrante de la vie quotidienne, facilitant les interactions, l'accès à l'information et la rationalisation des processus.. La technologie a entraîné de nombreux défis pour la protection du droit à la vie privée. Le droit à la vie privée, consacré par des instruments fondamentaux tels que l'article 8 de la Convention européenne des droits de l'homme et d'autres instruments internationaux relatifs aux droits de l'homme, est souvent menacé par les interférences technologiques. Ce chapitre explore les principales menaces associées aux technologies modernes, en mettant l'accent sur les pratiques de surveillance illégale, les atteintes à la cybersécurité, l'utilisation de technologies biométriques et la collecte excessive de données par le biais de dispositifs IoT (Internet of Things). L'analyse porte à la fois sur la dimension théorique de ces interférences et sur leurs implications pratiques et législatives.

263. Protection de la vie privée à l'ère numérique. La violation de la vie privée dans le nouveau contexte de la vie numérique est l'un des plus grands défis du droit contemporain, selon la littérature, car l'expansion technologique se poursuit à un rythme sans précédent ; dans ce contexte, les pratiques de surveillance deviennent également de plus en plus sophistiquées et présentent des risques, en particulier en ce qui concerne le droit fondamental à la vie privée de l'individu. Les systèmes juridiques sont constamment soumis à la pression des intérêts nationaux et mondiaux en matière de sécurité, ainsi qu'au besoin d'efficacité administrative ou de croissance économique. Ce chapitre analyse un certain nombre de concepts, de tactiques et d'études de cas, avec une vue d'ensemble de la littérature traitant des violations de la vie privée dans le contexte de l'interférence technologique.

264. Du Panopticon au panoptique numérique. Un premier concept central dans l'analyse de l'interférence technologique dans la vie privée est le « panoptique » proposé par Michel Foucault dans son ouvrage « Surveiller et punir. La naissance de la prison »[866], qui, dans la société contemporaine et selon la littérature récente, suggère que la surveillance continue conduit à l'autocontrôle et à la discipline, et dans les environnements numériques, où les données sont collectées à l'aide de la technologie, comme dans les réseaux sociaux ou l'IoT, un environnement permanent et presque omniprésent de surveillance prend forme (Ball, Haggerty, & Lyon, 2012). Un autre exemple tiré du monde urbain contemporain est le déploiement massif

[866] Voir M. Foucault, *A supraveghea și a pedepsi*, *(Surveiller et punir),* București, Humanitas, 1997.

de la vidéosurveillance (Norris, 2012), qui vise à prévenir et à surveiller la criminalité, mais qui soulève de multiples préoccupations en matière de protection de la vie privée[867].

265. Les instruments du biopouvoir contemporain. Le biopouvoir est un autre concept clé de Michel Foucault, qui se réfère à l'utilisation de techniques de surveillance pour la gestion des populations. Le biopouvoir[868] fait référence à la pratique des États-nations modernes qui, à l'aide d'un éventail de techniques, nombreuses et diverses, visent à « réaliser l'assujettissement des corps et le contrôle des populations ». Foucault a utilisé ce terme pour se référer spécifiquement aux pratiques de santé publique, parmi d'autres mécanismes de régulation (Sfetcu, 2020). Les applications du « bio-pouvoir » au sens de notre recherche sont identifiées dans les activités de collecte de données biométriques, par le biais de bases de données ou de documents de voyage biométriques, sont utilisées pour un contrôle efficace des frontières et la surveillance de l'accès à certaines zones. La littérature suggère que les études de cas sur la mise en œuvre des systèmes de reconnaissance faciale à l'échelle mondiale mettent en évidence les tensions entre le concept de sécurité et les droits fondamentaux des citoyens.

Section 1. **LA SURVEILLANCE CONTINUE MÈNE-T-ELLE À L'AUTOCONTRÔLE ET À LA DISCIPLINE?**

§1. A.I. - INTELLIGENCE ARTIFICIELLE

266. Le fer de lance de l'évolution technologique : l'intelligence artificielle. L'ère numérique, également appelée l'ère de la technologie de l'information, présente de nombreux avantages réels et pose de nombreux défis à la vie privée et à la protection des données, car le processus de collecte et de traitement devient de plus en plus complexe. L'ère de la technologie de l'information est caractérisée par l'utilisation des ordinateurs, d'Internet et de la technologie numérique, ce qui implique la collecte et le traitement de grandes quantités de données personnelles.

L'évolution de la technologie conduit à la reconnaissance de certains ensembles massifs de données qui identifient des modèles ou prennent des décisions basées sur des algorithmes, fournissant une image d'une profondeur sans précédent sur le comportement humain et la vie

[867] Voir C. Norris, *The success of failure : Accounting for the global growth of CCTV* (*Le succès de l'échec: explication de la croissance mondiale de la vidéosurveillance),* en K. Ball, K. D. Haggerty, & D. Lyon (eds.), *Routledge handbook of surveillance studies* (pp. 251-258), Routledge, 2012. p.251-258.

[868] Voir N. Sfetcu, "*Biopolitics in the pandemic COVID-19*," SetThings, 2020. https://www.telework.ro/ro/biopolitica-in-pandemia-covid-19/.

privée[869]. Après de longues analyses, il a été conclu que le citoyen montre de la peur, de l'inquiétude, de la timidité envers la pensée que son comportement et ses actions pourraient être suivis et analysés constamment par l'État, décourageant ainsi les individus d'exprimer leurs propres opinions.

L'intelligence artificielle est un terme qui caractérise l'intelligence des machines appelées « agents intelligents », dont le logiciel a la capacité de percevoir l'environnement dans lequel il se trouve et de connecter des algorithmes pour agir. Plus précisément, l'IA est la manifestation d'une machine qui imite les attitudes humaines, ces fonctions cognitives comme l'apprentissage et la résolution de problèmes spécifiques à une personne physique[870].

267. L'algorithme, base de l'intelligence artificielle. L'algorithme est une procédure spécifique utilisée pour le calcul, le traitement des données, l'évaluation, le raisonnement et la prise de décisions automatisées. En conclusion, les technologies modernes et les logiciels utilisent des algorithmes pour imiter le processus qu'une personne naturelle prend dans la prise de décision. Il s'ensuit que les appareils prennent des décisions automatisées basées sur ces algorithmes.

Un exemple type qui est basé sur la prise de décision automatisée est le profilage[871], qui est fait en fonction de modèles ou de facteurs prédéterminés, le processus décisionnel automatisé de l'intelligence artificielle nécessitant la compilation et le traitement de grands volumes de données qui peuvent provenir d'un environnement avec injuries ou du dispositif lui-même.

268. Prévisions comportementales avec le modèle OCEAN. Pour comprendre le fonctionnement de l'intelligence artificielle, nous nous référons à l'étude scientifique de la personnalité, appelée psychologie moderne, qui utilise une méthode moderne pour déterminer les types de personnalités approchées, appelée la méthode OCEAN[872]. La méthode OCEAN comprend cinq caractéristiques principales[873] de la personnalité d'une personne physique :

---

[869] Conclusions tirées de la *Résolution du Parlement Européen du 14 mars 2017 concernant les implications des métadonnées sur les droits fondamentaux : vie privée, protection des données, non discrimination, sécurité et imposition du respect de la loi,* Strasbourg, 2017. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0076_FR.html

[870] S. Russel, P. Norvig, *Artificial Intelligence: A Modern Approach,* 4e éd., Pearson, 2022.

[871] La création de profils est basée sur des schémas de découverte qui reflètent « *les caractéristiques d'un type particulier de personnalité* », comme la situation où une certaine boutique en ligne propose à l'acheteur des produits que vous pourriez aussi aimer, précisément sur la base des informations recueillies à partir du type de produits achetés et placés par le client dans le panier.

[872] O. Plaisant, J. Guertault, R. Courtois, C. Réveillère, G.A. Mendelsohn, O.P. John, *Histoire des « Big Five » : OCEAN des cinq grands facteurs de la personnalité. Introduction du Big Five Inventory français ou BFI-Fr*, Annales Médico-psychologiques, vol.168, issue7, 2010, p.481-486 https://www.sciencedirect.com/science/article/abs/pii/S0003448710001617

[873] Les cinq caractéristiques majeures de la méthode OCEAN sont appelés « Big Five ».

l'ouverture[874], l'extraversion[875], la conscience[876], l'acceptabilité[877], le névrotisme[878]. Toutes ces informations aident à créer le profil de la personne concernée, en identifiant les besoins, les peurs, comment elle réagit, le comportement, etc. En plus de ce profil psychologique de la personne, des données obtenues à partir de toute autre source disponible, telles que des données provenant des réseaux sociaux[879], la musique que la personne écoute en ligne, les données GPS et les lieux qu'elle fréquente, les données de suivi quotidien de l'itinéraire de la personne et les données associées obtenues auprès des courtiers, des achats en ligne, des intérêts artistiques, etc. sont utilisées. Après la collecte et l'analyse de toutes les données massives trouvées par rapport à une personne particulière, une masse de profils est créée, qui est ensuite comparée dans le but d'identifier des modèles similaires et de construire des groupes de personnalités.

Avec un accès libre aux données sur le comportement et l'attitude d'une personne, elles sont ensuite utilisées pour décrire la personnalité de l'individu, grâce à un test de personnalité inversé. Ce test de personnalité inversé suppose, par exemple, qu'en combinant les informations sur les « appréciations » de la personne des réseaux sociaux, la musique écoutée ou les films regardés, sur les données de localisation et de suivi à travers GPS, par le biais de l'IA, il est possible d'obtenir une image claire sur la personnalité de cette personne. Le processus de collecte, d'analyse et de complément des données, respectivement le processus d'identification de la personnalité d'une personne, ne nécessite pas de temps, car les informations peuvent être traitées en temps réel, ce qui permet à un logiciel intelligent d'envoyer en temps réel[880] des messages publicitaires et des informations adaptées à la personnalité de cette personne.

269. Dynamique de la technologie. La technologie et, implicitement, les techniques modernes de traitement des données sont en constante évolution, bénéficiant de la possibilité d'analyser, de collecter et d'identifier des demandes multiples et simultanées de données et informations différentes, assurant des réponses rapides et en temps réel, y compris en cas de demandes complexes[881].

---

[874] Caractéristique de la méthode OCEAN qui identifie à quel point une personne est ouverte au nouveau.
[875] Caractéristique de la méthode OCEAN qui identifie à quel point une personne est sociable
[876] Caractéristique de la méthode OCEAN qui identifie à quel point une personne est perfectionniste
[877] Caractéristique de la méthode OCEAN qui identifie à quel point une personne est agréable
[878] Caractéristique de la méthode OCEAN qui identifie à quel point une personne est vulnérable
[879] Pour créer le profil d'une personne à partir des informations recueillies sur les réseaux sociaux, y compris les appréciations (likes) de publications, les photos publiées et le message accompagnant la photo publiée sont utilisés - d'autant plus que l'utilisateur utilise hashtag (#), ce qui aide à cadrer la personne beaucoup plus rapidement avec un certain type de profil .
[880] Les techniques de traitement et les logiciels de nouvelle génération évaluent les informations relatives aux préférences d'une personne, analysent le moment où elle effectue des achats en ligne ou ajoute des articles à son panier en ligne en temps réel et peuvent proposer, sur la base des informations collectées, des « produits » susceptibles d'intéresser cette personne.
[881] Le développement de programmes informatiques pour le traitement de grands volumes de données en est encore à ses débuts. Cependant, des programmes analytiques ont récemment été développés, en particulier pour l'analyse en temps réel de données et d'informations massives relatives aux activités des personnes. La possibilité d'analyser

À l'heure actuelle, nous ne parlons pas d'une analyse à petite échelle des données personnelles, mais nous parlons d'une augmentation exponentielle de la quantité de données disponibles analysées, à savoir l'obtention de résultats à grande échelle. L'impact de l'intelligence artificielle sur la vie privée se fait précisément par référence au volume et à la variété des données personnelles traitées et implicitement au résultat obtenu de ces processus.

A. Web 2.0 et web 3.0.

a). L'internet des gens

270. Le passage du web statique (Web 1.0) au web dynamique (Web 2.0). Un attribut essentiel de l'exercice du droit à la vie privée par le biais de la technologie est « le réseautage social » grâce aux services des réseaux sociaux (SNS) qui sont des plateformes de communication en ligne permettant aux individus de se regrouper selon les choses qu'ils ont en commun et ainsi créer de nouveaux réseaux.

L'Internet est né du concept d'un réseau qui interconnecte et transmet des informations entre ordinateurs, la capacité des sites étant réduite seulement à la capacité de visualiser passivement le contenu par les utilisateurs, avec une capacité réduite d'échanger des données[882].

271. Interactivité, connectivité, collecte massive de données, caractéristiques déterminantes du Web 2.0. Aujourd'hui, l'internet est une véritable ère du web 2.0, caractérisée par la présence d'un forum infini dans lequel les utilisateurs interagissent, collaborent et génèrent des contenus.

Le réseautage social[883] est le processus par lequel les individus sont invités à rejoindre un réseau déjà créé, ou à créer un réseau, respectivement sont invités à fournir leurs données personnelles dans le but de créer un profil avec lequel interagir et générer du « contenu » numérique, à savoir photos, vidéos, liens et publications personnelles.

L'interconnexion via le web 2.0. est basée sur l'échange d'informations personnelles entre les utilisateurs, telles que l'âge, le sexe, la localisation, les intérêts personnels. Ainsi, bien

---

et de traiter de manière structurée de grands volumes de données a ouvert de nouvelles voies pour la création de profils et la publicité ciblée. Commission européenne, Communication de la Commission au Parlement Européen, au Conseil, au Comité économique et social européen et au Comité des régions, Vers une économie réussie fondée sur les données COM(2014) 442 final du 2 juillet 2014, Bruxelles; fiche d'information de la Commission européenne sur la réforme de la protection des données dans l'UE dans le contexte des données massives et du Conseil de l'Europe, Lignes directrices sur la protection des personnes à l'égard du traitement des données personnelles dans un monde de données massives , 23 janvier 2017, p.2.

[882] Conclusion appartenant à la Commission européenne (2016) pour le *Développement d'internet d'objets en Europe, SWD (2016),* p.110 final.

[883] Le nom familier de « *réseau social* » est attribué aux services de réseaux sociaux (SNS), ou plus largement aux plateformes de communication sociale.

que les SNS les plus populaires ne facturent pas de frais d'inscription, les fournisseurs de SNS bénéficient des données personnelles divulguées par les utilisateurs. Les rôles et responsabilités des intermédiaires de services internet ont été définis au niveau européen par le Comité des Ministres du Conseil de l'Europe[884], et chaque État membre a adapté ses propres règles.

b). Internet des objets

272. Le passage du Web dynamique au Web sémantique et interopérable. Un attribut - principe essentiel dans la protection de la vie privée par la technologie est le concept d'Internet of Things, en bref IoT, qui se traduit par l'Internet des objets (IdO), y compris le nom Web 3.0. Comme son nom l'indique, l'IoT fait référence aux règles de connexion des objets à Internet, ainsi qu'à l'interconnexion des objets entre eux. L'internet des objets est déjà une réalité actuelle, existant à ce jour des appareils qui peuvent être connectés et interagir avec d'autres appareils via Internet, mais nous sommes à un stade précoce de la technologie, cette ère du web 3.0. promettant d'une évolution fulgurante des appareils intelligents qui créeront des villes intelligentes[885]_bookmark211, des entreprises intelligentes, des maisons intelligentes. L'interaction de l'IoT avec la vie privée se produit lorsque des objets et des personnes sont interconnectés par le biais de réseaux de communication et envoient des rapports sur leur status[886]_bookmark212.

c). Influence sur la vie privée

273. Les nouvelles frontières de la vie privée. Le droit européen soutient que la protection de la vie privée dans le contexte des technologies numériques n'est juridiquement protégée que lorsque le traitement des données à caractère personnel est autorisé par le droit européen. Les

---

[884] Il s'agit d'une référence à la *Recommandation CM/Rec (2018)2 du 7 mars 2018 du Comité des Ministres du Conseil de l'Europe aux États membres sur les rôles et responsabilités des intermédiaires de services internet*, qui a complété la *Recommandation CM/Rec (2012)4 du 4 avril 2012 du Comité des Ministres du Conseil de l'Europe aux Etats membres sur la protection des droits de l'homme en relation avec les services de réseaux sociaux*.

[885] L'une des villes les plus intelligentes est Barcelone, qui utilise des technologies innovantes de gestion des déchets, grâce à des bacs intelligents qui surveillent le niveau des déchets pour optimiser les itinéraires de collecte. Ainsi, lorsque les bacs sont presque pleins, ils envoient des signaux à vider au logiciel de l'entreprise à laquelle ils appartiennent, via le réseau de communication. Grâce au logiciel, l'entreprise peut programmer par priorité le parcours de ramassage des bacs. Les autres technologies innovantes utilisées par Barcelone se réfèrent aux transports en commun, au stationnement, à l'éclairage public, etc.

[886] Conclusion tirée par la Commission européenne dans le Document de travail des services de la Commission, intitulé « *Développement d'Internet des objets en Europe », SWD(2016) 110 du 19 avril 2016*. Le document fait également référence à l'influence de l'IoT sur l'environnement, en ce sens qu'après l'interconnexion par les réseaux de communication, des rapports sur l'état de l'environnement sont envoyés, mais cet aspect ne fait pas l'objet d'intérêt de cette recherche.

fournisseurs de SNS peuvent également traiter les données personnelles des utilisateurs s'ils ont un consentement libre, spécifique, éclairé et sans ambiguïté[887].

L'accord de l'utilisateur sur le traitement des données personnelles est effectué selon les règles générales en matière consentement[888], dans le cadre des plateformes de médias sociaux, cependant, l'obtention d'un consentement libre, spécifique et éclairé pour tous les types de traitement des données effectués par le fournisseur SNS et des tiers peut être considérée comme discutable[889].

B. Homo numericus[890] – mutation identitaire de la personne physique ou sujet de droit?

274. Entièrement numérisé. La révolution numérique s'accompagne d'un besoin de communication instantanée, d'accès immédiat, de simultanéité, donnant naissance à la notion d'*homo numericus*, caractérisé par une connectivité permanente, un accès instantané à l'information et une interaction en temps réel[891]. L'ère numérique transforme l'information en une forme subtile de contrôle, sapant à la fois la vie privée et la démocratie elle-même. Contrairement à l'*homo economicus*[892], produit de la modernité classique, centré sur la rationalité et la maximisation de l'intérêt individuel, l'*homo numericus* est l'individu numérisé, fournisseur permanent de données et d'informations, dans une forme de servitude volontaire qui le rend à la fois vulnérable et captif dans cette bulle informationnelle où le vrai et le faux deviennent difficiles à distinguer. Ainsi, le concept classique de Foucault de « surveiller et punir »[893] est aujourd'hui remplacé par un concept beaucoup plus subtil, « motiver et optimiser »[894].

275. Prochaine étape : l'*homo algorithmicus*. L'*homo numericus* est construit à partir d'une série d'algorithmes d'apprentissage automatique, menant à une redéfinition technologique du

[887] Tiré du *Règlement général sur la protection des données, art. 4, 7* et de la *Convention 108 modernisée, art. 5*.
[888] Nous renvoyons à la section où nous avons traité le consentement dans cette thèse.
[889] Conclusions reprises de *l'Avis 15/2011 du 13 juillet 2011 du Groupe de travail « Article 29 » concernant le concept de consentement, WP 187*, Bruxelles, le 13 juillet 2011, p. 8
[890] M. Clément-Fontaine, « *L'homo numericus* », in Claire Bouglé-Le Roux (dir.), *Le corps et le droit : des cheveux du roi mérovingien à l'homo numericus*, Paris, LexisNexis, 2019, pp. 147-155
[891] G. Boenisch, *Pascal Josèphe, La société immédiate,* Questions de communication, 2008.
[892] U. Mäki (éd.), *Philosophy of Economics*, coll. « Handbook of the Philosophy of Science », sous la dir. de D. M. Gabbay, P. Thagard et J. Woods, Amsterdam – Boston, Elsevier, 2012. 1270 p.
[893] M. Foucault, *Surveiller et punir : Naissance de la prison*. Gallimard, 2014. https://shs.cairn.info/surveiller-et-punir-naissance-de-la-prison--9782070729685?lang=fr.
[894] C. Gruson (2024), Byung-Chul Han, *Infocratie. Numérique et crise de la démocratie*, Paris, PUF, 2023, p. 103. https://shs.cairn.info/revue-hermes-la-revue-2024-1-page-216?lang=fr.

soi et à l'apparition d'un *homo algorithmicus*[895], précaire et dépendant de la technologie[896]. Naît ainsi l'idée que la révolution technologique entraîne des altérations irréversibles de l'essence humaine, avec le risque de perdre la liberté, la dignité et la vie privée. Afin d'empêcher la « fin de l'homme » et de protéger le génome humain en tant que bien commun de l'humanité[897], un cadre juridique ferme et strict est nécessaire pour l'identité numérique[898].

276. Responsabilité pénale ? Une deuxième révolution est celle de l'apparition et du développement de l'intelligence artificielle[899]. L'*homo numericus* est la figure centrale de la civilisation actuelle, incarnant les contradictions du capitalisme numérique[900]. Liberté contre dépendance compulsive, autonomie contre surveillance permanente. Dans ce contexte apparaissent de nouveaux délits commis par le biais d'un système informatique ou contre un système informatique, l'*homo numericus* pouvant être à la fois auteur et victime[901]. À l'ère numérique, l'*homo numericus* n'est plus seulement le bénéficiaire de droits fondamentaux classiques, mais aussi le détenteur de droits connexes, configurés par les nouvelles réalités technologiques. Une analyse progressive de l'*homo numericus* le place comme une forme possible d'intelligence artificielle autonome, dont la responsabilité pénale est l'un des grands défis du XXIe siècle.

277. Tentative de législation. L'importance d'une législation prudente est déjà reconnue par le Parlement européen, dans sa résolution du 16 février 2017, qui contient des recommandations relatives aux règles de droit civil en matière de robotique[902]. Ce projet de législation n'est jamais

---

[895] D.M. Kotliar & R. Grosglik (2023), "On the Contesting Conceptualisation of the Human Body: Between «Homo-Microbis» and «Homo-Algorithmicus»" *Body & Society*, 29(3), 81-108. https://doi.org/10.1177/1357034X231151855 (Original work published 2023).

[896] D.M. Kotliar & R. Grosglik, *op. cit.* : En faisant une comparaison avec le microbiome humain, une interdépendance biologique spécifique et unique à chaque individu, un écosystème composé de milliards de micro-organismes qui, ensemble, forment le corps humain, les auteurs définissent *homo algorithmicus* comme une interaction entre les technologies numériques et algorithmiques, l'identité de l'individu se reconstruisant continuellement à travers les traces numériques et la modélisation algorithmique.

[897] Déclaration universelle sur le génome humain et les droits de l'homme, 11 nov. 1997, art. 1.

[898] F. Fukuyama, *La fin de l'homme. Les conséquences de la révolution biotechnique*, trad. fr., Paris, La Table Ronde, 2002, 320 p.

[899] X. Labbé, « *Respect et protection du corps humain. – L'homme nouveau* », in JurisClasseur Civil Code, art. 16 à 16-14, fasc. 56, LexisNexis, 2021.

[900] H. Guéguen: « *Les contradictions paradoxales de l'expressivité numérique L'étude des modèles identitaires au sein des espaces numériques*. », in Réseaux, 193(5), 2015. p.135-160. https://doi.org/10.3917/res.193.0135.

[901] Selon les statistiques du Ministère français de l'Intérieur, environ 350.000 dossiers relatifs à des infractions numériques ont été enregistrés en 2024. La plupart des infractions signalées concernent l'utilisation d'une fausse identité ou d'une fausse qualité en envoyant un e-mail à la victime afin de l'inciter à communiquer des informations personnelles ou simplement à ouvrir un lien permettant de collecter automatiquement ses données d'identification ou ses coordonnées bancaires. Le rapport met en évidence l'évolution des infractions numériques au cours des dernières années et tire la sonnette d'alarme concernant la réaction du droit pénal. Il peut être consulté ici : https://www.interieur.gouv.fr/Interstats/Actualites/Info-Rapide-n-48-Les-infractions-liees-au-numerique-enregistrees-par-les-services-de-securite-en-2024.

[902] *Résolution du Parlement européen du 16 février 2017 contenant des recommandations à la Commission concernant des règles de droit civil sur la robotique (2015/2103(INL))*
(2018/C 252/25) https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52017IP0051&from=FR

entré en vigueur en raison des contestations[903] formulées tant par les spécialistes en informatique[904] que par les juristes, car il représentait en réalité un premier pas vers l'octroi de la personnalité juridique à l'intelligence artificielle.

278. L'augmentation humaine. Le concept d'*homme augmenté*[905] soulève les mêmes défis juridiques, la difficulté consistant à établir la responsabilité pénale, de sorte que la dignité humaine et la responsabilité pénale ne soient pas annulées par l'innovation technologique.[906]

279. *Homo numericus* – sujet sociologique. Dans une perspective sociologique[907], l'*homo numericus* n'est pas seulement un utilisateur de la technologie, mais un concept heuristique, un nouveau type d'être social, connecté en permanence, accessible en permanence et en constante reconfiguration.

a). Homo numericus – sujet juridique hybride

280. Extension. D'un point de vue strictement juridique, les notions de personne physique et morale sont bien définies, toutes deux ayant des droits fondamentaux (vie privée, intimité, intégrité) et des obligations[908]. En fait, d'un point de vue juridique, la qualité de « sujet de droit » est attribuée aux personnes physiques et morales (par un artifice sémantique) de la naissance à la mort[909]. L'*homo numericus* ne doit pas être considéré uniquement comme un être, mais comme une identité numérique collective, similaire à une personnalité juridique distincte, qui vient comme une extension numérique de la personne physique[910]. Plus encore, il peut être considéré comme un bien d'affectation numérique[911], illustrant ainsi la capacité du droit à

---

[903] G. Loiseau, « *La personnalité juridique des robots : une monstruosité juridique* », in La Semaine juridique. Édition générale (JCP G), n° 22, 2018. p. 1039-1042.

[904] Le message des experts qui ont rédigé une lettre ouverte pour manifester leur opposition à la Résolution du Parlement européen est assez clair : - « *La création d'une personnalité juridique pour un robot est inappropriée d'un point de vue éthique et juridique, quel que soit le modèle de statut juridique. L'impact économique, juridique, sociétal et éthique de l'intelligence artificielle et de la robotique doit être pris en compte sans précipitation ni partialité. Le bénéfice pour l'humanité dans son ensemble devrait primer dans le cadre des règles de droit civil de l'UE relatives à la robotique et à l'intelligence artificielle* » - peut être consulté ici : https://robotics-openletter.eu/.

[905] L'homme augmenté = personne physique dont l'autonomie corporelle peut être remise en question par le contrôle technologique, avec le risque d'une réification, voir M. Clément-Fontaine, « L'*homo numericus* », in « *Le corps et le droit : des cheveux du roi mérovingien à l'homo numericus* » (dir. C. Bouglé-Le Roux), LexisNexis, Paris, 2019, pp. 147-155.

[906] A. Bensamoun, G. Loiseau. « *La gestion des risques de l'intelligence artificielle. De l'éthique à la responsabilité*. », in La Semaine juridique. Édition générale, 2017, p.2063-2072, doctrine 1203. ⟨halshs-02921302⟩

[907] Compiègne, I. (2010), « Chapitre V. Qui est l'*homo numericus* ? La société numérique en question(s) » (p. 59-70). Éditions Sciences Humaines. https://shs.cairn.info/la-societe-numerique-en-questions--9782361060077-page-59?lang=fr.

[908] F. Terré, D. Fenouillet, *Droit civil. Les personnes. Personnalité, incapacité, protection*, 8e éd., coll. « Précis Dalloz », Paris, Dalloz, 2012, n° 10.

[909] F. Rousseau, « *La personnalité juridique* », in « *Traité des droits de la personnalité* », LexisNexis, 2013, p. 57 et suiv.

[910] M. Clément-Fontaine, *op. cit.*

[911] R. Percerou, *La personne morale de droit privé : patrimoine d'affectation*, thèse dactylographiée, Paris, 1951.

répondre aux transformations sociales. Cette reconnaissance présente deux avantages majeurs : la protection de la vie privée (par l'anonymisation numérique) et la clarification de la responsabilité pénale[912].

281. Risque majeur de profilage. Le terme *homo numericus* apparaît également dans l'avis de la CNCDH de 2018 sur la protection de la vie privée à l'ère numérique, ses auteurs remettant en question la protection conventionnelle de la vie privée et réclamant de nouvelles méthodes de réglementation[913]. L'*homo numericus* a besoin d'un droit fondamental de contrôle sur son identité numérique, qui le protège contre les risques de profilage et de réification des données.

282. Réformes législatives numériques. Afin de soutenir la dépendance technologique de l'homme moderne, nous pouvons analyser plusieurs réformes législatives. Le Décret n° 2016-146 du 11 février 2016 impose à chaque municipalité de disposer d'un site web pour la publication des dispositions réglementaires[914]. En 2020, la loi n° 2020-797 du 29 juin 2020[915] relative à la réforme de la justice est adoptée. Elle vise à publier en ligne toutes les décisions judiciaires et administratives, dans le but d'assurer la transparence de la justice et le libre accès à la jurisprudence. Dans le même temps, elle renforce la définition de l'*homo numericus*, en obligeant chaque citoyen à avoir accès à Internet et en introduisant progressivement le terme de justice numérique[916]. Ce phénomène influence également le droit pénal, en permettant la dématérialisation des procédures, les audiences à distance, une meilleure accessibilité et en redéfinissant le rôle du juge[917].

283. La République numérique. Bien entendu, dans ce contexte, une redéfinition de la capacité juridique s'impose également. Une étape majeure dans la gouvernance numérique française a été franchie en 2016 avec l'adoption de la Loi Lemaire (loi n° 2016-1321 du 7 octobre 2016)[918] pour une République numérique, qui met l'accent sur la circulation des données, la protection des individus dans la société numérique et l'accès à l'information. Bien qu'elle fasse partie du Code des relations entre le public et l'administration, cette loi prépare le terrain pour l'intervention du droit pénal dans la cybercriminalité ainsi que pour la responsabilisation pénale des plateformes et des services numériques.

---

[912] M. Clément-Fontaine, *op. cit.*
[913] CNCDH, Avis « *Protection de la vie privée à l'ère numérique* », Assemblée plénière du 22 mai 2018, Paris, 2018.
[914] Décret n° 2016-146 du 11 février 2016 https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032036829.
[915] Décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042055251.
[916] F. Ost, A. Garapon, J. Lassègue, « *Justice digitale. Révolution graphique et rupture anthropologique* », Paris, PUF, 2018, 364 p., in Revue interdisciplinaire d'études juridiques, 81(2), 2018. p.395-403. https://doi.org/10.3917/riej.081.0395.
[917] A. Taleb Karlsonn, « *La procédure pénale numérique* », in Colloque Doctoriales, Toulon, 2021.
[918] *LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique* https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033202746

284. Les débuts. Dans le contexte des tensions actuelles entre le droit à la vie privée (droit fondamental) et les progrès technologiques ayant un impact sur l'intimité, le Rapport n° 441 intitulé « La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information »[919] a été rédigé en France en 2009. Il propose une mise à jour législative, soutenue par des normes juridiques, techniques et institutionnelles. De plus, le rapport souligne la nécessité de former un *homo numericus* actif et conscient, protecteur des données personnelles[920]. Dans ce contexte, des philosophes tels que Marzano[921] soulignent l'émergence du phénomène de la peur technologique, du dépassement des limites humaines et de la perte d'identité. Il souligne également l'indissociabilité de la peur et de la liberté : là où la peur apparaît, la liberté disparaît[922].

285. Inexistant dans le droit roumain. Bien que le terme *homo numericus* apparaisse pour la première fois dans un acte normatif français dès 2009, et qu'il ait été mentionné dans la doctrine auparavant[923], le droit roumain ne l'a pas encore emprunté. Le terme est présent dans « l'esprit » du droit roumain, mais il n'existe actuellement aucun acte législatif qui l'utilise, et la doctrine ne l'a adopté que timidement en 2025[924]. La littérature juridique précitée définit l'*homo numericus* comme le résultat exclusif du progrès technologique : « Le développement des biotechnologies, des technologies d'augmentation des capacités physiques et/ou mentales, des réseaux sociaux et de l'intelligence artificielle a profondément modifié la manière dont l'être humain vient au monde, mène son existence – sa vie intime, privée, familiale, professionnelle – et meurt. L'*homo numericus* est aujourd'hui connecté, collecté, profilé, contrôlé, commercialisé et condamné par le biais même de la technologie »[925].

286. Autonomie et intrusion. La protection pénale de l'*homo numericus* doit couvrir deux dimensions : d'une part, la protection contre l'intrusion dans la vie privée et, d'autre part, le droit à l'autonomie et au développement personnel, c'est-à-dire la capacité d'être soi-même[926]. Ces deux aspects doivent être maintenus dans un équilibre délicat, toute répression ou stigmatisation rappelant les régimes totalitaires du passé et leur intrusion tyrannique dans la vie privée de

[919] Rapport d'information n° 441 (2008-2009), déposé le 27 mai 2009 https://www.senat.fr/rap/r08-441/r08-441.html
[920] Guglielmi, « *Homo numericus*, *un citoyen digitalisé et numérisé conscientisé* », in Drôle d'en-droit – Droits de l'Homme et des Libertés fondamentales, 10 juin 2009, https://www.guglielmi.fr/guglielmi.fr/spipcd4e.html?article199, consulté le 24 août 2025.
[921] M. Marzano, *Visages de la peur*, PUF, coll. La condition humaine, 2009.
[922] M. Marzano, *op. cit.* p. 81-99.
[923] P. Josèphe, *La société immédiate*, Paris, Calmann-Lévy, 2008, 247 p., spéc. p. 139.
[924] L.M. Tec, « *Homo Numericus* : *reflecții și interogații* », Palatul de Justiție, 17 juill. 2025.
[925] L.M. Tec, *op. cit.*
[926] CNCDH, Avis « *Protection de la vie privée à l'ère numérique* », adopté à l'unanimité en Assemblée plénière du 22 mai 2018, Paris, 2018. https://www.cncdh.fr/sites/default/files/2021-04/180522_Avis%20Vie%20privée%20et%20numérique%20pour%20impression_0.pdf

l'individu[927]. Dans la société moderne, le droit institue et garantit la liberté, établissant ainsi des garanties fondamentales[928], telles que la dignité humaine, garantie qui s'applique également à l'*homo numericus*. Actuellement, la protection de l'*homo numericus* repose sur un double fondement européen : le droit traditionnel à la vie privée, conformément à l'article 8 de la CEDH[929] et le droit autonome à la protection des données personnelles, par la Convention 108[930] et son acte additionnel[931].

287. Une menace pour le droit à l'oubli. Une autre sensibilité juridique provient de la mémoire numérique absolue[932] qui caractérise l'*homo numericus*, incapable d'effacer son passé, annulant ainsi son droit à l'oubli, garanti par l'article 17 du RGPD[933]. L'oubli est une fonction vitale de la liberté, de la reconstruction de l'identité et de la protection de la vie privée. Cependant, cette nouvelle forme d'homme numérique, connecté, suppose une présence prolongée, une éternité numérique, survivant même à la mort biologique[934].

288. Sujet de droit hyperconnecté ? Sujet juridique en devenir, l'*homo numericus* n'est pas seulement un concept, mais une réalité sociale et une mutation identitaire qui nécessite un cadre normatif pour canaliser et protéger cette réalité. Il est également nécessaire de redéfinir la notion de « sujet de droit » en « sujet de droit connecté », l'*homo numericus* étant également titulaire d'une identité numérique légale[935]. De nouveaux droits fondamentaux peuvent ainsi être esquissés pour l'*homo numericus*, tels que le droit au partage, caractérisé par la liberté de partager des données et des informations, constituant une garantie de la démocratie dans la société de l'information[936]. Face à une émancipation continue grâce à la technologie, l'*homo numericus* risque de perdre sa vie privée à cause de la surveillance numérique[937]. Cette hyper-

---

[927] Conseil Constitutionnel, Décision n° 2003-467 DC du 13 mars 2003 https://www.conseil-constitutionnel.fr/decision/2003/2003467DC.htm

[928] X. Dijon, (2018). M. Fabre-Magnan, « *L'institution de la liberté* », Paris, PUF, 2018, 350 p. Revue interdisciplinaire d'études juridiques, 81(2), 407-412. https://doi.org/10.3917/riej.081.0407.

[929] European Convention on Human Rights https://www.echr.coe.int/documents/d/echr/convention_ENG

[930] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data https://rm.coe.int/1680078b37

[931] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No. 181) https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=181

[932] Kim, Seonghak, « *L'écologie déséquilibrante de l'oubli chez Homo Numericus* », in Sociétés, n° 116, 2012/2, p. 111-119, OpenEdition Journals, DOI : https://doi.org/10.3917/soc.116.0111.

[933] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (RGPD), JOUE L 119 du 4 mai 2016, art. 17 « Droit à l'effacement ('droit à l'oubli') ».

[934] V. Chuekou, « *Facebook rendrait-il l'homo numericus éternel* ? », in Village de la Justice, 6 oct. 2013 (7 oct. 2013), https://www.village-justice.com/articles/Facebook-rendrait-numericus-eternel,15362.html.

[935] X. Labbée, « *Le sujet de droits sujet connecté* ? », in Gaz. Pal. 31 oct. 2017, n° 37, p. 14.

[936] Laboratoire clé de la stratégie des mégadonnées (éd.), Droit des données 2.0 : Construction du système de droits, Peter Lang, Bruxelles, 2021.

[937] Marc Guerrini, « *Les droits et libertés de l'homo numericus* », communication au colloque Les droits et libertés numériques, Université Côte d'Azur, 7 oct. 2021, disponible sur : https://univ-droit.fr/38530-les-droits-et-libertes-numeriques

connexion représente en réalité une collecte continue de données privées : « l'homme connecté est collecté. Et l'homme collecté fait l'objet d'algorithmes programmés pour lire et contrôler les émotions (chaque like, chaque émoticône), les gestes, le langage (mots), la communication signes, symboles), pour contrôler, manipuler et faire des prédictions sur le comportement »[938].

§2. SÉCURITÉ DES DONNÉES ET SENSIBILISATION À LA PROTECTION DE LA VIE PRIVÉE

289. L'évolution technologique impose la sécurisation des données. La subsection « Sécurité des données et sensibilisation à la protection de la vie privée » traite d'un certain nombre de questions complexes liées à la protection de l'identité numérique à l'ère de l'information et des technologies émergentes qui modifient radicalement les définitions classiques de la vie privée et du comportement humain face à de nouveaux défis.[939] Il se penche sur l'usurpation d'identité numérique, c'est-à-dire la prise de contrôle non autorisée de l'identité en ligne d'une personne, un délit en pleine expansion.[940] En France, la politique d'ouverture et de réutilisation des données publiques (« open data ») – soutenue par des idéaux de transparence, de responsabilisation de l'administration et de valorisation économique – est en tension avec les exigences de protection de la vie privée et des données à caractère personnel.[941] La protection des données personnelles stockées sur des appareils numériques en vertu du code pénal 226-19 et la manière dont ces informations peuvent être compromises par des techniques d'hameçonnage et d'escroquerie sont également abordées. La biométrie est abordée comme un outil ayant un grand potentiel de protection de l'identité, mais avec ses propres défis en matière de confidentialité et de sécurité. La blockchain est considérée comme une technologie émergente qui peut être utilisée pour renforcer l'identité numérique, mais qui soulève des questions sur le droit à la vie privée. Les réseaux sociaux[942] sont examinés en tant qu'environnements dans lesquels l'identité numérique peut être compromise, tant par

---

[938] L.M. Tec, *op. cit.*

[939] G. Galustian, *La protection des données personnelles à l'épreuve du numérique*, Revue du droit public, 2018, p.1389-1415. https://droit.cairn.info/revue-revue-du-droit-public-2018-5-page-1389?lang=fr.

[940] N. Verly, *Usurpation d'identité numérique, cyberharcèlement, revenge porn… : éclairages sur la nouvelle criminalité de l'internet*, Légipresse, 63(HS3), 2020, p. 43-48. https://doi.org/10.3917/legip.hs63.0043. Les transformations numériques ont donné naissance à de nouveaux délits, caractérisés par l'usurpation d'identité en ligne, le harcèlement cybernétique, la divulgation non consentie d'images intimes, etc.

[941] G. Gorce, F. Pillet**,** *La Protection des données personnelles dans l'open data : une exigence et une opportunité,* rapport d'information fait au nom de la commission des lois nº 469, 2014. Le rapport formule plusieurs recommandations : renforcer la législation, garantir des processus d'anonymisation légitimes, classer le droit applicable à la réutilisation des données.

[942] P. Manière, « *Les GAFA* », France Culture, émission Le Monde selon Philippe Manière, 2015. Philippe Manière analyse l'influence économique et politique des grandes plateformes numériques — Google, Apple, Facebook et Amazon — sur la manière dont l'information circule et le pouvoir s'exerce.

l'usurpation d'identité que par le harcèlement en ligne ou le cyberharcèlement. Enfin, la manipulation de l'information dans l'environnement numérique, un phénomène croissant qui peut compromettre la réputation et l'identité d'une personne, est abordée.[943]

A. Technologies émergentes et défis pour la protection de la vie privée

290. Les défis de l'ère numérique. Ce sous-chapitre explore les défis que les technologies émergentes telles que la blockchain, la réalité virtuelle et augmentée, l'IoT ou la technologie 5G, etc. apportent à la protection de la vie privée. Il examine les questions relatives à la collecte des données, à la sécurité et à la protection de la vie privée, ainsi que la nécessité d'un cadre réglementaire actualisé pour relever ces défis.[944]

291. Innovations technologiques. Les technologies émergentes sont une catégorie d'innovations technologiques récentes qui visent principalement à redéfinir divers aspects de la société moderne, notamment les interactions entre les personnes, la façon dont chaque individu travaille et la façon dont les services sont fournis et consommés. Les technologies émergentes les plus importantes du 21e siècle comprennent l'intelligence artificielle, ci-après dénommée IA, l'internet des objets, ci-après dénommé IoT, la blockchain et la réalité augmentée, ci-après dénommée AR[945]. Ces technologies apportent déjà un certain nombre d'avantages majeurs à l'économie, à la santé et à l'éducation, mais ces avantages majeurs entraînent également un certain nombre de défis importants en termes de protection des données personnelles et de la vie privée des utilisateurs.[946]

292. Collecte et stockage des données personnelles. Dans le contexte actuel de numérisation, les données personnelles sont devenues une ressource très importante pour les entreprises et les institutions, grâce aux avantages qu'elles apportent, mais elles exposent en même temps les individus à des risques accrus d'atteinte aux informations personnelles et à la

---

[943] I. Falque-Pierrotin, *La Constitution et l'Internet*, N3C vol.3, n° 36, 2012. Isabelle Falque-Pierrotin, ancienne présidente de la CNIL, analyse les relations entre la Constitution et Internet, soulignant les tensions entre les libertés fondamentales garanties par l'ordre constitutionnel et les nouveaux risques liés à l'espace numérique. L'auteure montre qu'Internet est devenu un espace essentiel pour l'exercice des droits et libertés (liberté d'expression, accès à l'information, soutien à la démocratie), mais aussi une source de vulnérabilités pour la vie privée et la dignité de la personne. Elle soutient que les droits traditionnels doivent être réinterprétés à la lumière de l'environnement numérique afin de maintenir un équilibre.

[944] P. Ohm, Broken Promises of Privacy : Responding to the Surprising Failure of Anonymization, *UCLA Law Review*, vol. 57, 2010, p. 1701.

[945] *Top Technology Innovations in the 21st Century*, Timeline Blog, 2024. consulté le 27 novembre 2024, https://www.cloud4c.com/blogs/timeline-of-the-top-tech-innovations-in-the-21st-century.

[946] *Avantages et inconvénients des nouvelles technologies - Influence de la technologie sur l'activité commerciale*, (*Advantages and Disadvantages of New Technology - Technological Influence on Business Activity)* Eduqas - GCSE Business Revision, BBC Bitesize. consulté le 28 novembre 2024, https://www.bbc.co.uk/bitesize/guides/z4bjjhv/revision/6.

vie privée.[947] La confidentialité et la sécurité des données sont des éléments essentiels protéger, compte tenu de la grande quantité d'informations personnelles collectées par les technologies émergentes.[948] La collecte automatisée de données, le profilage et le stockage de données à long terme sont des facteurs majeurs qui contribuent à accroître les risques pour la vie privée des utilisateurs.[949]

293. Technologies innovantes. Si les technologies émergentes offrent d'énormes possibilités de développement et d'innovation, elles soulèvent également d'importantes questions concernant le contrôle des données à caractère personnel et la transparence de leur utilisation.[950] Par exemple, les technologies de reconnaissance faciale basées sur l'intelligence artificielle[951] peuvent être utilisées à des fins bénéfiques, telles que la protection du public, ainsi qu'à des fins préjudiciables, telles que la protection de la vie privée et de l'anonymat.[952] De même, les dispositifs IoT, tels que les assistants vocaux et les caméras intelligentes, collectent et transmettent des informations personnelles aux entreprises sans que les utilisateurs en soient conscients. En outre, bien qu'elle soit considérée comme un moyen d'améliorer la transparence et la sécurité des transactions, la création de la blockchain pose d'importants défis en matière de protection de la vie privée, car les données stockées sur la blockchain sont permanentes et n'importe qui peut accéder à ces informations. En vertu du Règlement Général sur la Protection des Données (RGPD), l'absence d'anonymat peut exposer des données sensibles, ce qui peut compliquer l'application du droit à l'oubli.[953]

Malgré les nombreux avantages qu'elles présentent, les technologies émergentes soulèvent également de nombreuses questions en matière de protection de la vie privée. Pour trouver un équilibre entre les avantages technologiques et la protection des données personnelles, des stratégies et des réglementations efficaces sont nécessaires pour protéger les droits des utilisateurs. Ce sous-chapitre examine les technologies les plus récentes et les risques qui sont associés, tant au niveau international qu'en Roumanie et en France, en mettant en

---

[947] T. Morey, *Customer Data: Designing for Transparency and Trust,* Harvard Business Review, 2015. consulté le 28 novembre 2024, https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

[948] PwC Romania, *L'impact des technologies émergentes sur les données à caractère personnel et des solutions possibles pour réduire les risques*, Romania Blog, 2022. https://blog.pwc.ro/2022/04/29/impactul- emerging-technologies-impact-emerging-technologies-on-personal-data-and-possible-risk-reduction-solutions/.

[949] LegalUp, *Qu'est-ce que le profilage et comment respecte-t-on le RGPD* ? , 2023. https://legalup.ro/profilarea-risk-persons/.

[950] A. Avram, „*Explorarea Echilibrului între Date Deschise și Confidențialitate*", InfoCons (blog), 2024. https://infocons.ro/explorarea-echilibrului-intre-date-deschise-si-confidentialitate/.

[951] A. Lévêque, *Données et intelligence artificielle : quels enjeux pour la cybersécurité des États ?,* Cahiers français, 419(1), 2021, p. 78-89. https://doi.org/10.3917/cafr.419.0078.

[952] RGPD ; *L'intelligence artificielle et le RGPD – l'impact de l'utilisation de l'IA sur la protection des données à caractère personnel – RGPD Complète*, 2023. https://gdprcomplet.ro/inteligenta-artificiala-si-gdpr/.

[953] Z. Delev, "*The Complex Relationship Between GDPR and Blockchain: Ensuring Compliance in the Decentralised Landscape*", GDPR Local (blog), 2024. https://gdprlocal.com/the-complex- relationship-between-gdpr-and-blockchain/.

lumière les réglementations et politiques actuelles visant à protéger la vie privée et la sécurité des données.

a). Big Brother contre le besoin de likes et de partages

294. Surveillance omniprésente.[954] Dans le roman *1984* de George Orwell, l'auteur fournit un cadre utile pour comprendre la technologie moderne et la manière dont elle a réussi à transformer la perception qu'ont les gens du contrôle et de la surveillance. À l'origine, la surveillance était perçue de manière classique, avec des microphones et des caméras cachées, mais les progrès technologiques des dernières décennies nous ont montré que les technologies développées permettent une surveillance omniprésente, souvent sans que l'on sen rende compte. Ces technologies prennent les désirs de chaque utilisateur et les transforment en ressources pour la collecte de données.[955] Contrairement au contrôle coercitif de la technologie de Big Brother, les plateformes sociales d'aujourd'hui exploitent le désir de chaque personne de créer des liens et de la pertinence par le biais de likes et de partages.[956] Les études sur la contagion émotionnelle démontrent que les flux d'informations manipulés par des algorithmes peuvent influencer les États et les comportements des utilisateurs individuels, ce qui soulève souvent des questions éthiques sur les limites de l'implication de la technologie dans la vie privée des utilisateurs individuels[957].

Dans ce contexte, les limites de la vie privée deviennent de plus en plus floues et, avec le développement continu de la technologie, il pourrait devenir de plus en plus difficile de les réglementer.[958] Le désir humain de rester connecté en permanence aux divertissements peut exposer les utilisateurs à diverses formes de surveillance, non seulement par l'État, mais aussi

---

[954] G. Berthoud, *L'horizon d'une surveillance omniprésente ?,* Revue européenne des sciences sociales, XL(2), 2002. https://doi.org/10.4000/ress.623

[955] B.E. Harcourt, *1.Le Big Brother de George Orwell. La Société d'exposition. Désir et désobéissance à l'ère numérique*, La Seuil, 2020. consulté le 26 novembre 2024, https://acrobat.adobe.com/id/urn:aaid:sc:EU:3ee23e09-e22c-44f0-9f97-754d180f125c

[956] Monitoire-Psychologie, « *Minute d'inspiration: la magie des algorithmes et leur impact sur la psyché humaine* », Monitoire de la Psychologie, 2024. https://monitorulpsihologiei.com/minutul-de-inspiratie-magia-algorithms-and-the-impact-on-the-human-psych/.

[957] F. Durach, «*Expériment : fake news et nos émotions. Comment la colère devient le sentiment le plus important*», spotmedia.ro (blog), 2022. https://spotmedia.ro/stiri/opinii-si-analize/experiment-stirile-fake-news-and-our-emotions-how-our-rage-gets-to-be-the-most-important-feeling.

[958] G. Loiseau*, La valeur contractuelle des conditions générales d'utilisation des réseaux sociaux*, Comm. com. électr., n° 7-8, 2012. Guillaume Loiseau analyse la nature juridique des conditions générales d'utilisation des réseaux sociaux, en discutant de la question de savoir si celles-ci peuvent être considérées comme de véritables contrats entre la plateforme et l'utilisateur. L'auteur montre que, bien que ces conditions remplissent formellement les critères d'un accord de volonté, elles se caractérisent par un déséquilibre structurel, dû au pouvoir unilatéral de la plateforme et à l'absence réelle de consentement éclairé de l'utilisateur.

par des entreprises privées. Cet équilibre précaire entre le désir humain et la vie privée redéfinit la protection de la vie privée à l'ère numérique actuelle.[959]

b). Nouvelles formes de surveillance, collaboration entre les géants de l'informatique et le gouvernement

295. Surveillance invisible. Le concept de « surveillance étatique » reflète la profonde transformation de manière dont les technologies modernes sont utilisées pour surveiller les individus. Les révélations sur les programmes de la NSA tels que Prism et XKeyscore ont mis en lumière le fait que la surveillance n'est plus une activité occasionnelle, mais une pratique systématique et extensive[960]. Grâce aux technologies numériques, les agences de renseignement ont accès à presque tous les détails des activités numériques des utilisateurs - les messages qu'ils envoient et les sites web qu'ils visitent, mais aussi leur localisation physique dans l'espace en temps réel. Contrairement aux formes traditionnelles de surveillance - qui nécessitaient un effort de contrôle actif - ces technologies numériques contemporaines permettent de collecter des données de manière invisible, intégrées dans le tissu numérique de l'utilisation quotidienne[961]. Ce niveau de contrôle soulève des questions sur le degré de protection de la vie privée à une époque dominée par l'interconnexion et l'accès mondial.

296. Interdépendance entre l'État et le secteur privé. Un aspect crucial de ces technologies est l'interdépendance entre l'État et le secteur privé.[962] Des entreprises telles que Microsoft, Google et Facebook jouent un rôle clé dans la facilitation de nouvelles formes de surveillance, non seulement en donnant accès aux données des utilisateurs, mais aussi en développant des technologies spécifiques pour renforcer les capacités des agences de renseignement de chaque

---

[959] DNI, « *La surveillance en masse et le modelage du comportement à l'ère numérique. Qu'est-ce qu'on peut encore en faire ?* », Département du Renseignement National (Roumanie), 2016, https://www.dni.org.ro/supravegherea-in-masa-si-modelarea-comportamentului-in-era-digitala/.

[960] B.E. Harcourt, «*2. L'État de surveillance ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.59-76. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-59?lang=fr.Harcourt.

[961] *La surveillance par les services de renseignements : mesures de protection et les moyens de récupération du préjudice concernant les droits fondamentaux dans L'Union Européenne*, vol.II, European Union Agency for Fundamental Rights, 2020. https://fra.europa.eu/ro/publication/2020/supravegherea-de-catre-intelligence-services-protection-measures-and-remedies.

[962] F. Diaz, **„***Coproduction" de la sécurité : une nouvelle forme de l'interventionnisme étatique* ?, Déviance et Société, vol. 27, n° 4, 2003, p. 429-458. Au cours des dernières décennies, on a assisté à une transition du monopole de l'État sur la protection vers une forme de coproduction de la sécurité, dans laquelle des acteurs privés participent activement à la prévention des risques et à la gestion de l'ordre public. Cette délégation partielle des attributions reflète une reconfiguration du pouvoir public, mais aussi une fragilisation de la notion classique d'autorité étatique. Diaz prévient toutefois que ce « partage » de la sécurité n'équivaut pas à un retrait de l'État, mais plutôt à une forme subtile d'interventionnisme moderne, dans laquelle l'État étend son contrôle par le biais de partenariats et de mécanismes de gouvernance participative. L'article met ainsi en lumière la tension entre efficacité et contrôle démocratique, entre sécurisation de la société et respect des libertés individuelles.

État[963]. Par exemple, Microsoft a développé des solutions qui permettent à la NSA de décrypter les données stockées sur des plateformes telles que Outlook et SkyDrive.[964] Ces partenariats illustrent la manière dont les intérêts économiques des grandes entreprises sont alignés sur les objectifs de sécurité nationale des États, créant un environnement dans lequel les frontières entre le public et le privé deviennent de plus en plus floues.[965] Cette forme de collaboration pose d'importants défis juridiques, car le cadre juridique actuel est souvent dépassé par le rythme accéléré de l'innovation technologique et laisse les utilisateurs exposés à des pratiques invasives et non transparentes.[966]

297. Sacrifier sa vie privée pour profiter des avantages offerts par le développement technologique. En outre, les nouvelles technologies transforment la perception qu'a le public de la vie privée.[967] Bien que les individus affirment attacher de l'importance à la confidentialité, dans la pratique, ils la compromettent souvent en échange des avantages immédiats offerts par la technologie. Les études[968] qui analysent les facteurs cognitifs, émotionnels et sociaux à l'origine de ce paradoxe montrent que les décisions relatives aux données personnelles sont souvent irrationnelles, influencées par le contexte, la confiance et la perception du contrôle. Contrairement aux méthodes traditionnelles de surveillanceperçues comme intrusives et coercitives, les nouvelles technologies redéfinissent cette dynamique en intégrant la surveillance aux avantages que la vie numérique est censée apporter. Les réseaux sociaux, les moteurs de recherche et les plateformes de streaming encouragent les utilisateurs à partager leurs informations personnelles, offrant en retour personnalisation, accès rapide et connectivité[969]. Cette forme de surveillance « volontaire » exploite le désir des utilisateurs de participer activement à leur propre exposition. Dans ce contexte, le droit à la vie privée devient un concept de plus en plus fragile, souvent sacrifié au profit de la commodité numérique. Ce changement fondamental dans la relation entre les individus et la technologie pose des défis

[963] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York, PublicAffairs, 2019.
[964] G. Greenwald et al., "*Microsoft Handed the NSA Access to Encrypted Messages*", The Guardian, 2013. https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user- data.
[965] P. Bruneteaux, *Maintenir l'ordre, les transformations de la violence d'État en régime démocratique*, Paris, Presses de Sciences Po, 1996.
[966] W. Ding, L. Chen, "*Regulating the use of big data : justifications, perspectives and the Chinese way forward*", Computer Law & Security Review, vol.46, 2022. https://doi.org/10.1016/j.clsr.2022.105729.
[967] A. Acquisti, L. Brandimarte, G. Loewenstein, *Privacy and Human Behavior in the Age of Information* , Science, vol. 347, no 6221, 2015, p. 509-514.
[968] A. Acquisti, L. Brandimarte, G. Loewenstein, *op. cit.*
[969] MLFA's Criminal Defense Department, "*How Government Surveillance and Big Tech Erase Your Privacy Rights*, MLFA, 2021. consulté le 28 novembre 2024, https://mlfa.org/how-government-surveillance-and-big-tech-erase-your-privacy-rights/.

importants, notamment en termes de protection des droits fondamentaux dans un environnement numérique en constante évolution.[970]

c). Foucault - Surveiller et punir

298. Interprétation moderne du panoptique. Le modèle du panopticon de Jeremy Bentham, réinterprété par Michel Foucault *dans Surveiller et Punir*, reste une métaphore puissante pour comprendre comment les technologies modernes reconfigurent nos vies privées.[971] Alors que le panoptique traditionnel était défini par une structure architecturale - une tour centrale à partir de laquelle un observateur pouvait voir sans être vu - les technologies numériques d'aujourd'hui ont créé un « panoptisme » invisible mais omniprésent. À la place de la tour d'observation physique, les algorithmes, les caméras de surveillance et les données collectées en masse ont désormais pour rôle de suivre, d'analyser et d'influencer le comportement humain.[972]

Cette adaptation moderne du panoptique rend la surveillance plus insidieuse. Contrairement au système imaginé par Bentham[973], dans lequel les prisonniers savaient qu'ils pouvaient être observés mais ne savaient pas exactement quand[974], la surveillance numérique fonctionne différemment : la plupart des utilisateurs ne sont pas conscients de l'étendue de leur surveillance ou sont indifférents à ses implications.[975] Foucault observait que le pouvoir panoptique fonctionne le mieux lorsque les individus intériorisent le regard de l'observateur, en s'autocensurant ou en ajustant leur comportement.[976] Aujourd'hui, les réseaux sociaux, les applications de localisation et les assistants virtuels utilisent ce principe, transformant notre désir de connectivité en un mécanisme d'exposition constante de soi.[977]

299. L'individu, participant actif à la mise en place des mécanismes de contrôle. Le défi majeur des technologies émergentes n'est pas seulement la surveillance en soi, mais aussi la

---

[970] *Rapports annuels du Contrôleur européen de la protection des données*, European Data Protection Supervisor, 2024. https://www.edps.europa.eu/annual-reports_en.

[971].B.E. Harcourt, «*3. Le Panoptique de Jeremy Bentham ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.77-97. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.

[972] *Ibidem*.

[973] J. Bentham, *Traités de législation civile et pénale*, trad. Étienne Dumont, Paris, Dalloz, coll. « Traités », n° 1, décembre 2010.

[974] *Ibidem*.

[975] R. Cover, *Chapter 8, Digital Surveillance, Archives, and Google Earth: Identities in/of the Digital World*, en *Digital Identities*, Academic Press, 2016. p.243-65. https://doi.org/10.1016/B978- 0-12-420083-8.00008-0.

[976] B.E. Harcourt, «*3. Le Panoptique de Jeremy Bentham ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.77-97. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.

[977] L. Rainie, M. Duggan, "*Privacy and Information Sharing*", Pew Research Center (blog), 2016. https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/.

manière dont cette surveillance façonne les relations de pouvoir et la confiance dans la société. Dans un « panoptique numérique », les individus ne sont plus simplement des sujets de surveillance, mais des participants actifs qui contribuent aux mécanismes de contrôle[978]. Foucault appelait ce phénomène le « pouvoir disciplinaire »[979], mais dans le monde numérique, ce concept évolue vers ce que l'on pourrait décrire comme le « pouvoir collaboratif », où les gens participent volontairement à la création et à l'extension de ces systèmes.[980] Cette dynamique redéfinit la notion de vie privée et met au défi les législateurs et la société civile de trouver des solutions qui rétablissent un équilibre entre l'innovation technologique et la protection des droits fondamentaux.[981]

d). Biométrie et protection de l'identité

300. Données biométriques : moyen d'authentification, risque pour la vie privée. L'identification biométrique est l'un des types d'authentification et de vérification les plus sophistiqués, basé sur l'utilisation de caractéristiques physiques spécifiques de l'utilisateur pour confirmer son identité. En utilisant les empreintes digitales, les traits du visage, l'iris, la rétine ou des indicateurs comportementaux, l'utilisateur est identifié, ce qui lui permet ou non d'accéder à l'information.[982] Les caractéristiques humaines sont difficiles à falsifier et ne peuvent être perdues ou oubliées, comme c'est le cas pour les mots de passe, ce qui fait de l'authentification biométrique l'une des méthodes les plus sûres de vérification de l'identité[983]. Cependant, l'utilisation de l'identification biométrique comporte des risques importants pour la protection des données à caractère personnel. Les données biométriques sont stockées en permanence et, en cas d'incident cybernétique, elles peuvent être compromises. En vertu de la législation européenne et nationale, les données biométriques sont sensibles, ce qui nécessite des mesures strictes pour les protéger. En Roumanie comme en France, le traitement des données biométriques est encadré par le Règlement Général sur la Protection des Données (RGPD), adopté par l'Union Européenne en 2016, qui classe les données biométriques parmi

[978] B.E. Harcourt, « *3. Le Panoptique de Jeremy Bentham ». La Société d'exposition Désir et désobéissance à l'ère numérique,* Le Seuil, 2020. p.77-97. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.
[979] Ibidem
[980] J. van Dijck, *The Culture of Connectivity: A Critical History of Social Media,* OUP USA, 2013.
[981] N. Ochoa, *Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition,* Revue française de droit administratif (RFDA), 2015. L'auteur soutient que les données personnelles ne peuvent être traitées comme des biens commerciaux, car elles expriment une forme d'autonomie de l'individu, qui protège sa dignité et son contrôle sur sa propre identité numérique.
[982] A. Ceyhan, *Enjeux d'identification et de surveillance à l'heure de la biométrie*, Cultures & Conflits, 64(4), 2006, p. 33-47. https://doi.org/10.4000/conflits.2176.
[983] *Biometric Identification - Innovatrics*, consulté le 26 novembre 2024. https://www.innovatrics.com/glossary/biometric-identification/.

les données spéciales, dont le traitement est autorisé dans des cas particuliers et strictement nécessaires, avec le consentement explicite de la personne concernée[984].

301. Du bertillonage aux empreintes digitales. L'évolution de la biométrie trouve son origine dans les progrès technologiques et le besoin croissant de sécurité de l'homme dans le contexte actuel des évolutions sociales et économiques des dernières décennies. En Europe, la biométrie a commencé à être utilisée de manière systématique au début du 20e siècle avec l'introduction de la méthode de « bertillonage » par le criminologue français Alphonse Bertillon. Cette technique, qui consiste à prendre des mesures anthropométriques détaillées pour identifier un délinquant, a été l'une des premières tentatives d'utilisation des caractéristiques physiques d'un individu pour l'identifier. Bien que le bertillonage ait été remplacé par la suite par des techniques plus avancées telles que les empreintes digitales, il a jeté les bases de la biométrie moderne, d'abord adoptée par la police française, puis par d'autres institutions européennes[985].

302. Technologie biométrique : utilisation internationale. Aujourd'hui, la technologie biométrique est utilisée dans presque tous les pays membres de l'Union Européenne, ayant comme principal objectif sécuriser les documents d'identité. Les passeports biométriques intègrent les empreintes digitales et les images faciales et constituent une norme requise par le règlement (CE) n° 2252/2004, qui vise à prévenir la falsification des documents et à améliorer la sécurité des frontières et de l'État[986]. En France, le système PARAFE (Passage Automatisé Rapide Aux Frontières Extérieures) est utilisé, les données biométriques permettant aux voyageurs de passer rapidement les points de contrôle, un modèle qui a été utilisé et adopté par d'autres pays européens[987]. En Roumanie, la biométrie a été adoptée de la même manière dans les documents d'identité et les passeports, conformément aux exigences imposées par l'Union Européenne[988]. La mise en œuvre de la technologie aux points de passage frontaliers est un exemple son utilisation pour prévenir l'immigration illégale et le trafic d'êtres humains[989]. Les institutions gouvernementales roumaines utilisent également des systèmes biométriques pour

---

[984] R. Sava, «*La protection des données en Roumanie par le Règlement RGPD. Quels sont les aspects les plus importants ?*», 2023. https://legalup.ro/protectia-datelor-in-romania/.

[985] S.A. Cole, *Suspect Identities*, Harvard University Press, 2001. consulté le 2 décembre 2024. https://www.hup.harvard.edu/books/9780674010024.

[986] *Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres*, http://data.europa.eu/eli/reg/2004/2252/oj/ron.

[987] *Passage rapide aux frontières : comment utiliser un sas Parafe ?,* Service public, 2024. consulté le 2 décembre 2024, https://www.service- public.fr/particuliers/vosdroits/F35295?lang=fr.

[988] *Le passeport biométrique: qu'est-ce que c'est, documents nécessaires, prix et validité*, Wise, 2022. https://wise.com/ro/blog/pasaport-biometric.

[989] Police de Frontière, *Synthèse des activités de la Police de Frontière réalisées en 2022*, Police Roumaine de Frontière, 2023. https://www.politiadefrontiera.ro:443/ro/main/i-sinteza-activitatilor-politiei-de- frontiera-desfasurate-in-anul-2022-32510.html.

authentifier les employés et sécuriser les informations sensibles. Ces développements reflètent une tendance générale en Europe à intégrer la biométrie dans l'infrastructure nationale pour répondre aux défis contemporains en matière de sécurité[990].

303. Utilisation tant dans le secteur public que dans le secteur privé. Au-delà du secteur public de chaque État, la biométrie joue un rôle clé dans le secteur privé, en particulier dans les domaines de la technologie et des services financiers. Par exemple, les systèmes d'authentification biométrique utilisés par des entreprises comme Apple[991] et Samsung[992] permettent aux utilisateurs d'accéder à des appareils mobiles ou d'effectuer des paiements sans contact, en utilisant des caractéristiques telles que les empreintes digitales ou la reconnaissance faciale. En France, en Roumanie et dans d'autres pays européens, ces technologies sont intégrées dans les applications bancaires pour sécuriser les et prévenir la fraude. Les entreprises du secteur de la santé utilisent également la biométrie pour protéger les données des patients en fournissant un accès sécurisé aux dossiers médicaux électroniques[993]. L'utilisation extensive de la biométrie va au-delà de l'authentification et de la sécurité. Les technologies modernes permettent également des applications dans d'autres domaines tels que l'éducation, les transports publics et les loisirs. Dans les universités, par exemple, la biométrie est utilisée pour contrôler l'assiduité des étudiants ou pour sécuriser l'accès aux salles d'examen[994].

304. Données biométriques : identification unique, authentification. La technologie biométrique peut être classée en deux catégories distinctes : l'authentification et l'identification. Bien que ces deux processus utilisent des caractéristiques biométriques uniques, ils diffèrent considérablement dans leurs objectifs, leurs méthodes et leurs risques potentiels. L'authentification biométrique consiste à vérifier l'identité déclarée d'une personne en comparant un « échantillon biométrique » fourni à un « échantillon » précédemment stocké. Ce processus est couramment utilisé dans les appareils mobiles, les applications bancaires et les systèmes d'accès sécurisé.[995] Par exemple, des technologies telles que l'Apple ID d'Apple ou les capteurs d'empreintes digitales intégrés dans les téléphones mobiles permettent aux

---

[990] Loi n° 363/2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention, de détection, d'enquête, de poursuite et de répression des infractions pénales ou d'exécution des peines, des mesures éducatives et de sécurité, ainsi qu'à la libre circulation de ces données. Consulté le le 2 décembre 2024, https://lege5.ro/gratuit/gmytinjygqza/art-5-lege-363-2018.

[991] *Apple Pay*, Apple. Consulté le 2 décembre 2024, https://www.apple.com/apple-pay/.

[992] *More than a Wallet*, Samsung Electronics America, consulté le 2 décembre 2024, https://www.samsung.com/us/samsung-pay/.

[993] *Biometrics in Healthcare: Applications, Advantages, Challenges*, ITRex (blog), 2021. https://itrexgroup.com/blog/biometrics-in-healthcare-applications-advantages-challenges/.

[994] *Benefits Of Using Biometrics In Educational Institutions*, CompuLynx, 2021. https://compulynx.com/resources/benefits-of-using-biometrics-in-educational-institutions/.

[995] S. E. O. Team, *What Is Biometric Authentication and How Does It Work?*, LoginTC (blog), consulté le 2 décembre 2024. https://www.logintc.com/types-of-authentication/biometric-authentication/.

utilisateurs d'accéder rapidement et en toute sécurité à leurs appareils et à leurs données personnelles. L'authentification biométrique est également utilisée dans le secteur financier pour autoriser les transactions numériques, réduisant ainsi le risque de cyberfraude[996]. L'identification biométrique, quant à elle, est basée sur la recherche et la reconnaissance d'une personne sans qu'elle ne décline directement son identité. Ce procédé est principalement utilisé dans les applications gouvernementales et de sécurité.[997] En France, l'identification biométrique a également été utilisée lors d'événements publics, tels que le Carnaval de Nice, pour identifier des personnes potentiellement suspectes[998]. En Roumanie, ce procédé est le plus souvent utilisé aux points de contrôle frontaliers, afin de permettre l'identification de personnes sans documents valides et d'assurer un niveau élevé de sécurité pour l'État et les pays limitrophes[999].

305. Risques d'usurpation d'identité, de surveillance et de discrimination. Les risques associés à l'utilisation de la biométrie sont divers et comprennent des problèmes de confidentialité, de sécurité des données et de discrimination. Contrairement aux mots de passe traditionnels, les données biométriques sont uniques et permanentes, ce qui les rend extrêmement précieuses mais aussi vulnérables aux failles de sécurité. L'un des risques les plus graves est la compromission des données biométriques. En 2019, une importante faille de sécurité a exposé les données biométriques de millions d'utilisateurs dans une base de données gérée par la société Suprema, y compris des empreintes digitales, des scanners faciaux et des informations personnelles.[1000] Cet incident a montré à quel point les mesures de sécurité sont essentielles pour protéger les données biométriques. Un autre risque est l'utilisation généralisée de la reconnaissance faciale dans la surveillance de masse. En France, par exemple, les autorités ont testé la reconnaissance faciale pour surveiller les manifestations, ce qui a suscité des inquiétudes quant à d'éventuels abus et violations de la vie privée.[1001]

---

[996] C Kuraku, .et.all., *Biometric Authentication In Digital Payments: Utilizing AI And Big Data For Real-Time Security And Efficiency Educational Administration: Theory and Practice,* vol.26(4), SSRN, 2020. p.954-964. https://doi.org/10.2139/ssrn.4977530.

[997] *Biometrics (Facts, Use Cases, Biometric Security)*, Thales, 2023. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics.

[998] S. Mayhew, *Facial Recognition Software Tested during Carnival in Nice*, Biometric Update, 2019. https://www.biometricupdate.com/201902/facial-recognition-software-tested-during-carnival-in-nice.

[999] *Les dispositifs de pré-enregistrement dans le cadre du système d'entrée/de sortie EES,* Ministère de l'Interieur, 2025. Le nouveau système d'entrée/de sortie (EES) sera en service le 12 octobre 2025. La France déploiera progressivement ce nouveau système aux points de passage frontaliers et sera pleinement opérationnel d'ici le 10 avril 2026.

[1000] Z. Doffman, "*New Data Breach Has Exposed Millions Of Fingerprint And Facial Recognition Records: Report*", Forbes, 2019. consulté le 2 décembre 2024, www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/.

[1001] Civic Space Watch, *FRANCE: Plagued by Mass Protests and New AI Surveillance Law*, 2023. consulté le 2 décembre 2024, https://civicspacewatch.eu/france-plagued-by-mass-protests-and-new-ai-surveillance-laws/#postcontent.

Cependant, depuis l'introduction et l'intégration de cette technologie, la biométrie a soulevé un certain nombre de défis éthiques et techniques. Une étude menée par le MIT Media Lab a révélé que les algorithmes de reconnaissance faciale peuvent avoir des taux d'erreur significativement plus élevés chez les femmes et les personnes de couleur, ce qui met en évidence les risques de discrimination et de biais algorithmiques. En outre, l'utilisation de données biométriques dans les espaces publics sans consentement explicite a suscité et continue de susciter de vives critiques de la part de la société civile et est perçue comme une menace vie privée[1002]. La réglementation législative joue un rôle crucial pour garantir l'utilisation responsable des technologies biométriques, protéger les droits fondamentaux et prévenir les abus. Dans l'Union Européenne, le Règlement Général sur la Protection des Données (RGPD) définit le cadre juridique du traitement des données biométriques, qui sont classées comme des données sensibles.[1003] Selon le RGPD, le traitement des données biométriques n'est autorisé que dans des cas exceptionnels, tels que la protection des intérêts vitaux de la personne concernée, le respect d'obligations légales ou le consentement explicite de l'individu[1004].

e). Blockchain et identité numérique

306. Identité numérique : l'architecture de la personne dans l'espace en ligne. Le contexte technologique actuel a révélé l'importance de l'identité numérique dans la société d'aujourd'hui, où les interactions et les transactions en ligne sont devenues un élément déterminant de la vie quotidienne. L'identité numérique est définie comme l'ensemble des informations qui décrivent une personne dans le cyberespace. L'identité numérique peut comprendre des éléments tels que le nom, l'adresse, l'historique en ligne ou d'autres informations permettant d'identifier une personne. L'identité numérique peut en fait être associée à l'identité en ligne d'un individu[1005]. Qu'il s'agisse d'accéder à des services financiers, à des réseaux sociaux ou à des plateformes d'administration en ligne, chaque individu a l'obligation morale de gérer et de sécuriser son identité numérique.

[1002] *Les dispositifs de pré-enregistrement dans le cadre du système d'entrée/de sortie EES,* Ministère de l'Interieur, 2025. Le nouveau système d'entrée/de sortie (EES) sera en service le 12 octobre 2025. La France déploiera progressivement ce nouveau système aux points de passage frontaliers et sera pleinement opérationnel d'ici le 10 avril 2026.

[1003] *What Personal Data Is Considered Sensitive?*, European Commission, consulté le 2 décembre 2024, https://commission.europa.eu/law/law-topic/data-protection/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en.

[1004] *General Data Protection Regulation (GDPR*), Art. 9 - Processing of Special Categories of Personal Data, consulté le 2 décembre 2024, https://gdpr-info.eu/art-9-gdpr/.

[1005] L. Popa, *Qu'est-ce que c'est l'identité numérique et pourquoi est-elle importante*, Capital, 2023. consulté le 27 novembre 2024, https://www.capital.ro/ce-este-identitatea-digitala-si-de-ce-este-importanta-tot-ce-trebuie-sa-stiti.html.

307. La lutte contre l'usurpation d'identité : la technologie Blockchain. Compte tenu du nombre croissant de cybermenaces, notamment la fraude, l'usurpation d'identité et l'accès non autorisé aux données personnelles. La sécurité et le contrôle de l'identité numérique deviennent donc une priorité pour les individus, ce qui a également conduit à la reconnaissance de la technologie blockchain comme une solution viable permettant de relever un grand nombre des défis actuels liés à la gestion de l'identité numérique.[1006] La blockchain est connue pour ses caractéristiques de décentralisation et d'immutabilité, qui permettent un stockage et une gestion sécurisés des données sans dépendre d'une entité centralisée. La blockchain est également un grand livre partagé, qui facilite le processus d'enregistrement des transactions d'une personne et le suivi des actifs d'un réseau d'entreprises[1007]. En fait, grâce à la blockchain, toute personne a la possibilité de suivre les transactions d'une personne sans que son identité ne soit révélée. Grâce à la blockchain, les données transactionnelles sont divisées en blocs qui sont partagés, chaque bloc ayant des identifiants uniques sous la forme de hachages cryptés. De cette manière, l'intégrité des données est assurée par une source d'information unique, ce qui rend impossible la duplication des données et accroît la sécurité[1008].

308. Contrôle absolu sur vos propres données. Un concept central dans ce domaine est l'identité auto-souveraine (SSI), qui donne aux utilisateurs un contrôle total sur leurs données personnelles. Ce modèle est basé sur la technologie blockchain et élimine le besoin d'intermédiation des données partagées, ce qui permet à tout utilisateur de décider qui et quand les informations personnelles peuvent être consultées, ce qui facilite le processus de sécurité et de confidentialité des données[1009]. En ce sens, un système blockchain offre la possibilité de prévenir la fraude et la falsification des données, car les données ne peuvent pas être modifiées sans l'autorisation de plusieurs participants au registre[1010].

f). Réseaux sociaux et protection de l'identité

309. Les réseaux sociaux : extensions de la vie réelle. Les réseaux sociaux sont devenus une partie intégrante de la vie moderne, permettant aux gens d'interagir, de partager des informations et de créer de nouvelles communautés en ligne. Selon le rapport *We Are Social*,

---

[1006] *Blockchain Identity Management: Complete Guide 2024*, Truvera, 2024. consulté le le 27 novembre 2024, https://www.dock.io/post/blockchain-identity-management.
[1007] *What Is Blockchain* ?, IBM, consulté le 27 novembre 2024, https://www.ibm.com/topics/blockchain.
[1008] *Qu'est-ce que c'est Blockchain?*, Oracle, consulté le 26 novembre 2024, https://www.oracle.com/ro/blockchain/what-is- blockchain/.
[1009] R. Chirila, *Identité numérique auto-souveraine pour tous*, LinkedIn, 2021. consulté le 26 novembre 2024, https://www.linkedin.com/pulse/identitatea-digitala-auto-suverana-radu-chiril%C4%83/.
[1010] *Qu'est-ce que c'est Blockchain*, Oracle, consulté le 26 novembre 2024, https://www.oracle.com/ro/blockchain/what-is- blockchain/.

d'ici 2023, le nombre d'utilisateurs de réseaux sociaux dans le monde dépassera les 4,9 milliards, soit environ 60% de la population mondiale totale[1011]. L'expansion rapide des interactions sociales en ligne a par la suite également conduit à une augmentation exponentielle de la quantité de données personnelles partagées, faisant de la protection de l'identité une priorité absolue pour les utilisateurs, mais aussi pour les plateformes sociales qui imposent des réglementations spécifiques visant à protéger l'identité[1012].

310. L'identité numérique, infrastructure critique des réseaux sociaux. L'identité numérique, telle que définie dans le sous-chapitre précédent, est à la base des réseaux sociaux, car chaque utilisateur doit se forger une identité numérique qui lui est propre. Dans le contexte des réseaux sociaux, chaque utilisateur a la possibilité de créer une identité numérique réelle ou fausse, en fonction des activités qu'il souhaite entreprendre en ligne. Fréquemment, les utilisateurs ont tendance à fournir autant d'informations personnelles que possible, sans avoir une idée générale des risques associés à cette tendance[1013]. Par exemple, sur des plateformes telles que Facebook et Instagram, qui sont toutes deux les réseaux sociaux les plus utilisés au monde, les utilisateurs de ces plateformes téléchargent quotidiennement un grand nombre de photos, ce qui les rend également très vulnérables aux attaques par hameçonnage, au vol de données personnelles et à d'autres techniques d'exploitation numérique.

311. Statistiques inquiétantes. Une enquête du *Pew Research Centre* a montré qu'environ 64% des internautes se préoccupent activement de la manière dont les entreprises administrent, gèrent et protègent les données personnelles des utilisateurs[1014]. Ce niveau élevé d'inquiétude reflète les risques accrus associés à l'utilisation des réseaux sociaux, mais aussi l'impact que la collecte et l'utilisation inappropriées des données personnelles peuvent avoir sur les utilisateurs. Au niveau de l', l'introduction du Règlement Général sur la Protection des Données (RGPD) en 2018, a conduit à des réglementations strictes sur la collecte et l'utilisation des informations personnelles, donnant à tous les utilisateurs un grand nombre de droits d'accès, de suppression et de partage de ces données[1015]. En Roumanie comme en France, la mise en œuvre du GDPR

[1011] *Digital 2023 : Global Overview Report*, DataReportal - Global Digital Insights, 2023. https://datareportal.com/reports/digital-2023-global-overview-report.

[1012] *Protection des données et de la vie privée en ligne*, Your Europe, consulté le 27 novembre 2024, https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_ro.htm.

[1013] *ENISA Threat Landscape 2022*, Report/Study, ENISA, 2021. consulté le 27 novembre 2024. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022. Raportul analizeaza amenintarile cibernetice la nivelul UE si ofera recomandari de contramasuri. ENISA a fost creata in 2004, prin Regulamentul UE nr.460/2004 si este functionala din 2005. In 2019, a fost consolidata prin Actul de Securitate Cibernetica al UE.

[1014] B. Auxier, et all., "*Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*", Pew Research Center (blog), 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and- privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[1015] B. Wolford, *What Is GDPR, the EU's New Data Protection Law?,* GDPR.eu, 2018. https://gdpr.eu/what-is-gdpr/.

a constitué une avancée majeure pour garantir la protection des utilisateurs, obligeant les entreprises à respecter et à adapter des normes élevées au niveau de la vie privée et de la sécurité.

312. Le cryptage, moyen de protection de l'identité numérique. Outre les réglementations légales qui ont été imposées au niveau de l'UE, les plateformes sociales telles qu'Instagram et Facebook, qui font toutes deux partie de la société Meta, ont introduit un grand nombre de mécanismes supplémentaires pour protéger les utilisateurs et leurs comptes, par exemple l'authentification en deux étapes (2FA)[1016].Les plateformes ont introduit le cryptage de bout en bout pour protéger les communications privées entre les utilisateurs afin qu'elles ne puissent pas être interceptées ou lues par des tiers sans avoir reçu l'approbation sur demande. L'un des exemples les plus notables est celui de Whatsapp, qui encourage la protection active des messages, des appels et des fichiers multimédias entre les utilisateurs[1017].

313. Campagnes d'éducation numérique continue. Le nombre de campagnes d'éducation à la sécurité en ligne a également augmenté ces dernières années, des organisations telles que l'Internet Society et l'Electronic Frontier Foundation offrant un large éventail de ressources et de guides visant à protéger les identités numériques, en se concentrant principalement sur l'importance d'utiliser des mots de passe sécurisés[1018] et de maintenir une vie privée stricte[1019]. Cependant, l'efficacité des mesures promues par les organisations dépend principalement du comportement des utilisateurs individuels. À cet égard, l'une des mesures les plus utiles pour générer et stocker des mots de passe complexes consiste à utiliser des applications spécifiquement conçues pour effectuer ces opérations[1020].

314. La vulnérabilité des réseaux sociaux. Depuis leur apparition, les réseaux sociaux constituent un environnement vulnérable pour les utilisateurs, principalement pour protéger leur identité numérique. Chaque utilisateur partageant de plus en plus de données personnelles, les cyber-attaques ciblant ces plateformes deviennent de plus en plus sophistiquées. Cela peut rendre chaque utilisateur plus vulnérable d'être victime d'une cyberattaque. Les principaux risques pour l'identité numérique sont le phishing, l'usurpation d'identité, le doxing et d'autres techniques avancées d'exploitation des données, qui seront examinées ci-dessous.

[1016] *Comment fonctionne l'authentification en deux étapes sur Facebook*, Facebook Help Centre, consulté le 26 novembre 2024. https://www.facebook.com/help/148233965247823.

[1017] *About end-to-end encryption*, WhatsApp Help Center, consulté le 26 novembre 2024, https://faq.whatsapp.com/820124435853543/?locale=en_US.

[1018] *Creating Strong Passwords*, Surveillance self-defense, 2023. consulté le 26 novembre 2024, https://ssd.eff.org/module/creating-strong- passwords.

[1019] *Fiche sur les politiques publiques: Introduction à la confidentialité sur l'Internet,* Internet Society (blog), 2015. consulté le26 novembre 2024, https://www.internetsociety.org/policybriefs/privacy/.

[1020] *How to create a secure password*, Norton, consulté le 26 novembre 2024. https://us.norton.com/blog/how-to/how-to-choose-a-secure-password.

315. Le *phishing*, principale menace pour l'identité numérique. La principale menace identité numérique reste le *phishing* (l'hameçonnage). Sur les réseaux sociaux, cette forme d'attaque se manifeste par l'envoi de messages directs entre deux ou plusieurs utilisateurs ou par de faux messages, généralement promus, qui usurpent l'identité d'entreprises ou de personnes connues. Selon le 2024 Verizon Data Breach Investigations Report, les attaques par hameçonnage ont été impliquées dans environ 68% de toutes les atteintes à la sécurité signalées dans le monde au moment de l'étude[1021]. En outre, les plateformes sociales constituent un environnement favorable pour les attaquants, car ils peuvent accéder à la liste de contacts de la victime pour faire paraître les attaques plus légitimes. En général, toute personne a un niveau de confiance élevé envers ses amis et connaissances en ligne, et les attaquants profitent de cette vulnérabilité.

Le vol d'identité comprend l'utilisation de données personnelles et d'informations partagées sur Internet et les réseaux sociaux pour créer de faux comptes, obtenir des prêts bancaires ou d'autres avantages financiers, ou pour commettre des infractions pénales.[1022] Au niveau mondial, le vol d'identité a augmenté environ 354% depuis 2023, la majorité des pertes causées par la fraude provenant du transfert de crédit. Au niveau de l'Union Européenne, ont été causées des pertes d'environ 1,13 milliard d'euros, les transactions à distance étant les plus couramment utilisées par les attaquants, représentant environ 99% de ces vols[1023]. Selon une étude d'IN Groupe, quelque 210.000 personnes sont touchées chaque année en France par l'usurpation d'identité numérique, ce qui représente 4,2 % des infractions signalées[1024]. Martin T. Bigelman souligne dans son livre *Identity Theft Handbook : Detection, Prevention and Security que* la protection des informations personnelles sur Internet est cruciale, car elles représentent la monnaie la plus précieuse de chaque utilisateur, et que chaque individu doit donc adopter une approche préventive et faire attention aux informations qu'il partage sur Internet[1025].

316. Le concept de transparence numérique : tout voir et être toujours vu. Le chapitre « Notre pavillon en verre-miroir » explore le concept de « société en verre-miroir », où les individus non seulement ils participent activement à leur propre surveillance, mais ils

---

[1021] *2024 Data Breach Investigations Report*, Verizon, consulté le 26 novembre 2024, https://www.verizon.com/business/resources/reports/dbir/.
[1022] *Identity theft*, USAGov, consulté le 26 novembre 2024. https://www.usa.gov/identity-theft.
[1023] A. Bercea, *Le vol d'identité a augmenté de 354% par rapport à l'année précédente. L'augmentation du nombre d'interactions dans l'espace numérique est l'une des principales raisons*, Libertatea, 2024. Consulté le 26 novembre 2024. https://www.libertatea.ro/stiri/furtul-de-identitate-a-crescut-cu-354-comparativ-cu-anul-precedent-cresterea- number-of-interactions-in-the-digital-space-one-of-the-main-reasons-5038379.
[1024] *Fraud: What Exactly Is Digital Identity Theft?,* IN Groupe, consulté le 26 novembre 2024. https://ingroupe.com/insights/fraud-digital-identity-theft/.
[1025] M. T. Biegelman, *Identity Theft Handbook : Detection, Prevention, and Security,* John Wiley & Sons, 2009.

deviennent également des acteurs de la surveillance des autres.[1026] Cette dynamique transforme les réseaux sociaux en un espace paradoxal : un espace dans lequel les utilisateurs recherchent la reconnaissance et la connexion, mais compromettent en même temps la confidentialité et la sécurité de leur identité numérique. Facebook, Instagram ou TikTok fonctionnent comme de véritables « pavillons de verre », où chaque post, photo ou commentaire devient une pièce d'un puzzle qui construit un profil détaillé de l'utilisateur.[1027] Ces informations ne sont pas seulement visibles par les amis et la famille[1028], mais deviennent souvent accessibles à des tiers - entreprises, gouvernements ou même pirates informatiques.[1029] Harcourt souligne comment les utilisateurs acceptent ce compromis par désir d'être vus, aimés ou validés, réaliser pleinement les implications de leur exposition.[1030] Par exemple, les algorithmes qui personnalisent les fils d'actualité ou les publicités fonctionnent en analysant le comportement des utilisateurs, ce qui crée un environnement où la vie privée est subordonnée aux intérêts économiques et commerciaux des plateformes numériques[1031].

317. Visibilité obligatoire : pression sociale et esthétique. Un autre aspect des réseaux sociaux est la manière dont ils affectent la perception de l'identité des utilisateurs. L'article note que dans cette « société de l'exposition », l'identité devient non seulement quelque chose que l'individu contrôle, mais aussi quelque chose qui se construit à travers le prisme du regard des autres.[1032] Ce processus crée une pression constante pour se conformer à certaines normes sociales ou esthétiques, ce qui peut conduire à des problèmes de perception de soi et même à des risques psychologiques[1033]. En outre, l'absence de contrôle sur les données partagées - une fois qu'elles sont téléchargées sur les plateformes - expose les utilisateurs à des risques

---

[1026]. B.E. Harcourt, *«4. Notre pavillon en verre-miroir ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.101-124. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-101?lang=fr.

[1027] *Identité numérique européenne*, Commission Européenne, consulté le 27 novembre 2024. https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_ro.

[1028] K.Terrell, G. Wright, K.Yasar, *What Is Social Networking and How Does It Work ?*, TechTarget Definition, 2025. consulté le 27 novembre 2024, https://www.techtarget.com/whatis/definition/social-networking.

[1029] T. J. Holt, D.A. Strumsky, O. Smirnova, M. Kilger, *Examining the Social Networks of Malware Writers and Hackers*, International Journal of Cyber Criminology, vol.6(1), 2021. le 22 octobre 2024, https://www.researchgate.net/publication/265260799_Examining_the_Social_Networks_of_Malware_Writers_and_Hackers.

[1030] B. E. Harcourt *« 4. Notre pavillon en verre-miroir ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.101-124. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-101?lang=fr.

[1031] A. Jivan*, «Comment fonctionne l'algorithme Facebook et comment on peut enlever les réclames de l'étape d'apprentissage (learning)?»,* LinkedIn. Consulté le 27 novembre 2024, https://www.linkedin.com/pulse/cum-func%C8%9Bioneaza- algorithm-facebook-%C8%99i-sco%C8%9Bi-advertising-alex-jivan/.

[1032] B.E. Harcourt, « *4. Notre pavillon en verre-miroir ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.101-124. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-101?lang=fr.

[1033] McLean Hospital, "*Here's How Social Media Affects Your Mental Health*. consulté le 27 novembre 2024, https://www.mcleanhospital.org/essential/it-or-not-social-medias-affecting-your-mental-health.

supplémentaires, tels que l'usurpation d'identité ou l'utilisation abusive d'informations personnelles[1034].

318. Le défi de la protection des données personnelles. Alors qu'ils s'intègrent de plus en plus dans la vie quotidienne, la protection de l'identité des utilisateurs reste un défi majeur. Dans un tel environnement, la législation joue un rôle essentiel mais insuffisant pour répondre à la complexité de ces questions. Il faut des mesures réglementaires plus strictes, mais aussi une éducation plus approfondie des utilisateurs sur le fonctionnement de ces plateformes et les risques qui y sont associés. Ainsi, les réseaux sociaux ne devraient pas seulement être un lieu d'exposition, mais aussi un lieu qui protège et respecte les droits fondamentaux des utilisateurs à la vie privée et à l'identité numérique.

B. Protection de l'identité numérique

319. Le vol d'identité numérique, conséquence du progrès technologique. L'usurpation d'identité numérique, également connue sous le nom de vol d'identité, désigne l'acte consistant à revendiquer frauduleusement l'identité d'une autre personne dans l'espace numérique. Elle implique également l'utilisation d'un document volé à une personne présentant des caractéristiques similaires, qui peut également être combiné avec des documents falsifiés, par exemple en remplaçant l'image de la carte d'identité d'une personne réelle par l'image de l'imposteur[1035]. Il s'agit également de tous les types de délits dans lesquelles la personne qui s'approprie les données de la victime pour commettre des délits de fraude ou de tromperie en vue d'un gain financier. Ainsi, les informations personnelles, les listes, les comptes bancaires, les informations sur les cartes de crédit ou de débit ou d'autres données d'identification qui peuvent être utilisées pour ouvrir des comptes afin d'obtenir un prêt ou une hypothèque[1036].

320. Rapports inquiétants concernant l'usurpation d'identité. Avec les progrès technologiques et l'utilisation accrue de l'internet, le vol d'identité numérique est devenu un problème majeur à l'échelle mondiale. Selon un rapport annuel de la Commission fédérale du commerce (FTC) des États-Unis, en 2020, l'usurpation d'identité a été classée comme le délit en ligne le plus courant, avec plus de 1,4 millions de plaintes[1037]. Par ailleurs, une étude menée

---

[1034] K. Lewis, "*How Social Media Networks Facilitate Identity Theft and Fraud*", Octane Magazine. consulté le 27 novembre 2024. https://member.eonetwork.org:443/octane-magazine/special-features/social-media-networks-facilitate-identity- theft-fraud.

[1035] FATF*, Indrumari cu privire la identitatea digitala,* FATF, Paris, 2020. consulté le 27 novembre 2024, https://ro.scribd.com/document/726540933/Guidance-on-Digital-Identity-RO-1-identitatea-digitala-ceccar.

[1036] J. Kremling, A. M. Sharp Parker, SAGE Publications Inc, *Cyberspace, Cybersecurity, and Cybercrime,* SAGE Publications, 2017.

[1037] FTC, *Consumer Sentinel Network Data Book,* Federal Trade Commission, 2020. consulté le 27 novembre 2024, https://www.ftc.gov/reports/consumer-sentinel-network-data-book-2020.

par Javelin Strategy & Research en 2021 a révélé que les pertes financières liées à la fraude d'identité dépassaient 56 milliards de dollars, ce qui souligne l'impact financier de ce phénomène sur l'économie mondiale[1038].

a). Usurpation d'identité numérique en France

321. Le vol d'identité numérique, un délit depuis 2011 en France. L'usurpation d'identité numérique est un délit grave en France et est officiellement reconnue par la LOI n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure. En vertu de l'article 226-4-1 du code pénal français, tout acte d'usurpation d'identité numérique est puni d'un an d'emprisonnement et de 15 000 euros d'amende[1039]. Selon cet article, l'usurpation d'identité est définie comme le fait pour une personne d'utiliser sans droit l'identité ou toute information permettant d'identifier une autre personne, dans le but de nuire à sa réputation, à sa tranquillité ou à son intégrité[1040]. Cette définition inclut l'utilisation frauduleuse du nom, de la photographie personnelle, de l'adresse électronique ou d'une adresse similaire, ou de toute autre donnée personnelle d'une personne, dans le but d'induire celle-ci en erreur ou d'obtenir un avantage. La loi a été introduite pour prévenir le nombre croissant de cybercrimes, car les données personnelles sont vulnérables au vol et à l'utilisation non autorisée. Avec l'augmentation du nombre d'utilisateurs des réseaux sociaux, ce phénomène a facilité l'accès aux informations personnelles, faisant de l'usurpation d'identité numérique un problème majeur pour l'État français.

322. L'usurpation d'identité, traitée sévèrement par le droit français. Un exemple notable s'est produit en 2017, lorsqu'un ingénieur informaticien a profité d'un dysfonctionnement du site web d'un homme politique français, qui a créé un faux site web avec le nom et la photo de l'homme politique. En créant le site en question, d'autres personnes ont pu créer et poster de faux communiqués de presse, ce qui a considérablement nui à la réputation du responsable politique[1041]. Ces affaires similaires montrent le sérieux avec lequel les autorités françaises traitent les cas d'usurpation d'identité et les sanctionnent sévèrement. Dans l'affaire précitée, l'ingénieur informaticien a été condamné à une amende de 3.000 euros et un complice

---

[1038] J. Buzzard, T. (K.) Goldberg, *2021 Identity Fraud Study: Shifting Angles*, Javelin Strategy & Research, 2021. https://www.javelinstrategy.com/research/2021-identity-fraud-study-shifting-angles.

[1039] Code pénal, Article 226-4-1, consulté le 27 novembre 2024. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193593/2021-02-11.

[1040] *Ibidem*.

[1041] A.-L. Villedieu, H. Chalmeton, «*Usurpation d'identité numérique: Premiers enseignements de la jurisprudence*», CMS Law, 2017. consulté le 27 novembre 2024. https://cms.law/fr/fra/news-information/usurpation-d-identite-numerique.

à une amende de 500 euros[1042]. En substance, le droit français définit explicitement l'usage abusif de l'identité numérique et prévoit des sanctions sévères pour les contrevenants. En outre, sur la base du droit de l'Union Européenne, la France assure l'un des plus hauts niveaux de protection des données personnelles dans l'environnement numérique.

b). Protection des informations personnelles contenues dans les fichiers ou stockées sur l'ordinateur

323. Sensibilisation aux risques numériques. À l'heure actuelle, le concept de *security awareness* (sensibilisation à la cybersécurité) est devenu une mesure de protection impérative que tout utilisateur connaître pour pouvoir la mettre en œuvre. La croissance exponentielle de l'utilisation des technologies de l'information et de l'internet, ainsi que la diversification des méthodes de cyber-attaques, soulignent importance d'une sensibilisation accrue aux risques de sécurité à tous les niveaux de la société.[1043] *Security awareness* ne se limite pas à la mise en œuvre de solutions technologiques sophistiquées, mais implique également d'éduquer les utilisateurs pour qu'ils adoptent un comportement responsable et préventif. Sans une solide culture de la sécurité, même les systèmes de protection les plus avancés peuvent être compromis.

324. Reconnaissance des menaces cybernétiques actuelles. La définition du concept de *security awareness* fait référence au niveau de connaissances, de compétences et d'attitudes que les utilisateurs acquièrent pour reconnaître et contrer les cybermenaces.[1044] Cette sensibilisation s'étend à des pratiques telles que la reconnaissance des tentatives d'hameçonnage, l'utilisation de mots de passe complexes, la mise à jour régulière des logiciels et l'évitement du téléchargement de fichiers à partir de sources non sûres. Le rôle de l'éducation dans ce processus est crucial, et la cybersécurité doit être considérée comme une responsabilité individuelle, qu'il s'agisse d'utilisateurs à domicile ou d'employés d'une organisation.

325. Comprendre les bonnes pratiques en matière de cybersécurité. En même temps, *security awareness* est un processus continu, qui évolue en fonction des nouvelles menaces et technologies. Alors que les cyberattaques deviennent de plus en plus sophistiquées et que des techniques telles que l'ingénierie sociale et les ransomwares[1045] sont de plus en plus utilisées,

---

[1042] *Ibidem*.

[1043] Student Center, « *L'importance de la cybersécurité à l'ère numérique* », studentcenter.ro, 2024. https://studentcenter.ro/2024/09/11/importanta-securitatii-cibernetice-in-era-digitala/.

[1044] D. Gitlan, « *Qu'est-ce que la sensibilisation à la cybersécurité ?* », SSL Dragon, 2023. https://www.ssldragon.com/ro/blog/cybersecurity-awareness/.

[1045] S. Fronczak, *Ransomware : le dossier comprendre l'ennemi. Revue Cyber & Conformité*, 1(1), 2021. P.25-30. https://doi.org/10.3917/cyco.001.0027.

la sensibilisation et la formation des utilisateurs deviennent les méthodes les plus efficaces pour protéger les informations personnelles.[1046] Au niveau mondial, l'importance de la sensibilisation à la sécurité est reconnue par le biais d'initiatives et de réglementations promouvant l'éducation à la cybersécurité. Dans l'Union Européenne, des directives telles que la directive NIS (Network and Information Systems Directive) imposent des normes strictes en matière de mesures préventives et de formation des employés. En Roumanie, ce concept est abordé à la fois par la législation et par des campagnes d'information du public, qui mettent l'accent sur la nécessité de protéger les données personnelles et les systèmes d'information. Malgré les efforts déployés, il existe encore un besoin aigu d'intégrer ce concept dans la culture organisationnelle et la routine quotidienne de chaque utilisateur.[1047]

La sensibilisation à la sécurité n'est donc pas un ensemble de règles, mais une façon de penser et d'agir face aux cybermenaces. Il s'agit d'adopter une attitude proactive, qui comprend une formation constante, une évaluation régulière du niveau de connaissance et l'application de mesures préventives dans les activités quotidiennes.

326. La négligence et le manque de connaissances, les armes de la cyberattaque. La sensibilisation à la cybersécurité est essentielle pour protéger les informations personnelles stockées sur les ordinateurs et dans les fichiers. Dans un monde numérique en constante évolution, les utilisateurs sont souvent considérés comme le maillon faible de la chaîne de sécurité[1048]. Les cyber-attaquants exploitent souvent le comportement humain, comme la négligence ou le manque de connaissances, pour compromettre des données sensibles[1049]. Par exemple, les attaques par hameçonnage, qui visent à obtenir des informations confidentielles par la tromperie, sont devenues de plus en plus sophistiquées et difficiles à détecter en l'absence d'une formation adéquate.

327. Modèles de cybersécurité : Zero-Trust. La mise en œuvre de programmes de sensibilisation à la cybersécurité dans les organisations et les établissements d'enseignement contribue de manière significative à la réduction des risques liés aux cyberattaques. Ces programmes forment les utilisateurs à reconnaître et à éviter les menaces, adopter des pratiques sûres lorsqu'ils utilisent la technologie et à réagir de manière appropriée dans les situations à risque. Selon une étude menée par Microsoft, quatre des meilleures pratiques en matière de

---

[1046] « *L'importance de la sensibilisation à la cybersécurité* », Service Technologie de l'Information et Cybersécurité, 2022. https://stisc.gov.md/ro/comunicate-de-presa/importanta-constientizarii-securitatii-cibernetice.

[1047] National Institute of Standards and Technology (NIST), *NIST Special Publication 800-12: An Introduction to Computer Security*, chapitre 13: *Awareness, Training and Education*, 2004,consulté le 27 novembre 2024, https://csrc.nist.rip/publications/nistpubs/800-12/800-12-html/chapter13.html.

[1048] I. Goian, "*End User Security Awareness – Solutions Sécurité*", Dendrio (blog), 2021. https://www.dendrio.com/blog/end-user-security-awareness/.

[1049] D. Gitlan, « *Qu'est-ce que la sensibilisation à la cybersécurité ?* », SSL Dragon, 2023. https://www.ssldragon.com/ro/blog/cybersecurity-awareness/.

cybersécurité sont l'activation d'une stratégie de sécurité « Zero Trust », la mise en place de processus de cybersécurité, l'investissement dans des solutions globales et la protection des données personnelles.[1050] En outre, la sensibilisation à la cybersécurité favorise le respect des réglementations légales et des normes internationales. Par exemple, la directive NIS 2 de l'Union Européenne établit un cadre réglementaire commun pour la cybersécurité, exigeant des États membres qu'ils renforcent leurs capacités en matière de cybersécurité et introduisant des mesures de gestion des risques et des exigences en matière de rapports pour les entités critiques et importantes.[1051]

328. L'importance de la formation en matière de cybersécurité. La mise en œuvre d'un programme efficace de sensibilisation à la sécurité au sein des organisations est essentielle pour se protéger contre les cybermenaces. Selon une étude menée par Bit Sentinel, l'éducation des employés à la cybersécurité contribue de manière significative à la réduction des risques associés aux cyberattaques.[1052] Une formation continue adaptée à des rôles spécifiques est cruciale. Les employés doivent être régulièrement formés à reconnaître les différentes cybermenaces et à y répondre de manière appropriée[1053]. Par exemple, le personnel informatique doit être formé à la détection et à la gestion d'attaques complexes, les services de première ligne, tels que les ventes ou les relations avec la clientèle, doivent se concentrer sur l'identification des tentatives d'hameçonnage et d'autres formes d'ingénierie sociale.

329. Intégration de la formation technologique dans le système éducatif. L'intégration des technologies pour soutenir l'éducation peut accroître l'efficacité des programmes de sensibilisation. L'utilisation de plateformes d'apprentissage en ligne et de tests de sécurité simulés permet aux employés d'apprendre dans un environnement contrôlé et de développer les compétences nécessaires pour faire face à des menaces réelles[1054]. Par exemple, la mise en œuvre de campagnes d'hameçonnage simulées peut aider à évaluer les niveaux de sensibilisation et à identifier les domaines à améliorer. Des politiques claires en matière d'utilisation des appareils et d'accès aux données sont également essentielles. Les organisations devraient établir des règles claires sur l'utilisation des appareils personnels à des fins

---

[1050] Microsoft Security, « *Qu'est-ce que la cybersécurité ?* », Microsoft,consulté le 27 novembre 2024, https://www.microsoft.com/ro-ro/security/business/security-101/what-is-cybersecurity.

[1051] *Cybersécurité des réseaux et des systèmes d'information*, EUR-Lex, 2022. consulté le 27 novembre 2024, https://eur-lex.europa.eu/RO/legal-content/summary/cybersecurity-of-network-and-information- systems-2022.html.

[1052] *Instruction et sensibilisation à la cybersécurité (Instruire și conștientizare în securitatea cibernetică)*, Bit Sentinel (blog), consulté le 27 novembre 2024. https://bit-sentinel.com/ro/cursuri-practice-de-cyber-security-si-awareness/.

[1053] Ibidem.

[1054] C. Ducu, *Integrarea Tehnologiilor Noi Și Emergente În Sistemul Educațional Românesc (Intégration des technologies nouvelles et émergentes dans le système éducatif roumain*), EduPol, 2019. consulté le 27 novembre 2024, https://doi.org/10.13140/RG.2.2.23038.97608.

professionnelles et mettre en œuvre des mesures pour contrôler l'accès aux informations sensibles. Selon un article publié par Bitdefender, l'adoption de politiques de sécurité strictes et la sensibilisation des employés à ces politiques peuvent réduire considérablement le risque de failles de sécurité[1055].

Le rôle de l'éducation dans la sensibilisation à la cybersécurité est essentiel pour instaurer une solide culture de la sécurité, tant au niveau individuel qu'organisationnel[1056]. L'éducation dans domaine va au-delà de la transmission d'informations techniques, mais vise à développer des comportements et des attitudes proactifs cyberrisques. L'intégration de la cybersécurité dans les programmes d'enseignement est une étape cruciale.[1057] Les établissements d'enseignement ont la responsabilité de préparer les élèves et les étudiants aux défis numériques du 21e siècle. En incluant des modules sur la cybersécurité dans les programmes scolaires et universitaires, les jeunes peuvent se familiariser avec les menaces en ligne, l'importance de la protection des données personnelles et les moyens efficaces de prévenir les cyberattaques. En Roumanie, par exemple, l'Association roumaine pour l'assurance de la sécurité de l'information (ARASEC) a publié le livre « Cybersécurité : Défis et perspectives en éducation », qui souligne la nécessité d'intégrer ces concepts dans le système éducatif.[1058]

330. Le projet « Mois européen de la cybersécurité ». La formation continue des employés est tout aussi importante. Les organisations doivent investir dans des programmes de formation et des ateliers pour actualiser les connaissances du personnel sur les nouvelles menaces et les techniques de défense. Selon un article publié par Prodefence, l'éducation à la cybersécurité contribue à créer une culture organisationnelle qui donne la priorité à la protection des données et de l'infrastructure informatique[1059]. Les campagnes de sensibilisation du public jouent également un rôle important. Des événements tels que le Mois Européen de la Cybersécurité, célébré chaque année en octobre, visent à informer et à éduquer le grand public sur l'importance de la sécurité en ligne.[1060] L'éducation à la cybersécurité ne doit pas être un processus ponctuel, mais continu, qui s'adapte en permanence aux évolutions technologiques et aux nouveaux types

---

[1055] V. Constantinescu, *Étude de cas : une attaque du type ransomware frappe une petite clinique*, Hot for Security, 2024. consulté le 27 novembre 2024, https://www.bitdefender.com/ro-ro/blog/hotforsecurity/studiu-de- case-attack-ransomware-clinica-mica.

[1056] *La culture de la sécurité. La prévention par l'éducation*, Intelligence Magazine (blog), 2017. https://intelligence.sri.ro/cultura-de-securitate-prevenire-prin-educatie/.

[1057] *La cybersécurité dans les écoles. 5 modèles européens de bonnes pratiques*, NOD Academy, 2024. https://nodacademy.ro/blog/noutati/securitate-cibernetica-in-scoli-5-modele-de-bune-practici-europene/.

[1058] ARASEC, *Securitatea cibernetică: Provocări și perspective în educație*, (Cybersécurité: Défis et perspectives en éducation), ARASEC / CERT-RO / Ministerul Educației și Cercetării, 2020. https://www.arasec.ro/comunicate-de-presa/cartea- cyber-security-challenges-and-perspectives-in-education/.

[1059] A. Anghelus, « *Le rôle essentiel de l'éducation dans la cybersécurité* », Cyber Security Services, 2024. https://www.prodefence.ro/rolul-esential-al-educatiei-in-securitatea-cibernetica/.

[1060] *Le Mois Européen de la Cybersécurité et la Protection des Enfants à l'ère numérique*, Code School Clubs , 2024. https://codeschoolclubs.ro/luna-europeana-a-securitatii-cibernetice-si-protejarea-copiilor-in-era-digitala/.

de menaces.[1061] En promouvant une bonne éducation dans ce domaine, la société peut développer une plus grande résilience face aux cyberattaques et à l'utilisation des technologies de l'information et de la communication. En promouvant une bonne éducation dans le domaine, la société peut développer une plus grande résilience face aux cyberattaques et peut assurer la protection des informations personnelles et des infrastructures critiques.

C. Techniques de tromperie en ligne

331. Des techniques de fraude en ligne toujours plus sophistiquées, une détection toujours plus difficile. Compte tenu du développement de l'environnement numérique au cours des dernières décennies, l'internet est devenu un support favorable au développement d'activités commerciales, sociales et d'information. À mesure que les gens sont devenus plus dépendants de l'environnement en ligne, diverses méthodes de tromperie sont apparues, conçues pour exploiter l'insouciance et le manque d'information des utilisateurs. Les techniques utilisées par les cybercriminels sont devenues de plus en plus complexes et de plus en plus difficiles à détecter et à prévenir. Elles visent à voler des données personnelles ou financières ou à obtenir un accès non autorisé à des ressources numériques. Dans ce sous-chapitre, nous analyserons certaines des méthodes les plus courantes de fraude en ligne, notamment l'escroquerie, l'usurpation d'identité et la fraude publicitaire, afin d'acquérir une meilleure compréhension de ces méthodes et des moyens de les prévenir.

a). Délits d'hameçonnage

332. Phishing: définition, mécanismes, moyens de prévention. Le *phishing* est une technique d'ingénierie sociale par laquelle un attaquant tente d'obtenir des données personnelles telles que des mots de passe, des détails de comptes bancaires, des détails de cartes de crédit ou de débit ou toute autre information personnelle.[1062] Il s'agit de l'un des types de cybercriminalité les plus courants, et il est réalisé par le biais de courriels, de messages textuels, d'appels téléphoniques ou de toute autre forme de communication. Les attaques par hameçonnage sont basées sur l'exploitation de la confiance et de l'insouciance des victimes, en exploitant leur

[1061] M. Bada, J. R.C. Nurse, *Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises,* Information and Computer Security, vol.27(3), 2019. p.393–410. https://doi.org/10.1108/ICS-07-2018-0080

[1062] KnowBe4, *Phishing, What Is Phishing?*, consulté le 27 novembre 2024, https://www.phishing.org/what- is-phishing.

besoin de résoudre certains problèmes ou de profiter d'offres supposées irréfutables. Les attaquants se font passer pour des personnes morales ou privées légitimes afin de créer un niveau de confiance entre la victime et l'attaquant, et la nature urgente du prétexte offert signifie que la victime n'a pas le temps nécessaire pour réfléchir et se rendre compte si la demande est réelle ou non.[1063]

Pour mener à bien une attaque par hameçonnage, la première étape consiste à créer un faux site web imitant une institution financière ou commerciale et exigeant l'utilisation de cartes de crédit ou de débit. L'étape suivante consiste à obtenir les données personnelles des victimes, la tentative d'hameçonnage peut être envoyée. Par données personnelles, nous entendons les adresses électroniques ou les numéros de téléphone. Ces données sont obtenues par des fuites de données, dues à la négligence des utilisateurs ou à l'absence de sécurité adéquate de la part des entreprises nationales et multinationales. L'étape finale d'une attaque par hameçonnage consiste à envoyer des messages, qui semblent réels, aux victimes, en leur demandant de mettre à jour leur méthode de paiement (par exemple, le numéro de la carte, le code PIN ou la date d'expiration). Ces informations sont ensuite utilisées pour accéder aux cartes de crédit/débit et voler l'argent sur le compte de la victime.[1064]

333. Évolution des fraudes informatiques. L'évolution des attaques de cyber-hameçonnage montre comment ce domaine s'est adapté aux développements technologiques et aux changements de comportement des utilisateurs Internet. Les premiers cas d'hameçonnage sont apparus dans les années 1990, avec la popularité croissante du service en ligne AOL (America Online). À l'époque, les attaquants utilisaient des techniques de génération aléatoire et automatique de numéros de cartes de crédit pour créer de faux comptes et obtenir un accès gratuit aux services internet. En 1995, AOL a modifié sa politique de sécurité et mis en place des mesures plus strictes, obligeant les cybercriminels à adopter de nouvelles mesures pour obtenir l'accès à l'Internet. C'est ainsi que sont apparus les premiers cas de faux messages électroniques, prétendant être des employés d'AOL, demandant aux utilisateurs de confirmer les informations de leur compte, ce qui leur permettait d'accéder à leurs informations et, par la suite, à l'Internet.[1065]

334. Exemples notoires de phishing : Love-Bug, Cryptolocker. L'année 2000 a marqué un tournant dans les attaques par hameçonnage, le premier cas célèbre étant celui du « Love Bug ». Il a démontré l'efficacité d'une attaque exploitant la curiosité humaine. Les messages

[1063] *What Is Phishing - Definition, Types of Attacks & More,* Proofpoint US, 2021. https://www.proofpoint.com/us/threat-reference/phishing.
[1064] *Ibidem*.
[1065] P.Gillin, *The History of Phishing Attacks*, Verizon Business, consulté le 27 novembre 2024. https://www.verizon.com/business/resources/articles/s/the-history-of-phishing/.

contenaient un fichier infecté appelé « LOVELETTER », et lorsque ce fichier était ouvert, tant les systèmes des utilisateurs que les réseaux sociaux de leur cercle social étaient infectés[1066]. Après 2001, les attaques ont commencé à cibler les systèmes de paiement et d'achat en ligne, principalement PayPal et eBay, en envoyant de faux courriels encourageant les utilisateurs à cliquer sur des liens pour être redirigés vers de faux sites. Entre 2004 et 2005, par exemple, environ un million de personnes ont été victimes de ces attaques, causant des dommages pour un montant total d'environ un milliard de dollars[1067].

L'avènement des crypto-monnaies en 2008 a permis aux attaquants d'atteindre un nouveau niveau d'anonymat et de sécurité, facilitant le vol de données personnelles et d'argent par le biais de transactions difficiles à retracer[1068]. En outre, en 2013, le *ransomware* Cryptolocker est devenu la première attaque de logiciel malveillant à utiliser des techniques d'hameçonnage pour diffuser le logiciel malveillant. Pour l'essentiel, l'attaque a été menée à l'aide de deux adresses électroniques, l'une ciblant les entreprises et la seconde, un lien malveillant ciblant le reste des utilisateurs[1069]. Aujourd'hui, l'hameçonnage est resté la principale technique par laquelle les cybercriminels compromettent les données et la cyberinfrastructure. L'émergence de techniques spéciales ciblant certaines catégories de personnes, comme le spear-phishing, pose des problèmes considérables aux utilisateurs, et cette évolution constante montre comment les attaquants s'adaptent aux nouvelles technologies et aux changements de comportement des utilisateurs[1070].

335. Nouvelles méthodes de phishing : spear phishing. Outre l'hameçonnage classique, différents types d'attaques sont apparus au fil du temps, dans lesquels les attaquants ciblent quelque chose de spécifique, par exemple des organisations spécifiques ou des utilisateurs spécifiques de ces organisations. En ce sens, le *spear phishing* est une technique avancée, dont l'objectif principal est de cibler une personne au sein d'une organisation, où les attaquants utilisent des messages personnalisés pour rendre le message aussi réel que possible et persuader la victime divulguer des informations sensibles ou de prendre des mesures qui pourraient être préjudiciables à l'entreprise. La principale différence entre le *phishing* classique et le *spear phishing* réside dans le message envoyé, qui contient des informations détaillées sur la cible[1071].

[1066] *The History of Phishing Attacks*, Cofense, consulté le 27 novembre 2024. https://cofense.com/knowledge-centre/history-of-phishing/.

[1067] KnowBe4, *Historique d'hameçonnage,* Phishing, consulté le 27 novembre 2024. https://www.phishing.org/history-of-phishing.

[1068] K. Sultan, U. Ruhi, R. Lakhani, *Conceptualizing Blockchains: Characteristics & Applications*, Researchgate, 2018. consulté le 27 novembre 2024. https://www.researchgate.net/figure/Nakamotos-Blockchain-Proposal-Nakamoto-2008_fig2_325464908

[1069] *CryptoLocker Ransomware Infections*, CISA, 2016. https://www.cisa.gov/news-events/alerts/2013/11/05/cryptolocker-ransomware-infections.

[1070] KnowBe4, *History of Phishing*, https://www.knowbe4.com/resource-center/phishing#history.

[1071] *What Is Spear Phishing?*, IBM, 2024. https://www.ibm.com/topics/spear-phishing.

b). Le scamming

336. L'arnaque en ligne scamming : définition, méthodes. Le *scamming* est une activité illégale dans laquelle un individu ou un groupe d'individus tente d'obtenir des avantages financiers ou des informations personnelles d'une victime en utilisant des tactiques coercitives et trompeuses. En fin de compte, l'escroquerie exploite la confiance et les vulnérabilités humaines des individus pour les inciter à prendre des décisions qui peuvent avoir un impact financier ou émotionnel négatif sur eux.[1072] L'escroquerie peut fonctionner de différentes manières, en s'adaptant aux nouvelles technologies et aux tendances sociétales. Des courriels d'hameçonnage les plus avancés aux appels téléphoniques coercitifs et aux messages textuels trompeurs, les cybercriminels utilisent un large éventail de méthodes pour atteindre leurs objectifs[1073].

Il existe des méthodes plus complexes de *scamming*, et l'une d'entre elles est l'escroquerie à la romance. Les criminels ou les escrocs créent de faux profils sur les réseaux sociaux ou les sites de rencontre, nouent des relations fictives avec leurs victimes, gagnent leur confiance et, au fil du temps, en tirent profit en demandant des faveurs, de l'argent ou des cadeaux.[1074] Les cybercriminels, généralement basés dans d'autres pays pour éviter les rencontres en face à face, utilisent la confiance qu'ils ont gagnée en manipulant leurs victimes et recourent à différentes méthodes pour leur soutirer des ressources financières. Ces méthodes vont des problèmes de santé aux difficultés financières[1075].

337. Exploitation de l'instinct humain pour maximiser les gains financiers. Les escroqueries en ligne portant sur des prix, de l'argent ou des primes sont une autre forme courante d'escroquerie. On dit souvent aux victimes qu'elles ont gagné une loterie ou un prix et on leur demande de payer des frais ou de fournir des informations personnelles pour réclamer le prix[1076]. Ce type d'escroquerie repose sur l'instinct humain de cupidité et de maximisation du gain financier en offrant un faux espoir d'enrichissement immédiat. Les messages gagnants sont souvent accompagnés de logos et d'images professionnels pour en renforcer l'aspect. Un autre

---

[1072] *How To Avoid a Scam*, Federal Trade Commission, Consumer Advice, consulté le 27 novembre 2024. https://consumer.ftc.gov/articles/how-avoid-scam.
[1073] *Action Fraud : Stay Safe Online after £1.4 Million Lost from Email and Social Media Account Hacking in Last Year*, Action Fraud, 2024. https://www.actionfraud.police.uk/news/socialmediahacking.
[1074] *Romance Scams*, Federal Bureau of Investigation. consulté le 27 novembre 2024, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/romance-scams.
[1075] Ibidem
[1076] A. Iyer, *Lottery and Sweepstakes Scams: Recognize and outsmart scammers*, Fraude Awareness, 2024. consulté le 27 novembre 2024, https://www.westernunion.com/blog/en/top-five-warning-signs-of-lottery-sweepstakes-scams/.

exemple d'escroquerie est celui des faux investissements financiers, qui consistent à espérer des retours importants sur l'investissement initial. Généralement, les criminels qui utilisent de faux investissements sont des personnes qui donnent une image de confiance, offrant des garanties de retour sur le montant initial investi avec un profit substantiel. Le plus souvent, les offres sont présentées comme attrayantes et fermées, de sorte que les victimes entreprennent certaines actions sans pouvoir sortir de l'escroquerie[1077].

338. Le *scamming* au support technique consiste à impliquer les victimes dans de faux appels téléphoniques ou des messages pop-up les avertissant que le système d'exploitation de l'ordinateur est infecté, qu'une activité dangereuse a été détectée ou que des informations bancaires ont été perdues.[1078] Les auteurs se font passer pour des employés d'une entreprise, proposant de résoudre des problèmes techniques. Dans la plupart des cas, les problèmes techniques spécifiés sont inexistants, la raison principale étant d'obtenir les informations bancaires de la victime et éventuellement d'introduire des logiciels malveillants. Dans la plupart des cas, les victimes n'ont pas la formation informatique nécessaire et sont manipulées pour leur remettre l'ordinateur par l'intermédiaire de systèmes à distance[1079].

339. Prévention de la fraude numérique : signaux d'alerte et bonnes pratiques. La détection des escroqueries peut s'avérer compliquée, car les criminels développent des méthodes très élaborées de manipulation et de tromperie. Toutefois, certains signes avant-coureurs de la tromperie peuvent être efficaces[1080] Offres trop belles pour être vraies : si une offre semble trop belle pour être vraie, il s'agit probablement d'une arnaque.

Demandes d'informations personnelles : aucune organisation digne de confiance ne demandera jamais l'envoi d'informations personnelles sensibles par courrier électronique ou par téléphone.

La notion d'urgence : les criminels créent souvent un sentiment d'urgence pour forcer les victimes de leurs escroqueries à agir sans réfléchir.

Il y a des fautes de grammaire et d'orthographe : de nombreux courriels et messages frauduleux contiennent des fautes de grammaire et d'orthographe.

[1077] Ibidem.

[1078] *Learning How a Scam Works*, Digital Skills and Jobs Platform, consulté le 27 novembre 2024. https://digital-skills-jobs.europa.eu/en/community/online-discussions/learning-how-scam-works.

[1079] *Protect yourself from tech support scams*, Microsoft Support. consulté le 27 novembre 2024. https://support.microsoft.com/en-us/windows/protect-yourself-from-tech-support-scams-2ebf91bd-f94c-2a8a- e541-f5c800d18435.

[1080] *Avoiding Scams and Scammers*, FDIC, consulté le 27 novembre 2024. https://www.fdic.gov/consumer-resource-center/2021-10/avoiding-scams-and-scammers.

Adresses suspectes : les faux sites web utilisés pour les escroqueries ont souvent des adresses web qui ressemblent à celles des organisations légitimes, mais qui contiennent de petites différences.

340. Prévention, vigilance, éducation : la tirade anti-fraude. Éviter le *scamming* n'est possible que par une attitude préventive, un processus qui comprend la vigilance, l'éducation et l'adoption de mesures de sécurité.[1081] Tant les opérateurs commerciaux que les utilisateurs doivent comprendre les risques auxquels ils sont exposés dans l'environnement en ligne et se montrer critiques à l'égard de toute demande de renseignements ou de toute offre suspecte. Il est important d'enquêter sérieusement sur l'identité de toute personne ou acteur demandant des informations personnelles telles que des données financières et d'éviter de cliquer sur un lien ou d'ouvrir pièces jointes à un message suspect. Il est également essentiel de sécuriser et d'utiliser des solutions appropriées, par exemple l'utilisation de systèmes anti-virus, ainsi que la mise à jour constante des systèmes d'opération et des applications critiques de l'ordinateur[1082].

En conclusion, le *scamming* est une menace réelle et évolutive dans l'environnement en ligne. Pour la combattre efficacement et avec succès, il faut adopter une approche holistique et à large spectre impliquant l'éducation, la surveillance et l'utilisation de mesures de sécurité appropriées dans l'environnement. En prenant conscience des dangers et en adoptant des mesures préventives appropriées, les utilisateurs peuvent se protéger contre ces escroqueries ou assurer leur sécurité sur l'internet.

c). Le spoofing

341. L'arnaque en ligne par spoofing : définition, méthodes. Le *spoofing* est un type de cyberattaque dans lequel un cybercriminel se fait passer pour une source légitime afin de tromper une victime ou un système. Par cette forme de tromperie, les criminels usurpent des adresses IP, des adresses électroniques ou tout autre identifiant pouvant attester d'une source légitime afin d'obtenir un accès non autorisé à des informations personnelles ou de mener d'autres activités malveillantes, par exemple en facilitant le processus de développement d'une attaque par logiciel malveillant. Le *spoofing* est souvent utilisé dans les attaques de *phishing* et

[1081] *6 Scan-Savvy Tips For Avoiding Online Traps*, Global Reach. consulté le 27 novembre 2024, https://www.globalreach.com/global-reach-media/newsletters/grip-newsletter/6-ways-to-avoid-internet-scams/6-scam-savvy-tips.

[1082] K. Peterson, *5 Tips to Prevent Online Fraud*, Facebook. https://www.bannerbank.com/financial-resources/blog/tips-to-prevent-online-fraud.

constitue également l'une des méthodes les plus essentielles pour tromper les utilisateurs et collecter leurs données sans leur consentement[1083].

Les tentatives de *spoofing* peuvent se faire de différentes manières, chacune d'entre elles ayant des caractéristiques spécifiques qui permettent de les reconnaître plus facilement. Les types de *spoofing* les plus courants sont l'usurpation d'adresse électronique (*Email spoofing*), l'usurpation d'adresse IP (*IP spoofing*) et l'usurpation d'adresse DNS (*DNS spoofing*).[1084] L'usurpation d'adresse électronique est l'une des formes les plus répandues de cyber-attaques, utilisée par les cybercriminels pour confondre et tromper les destinataires de courriels en usurpant l'adresse de l'expéditeur. En utilisant cette technique, les attaquants donnent l'impression que les courriels envoyés par des sources fiables telles que des banques, des entreprises ou des personnes connues, et dans la plupart des cas, ces attaques sont accompagnées de techniques d'ingénierie sociale[1085]. Ce type d'attaque est possible et très facile car le protocole standard de messagerie Simple Mail Transfer Protocol (SMTP) ne contient pas de mesures de sécurité permettant d'identifier l'expéditeur. Les attaquants exploitent ce problème technique en envoyant des messages dans lesquels les adresses électroniques sont falsifiées[1086]. Dans la plupart des cas, les criminels ont également recours à la modification de l'en-tête du courrier électronique pour dissimuler l'adresse source réelle du message, ce qui lui donne une apparence plus légitime et rend les personnes qui manquent de connaissances techniques plus susceptibles d'en être victimes.

342. Technologies visant à minimiser la cybercriminalité. Pour minimiser le taux de réussite de ces attaques, des technologies telles que Sender Policy Framework (SPF) et DomainKeys Identified Mail (DKIM) ont été développées et ont le rôle d'authentifier la véracité de la source du message entrant. La technologie SPF permet aux domaines de déclarer quelles adresses IP sont autorisées à envoyer des courriers électroniques au nom de l'entreprise[1087], et par DKIM on utilise une signature numérique pour vérifier si le message a été modifié ou pas en transit.[1088] Avec la mise en œuvre des technologies SPF et DKIM, tout administrateur de compte a la possibilité de mettre en œuvre la technologie DMARC (Domain-based Message Authentication, Reporting and Conformance), qui permet à un utilisateur de

---

[1083] *What Is Spoofing & How to Prevent It*, Kaspersky, 2020. https://www.kaspersky.com/resource-centre/definitions/spoofing.
[1084] *What Is Spoofing? Definition, Types & More*, Proofpoint US, 2023. https://www.proofpoint.com/us/threat-reference/spoofing.
[1085] *What Is Email Spoofing*?, Cloudflare, consulté le 27 novembre 2024. https://www.cloudflare.com/learning/email-security/what-is-email-spoofing/.
[1086] Ibidem.
[1087] S. Gupta et al, *Forensic analysis of E-mail address spoofing*, 5th International Conference - Confluence The Next Generation Information Technology Summit (Confluence), 2014. p.898-904, https://doi.org/10.1109/CONFLUENCE.2014.6949302.
[1088] Ibidem

recevoir des courriels qui n'ont pas passé les contrôles SPF et DKIM. En outre, grâce à la technologie DMARC, tout administrateur de compte peut identifier les problèmes d'authentification ou les tentatives malveillantes qui ont été envoyées par l'intermédiaire de ce domaine[1089]. Bien que ces technologies se soient développées au fil du temps et aient contribué à réduire le nombre croissant d'attaques par usurpation d'adresse électronique, elles ne sont pas universellement déployées, ce qui permet à ces attaques d'être efficaces dans des situations différentes.

343. Cyberattaques contre l'adresse IP. L'usurpation d'adresse IP est une technique par laquelle les attaquants usurpent l'adresse IP d'un paquet de données pour le faire apparaître comme légitime. L'usurpation d'adresse IP est le plus souvent utilisée dans les attaques Denial of Service (DoS) et Distributed Denial of Service (DDoS), mais elle peut également être utilisée pour intercepter des communications ou contourner des politiques de sécurité basées sur une adresse IP[1090]. Lorsqu'un fichier de données est transmis sur un réseau, il contient, en plus des informations paquet, l'adresse IP de l'expéditeur et celle du destinataire. Au cours de l'attaque par usurpation d'adresse IP, l'attaquant obtient et modifie l'adresse IP de l'expéditeur, usurpant ainsi une autre adresse légitime[1091]. Cette méthode est possible en raison des limites rencontrées dans la vérification de l'authenticité de la source des paquets de données entrants, car la plupart des protocoles de réseau, par exemple IPv4, n'ont pas de mécanismes intégrés capables d'intercepter et de vérifier l'intégrité et l'authenticité de l'adresse IP[1092].

Comme nous l'avons mentionné, l'usurpation d'adresse IP est le plus souvent utilisée dans les attaques DoS et DDoS. Dans les deux, les attaquants envoient un volume massif de données usurpées à un réseau ou à un serveur afin de remplir leur capacité et de rendre difficile le traitement du trafic, ce qui entraîne un blocage précoce des services[1093]. Dans les attaques DDoS, les paquets usurpés proviennent de multiples sources compromises, également connues sous le nom de botnets, où les adresses IP des paquets sont usurpées afin de cacher l'identité originale de l'attaquant et de rendre son identification plus difficile. En fait, dans les attaques

---

[1089] *Set up DMARC*, Google Workspace Admin Help, consulté le 27 novembre 2024. https://support.google.com/a/answer/2466580?hl=en.

[1090] K. Bhushan, B. B. Gupta, "*Distributed Denial of Service (DDoS) Attack Mitigation in Software Defined Network, (SDN)-Based Cloud Computing Environment*, Journal of Ambient Intelligence and Humanized Computing vol.10, no.5, 2019. p.1985-97 https://doi.org/10.1007/s12652-018-0800-9.

[1091] I. Yaser Aljanabi et al, "*Detect and Mitigate Blockchain-Based DDoS Attacks Using Machine Learning and Smart Contracts*," Informatica, vol.46, no.7, 2022. https://doi.org/10.31449/inf.v46i7.4033.

[1092] K. Bhushan, B. B. Gupta, "*Distributed Denial of Service (DDoS) Attack Mitigation in Software Defined Network (SDN)-Based Cloud Computing Environment*," Journal of Ambient Intelligence and Humanized Computing vol.10, no.5, 2019. p.1985-97 https://doi.org/10.1007/s12652-018-0800-9. https://doi.org/10.1007/s12652-018-0800-9.

[1093] I. B. Mopari, S. G. Pukale, M. L. Dhore, "*Detection and defence against DDoS attack with IP spoofing*", Communication and Networking, 2008. p.1–5 https://doi.org/10.1109/ICCCNET.2008.4787693.

par amplification de données, les attaquants utilisent des techniques d'usurpation d'identité pour envoyer de petits paquets de données à des serveurs, qui répondent ensuite par des paquets de données plus importants. En usurpant l'adresse IP de l'expéditeur, les réponses sont envoyées à la cible visée, ce qui a pour effet d'amplifier le volume du trafic sur le réseau et de créer une surcharge qui rend l'utilisation du réseau impossible[1094].

344. Cyberattaques contre l'adresse DNS. Le dernier type, souvent utilisé, est le DNS Spoofing, également connu sous le nom de DNS cache poisoning. Il s'agit d'une technique de cyberattaque dans laquelle les attaquants manipulent le système de noms de domaine (DNS) pour rediriger les utilisateurs vers des sites web infectés, que les utilisateurs aient ou non saisi l'adresse web correcte. Le DNS est conçu transformer les noms de domaine en adresses IP, que tout appareil électronique connecté à l'internet utilise pour se localiser et communiquer entre eux[1095]. En compromettant le DNS, les attaquants ont la possibilité d'intercepter ou de rediriger le trafic web, ce qui porte atteinte à la confidentialité et à la sécurité des données des utilisateurs.

Principalement, pour prévenir les attaques de DNS Spoofing, il existe un certain nombre de mesures techniques que les administrateurs de réseaux et les utilisateurs peuvent mettre en œuvre. D'abord, il est nécessaire d'utiliser un ensemble d'extensions destinées à ajouter une signature numérique aux réponses DNS, appelée Domain Name System Security Extensions (DNSSE). Ainsi, on permet aux serveurs de vérifier l'authenticité de toutes les données transmises, ce qui rend plus difficile la falsification des réponses DNS et empêche les attaques[1096]. Il est également recommandé d'utiliser des serveurs DNS sécurisés, proposés par des fournisseurs connus et fiables, tels que Cloudfare, Google Public DNS et OpenDNS. En outre, les opérateurs de services internet ont la possibilité de prendre des mesures proactives pour surveiller et sécuriser les serveurs DNS contre toute tentative d'altération[1097]. Enfin, l'utilisation du cryptage est également recommandée pour protéger les communications entre le client et les serveurs DNS. Les protocoles de cryptage DNS over HTTPS (DoH) et DNS over TLS (DoT) permettent de protéger les requêtes de l'interception et la modification du système DNS, garantissant que les données envoyées ne soient pas compromises.[1098]

345. Facilitation des cyberattaques par usurpation d'identité. Ainsi, l'usurpation d'identité (le *spoofing*) reste l'une des formes les plus complexes et les plus fréquemment

---

[1094] Azure Network Security Team, "*Anatomy of a DDoS Amplification Attack*", Microsoft Security Blog, 2022. https://www.microsoft.com/en-us/security/blog/2022/05/23/anatomy-of-ddos-amplification-attacks/.

[1095] *What is DNS Spoofing*, *Cache Poisoning Attack Example*, Imperva. consulté le 27 novembre 2024. https://www.imperva.com/learn/application-security/dns-spoofing/.

[1096] T.R. Kukutla*, A Deep Dive into DNS Spoofing and Security Measures*, Research Gate, 2023. consulté le 27 novembre 2024. https://www.researchgate.net/publication/376271471_A_Deep_Dive_into_DNS_Spoofing_and_Security_Measure.

[1097] *Ibidem*.

[1098] *Ibidem*.

utilisées de tromperie en ligne, exploitant les vulnérabilités inhérentes aux protocoles de communication numérique. Par essence, les techniques d'usurpation d'identité sont les plus couramment utilisées et ont un impact significatif sur la sécurité, la vie privée et l'intégrité des données personnelles des utilisateurs. Les attaquants utilisent l'usurpation d'identité pour faciliter des cyber-attaques plus importantes, comme nous l'avons souligné plus haut, avec des conséquences potentiellement significatives pour l'infrastructure numérique. Bien que des solutions de sécurité aient été développées au fil du temps pour prévenir ces attaques, leur application est laissée aux utilisateurs et aux opérateurs de services, car les attaquants continuent de trouver des moyens d'exploiter les vulnérabilités des systèmes d'information.

d). Ad stacking (la fraude au clic)

346. Manipulation des systèmes publicitaires en ligne : fraude complexe, modalités multiples. La fraude publicitaire est l'un des plus grands défis de la publicité numérique, ayant un impact majeur sur l'industrie numérique et les utilisateurs. Cette pratique implique des actions trompeuses de la part d'acteurs manipulant les systèmes de publicité en ligne, dans le but premier de réaliser des gains financiers ou d'avoir un impact négatif sur les campagnes publicitaires.[1099] La publicité étant devenue la principale méthode de promotion des produits et services, les pratiques de publicité mensongère sapent la confiance des gens et l'efficacité du marché.[1100] Ce type de fraude est complexe et peut comporter de nombreuses variantes, des clics générés par des robots à l'insertion de publicités sur des sites web sans le consentement direct des propriétaires de ces sites. À l'instar de la fraude informatique décrite ci-dessus, la fraude publicitaire peut être divisée en plusieurs types :

347. Trafic frauduleux imitant le comportement humain. Le trafic non valide (IVT) est toute activité qui déclenche un affichage, un clic, une conversion ou toute autre action en ligne qui peut être interprétée comme ayant été créée par un véritable utilisateur d'Internet. Le trafic non valide peut provenir d'un large éventail de sources, y compris, mais sans s'y limiter, les robots, les logiciels automatisés, les fermes à clics et même les dispositifs détournés. Il existe deux principaux types d'IVT[1101] :

[1099] *What Is Ad Fraud?, Ad Click Fraud*, Cloudflare, consulté le 27 novembre 2024, https://www.cloudflare.com/learning/bots/what-is-ad-fraud/.

[1100] *What Is the Importance of Advertising ? (Plus Definition and Tips)*, Indeed Career Guide. consulté le 27 novembre 2024. https://www.indeed.com/career-advice/career-development/importance-of-advertising.

[1101] O. Lynch, *What Is Invalid Traffic (IVT)?,* CHEQ blog, 2022. https://cheq.ai/blog/what-is-invalid-traffic-ivt-2/.

Trafic sophistiqué non valide (SIVT) : cette catégorie concerne le trafic généré par des robots sophistiqués qui imitent les activités humaines, ce qui les rend difficiles à détecter. Certains exemples de SIVT[1102] :

Les bots de navigation qui peuvent s'apparenter à la navigation humaine : ces navigateurs peuvent même naviguer sur des sites web, remplir des formulaires, regarder des vidéos et même ajouter des articles à leur panier.

Les bots de pollupostage : Il s'agit des types de robots qui cliquent automatiquement sur une page web qui finirait par faire payer l'annonceur sans qu'il ait vraiment l'intention de visiter le site.

Les bots d'usurpation d'adresse : ces robots peuvent masquer votre adresse et peuvent afficher une annonce publique erronée.

Les bots de conversion : ces robots envoient des formulaires de contact, s'inscrivent à des lettres d'information et effectuent même une sorte d'achat pour fournir des données trompeuses sur les performances de la campagne.

348. Trafic identifié par des moyens de filtrage de routine. La trafic générale invalide (GIVT) couvre tout le trafic provenant de sources non humaines et est relativement facile à identifier. Exemples de GIVT[1103] :

Web Crawler : il s'agit de programmes utilisés par les moteurs de recherche pour indexer le contenu des sites web.

Bots simples : ils génèrent du trafic grâce à un accès continu aux pages ou à des requêtes automatisées.

Erreurs de configuration du serveur : elles peuvent créer un faux trafic dans la manière où les requêtes automatisées sont envoyées aux serveurs web.

349. Méthodes de création et de distribution du trafic invalide. Plusieurs facteurs contribuent à la création et à la dispersion des IVT[1104] :

Gains financiers : la fraude publicitaire est une activité lucrative pour ceux qui la pratiquent, les revenus les plus importants étant générés par les fausses recettes publicitaires ou par l'escroquerie aux agents de publicité.

Manque de transparence : le manque de transparence autour de l'écosystème de la publicité en ligne rend difficile la détection et la prévention du IVT.

[1102] J. Edwards, *What Is Sophisticated Invalid Traffic (SIVT), and How to Block It*, CHEQ blog, 2022. https://cheq.ai/blog/what-is-sophisticated-invalid-traffic-sivt-how-to-detect-and-block-sivt/.

[1103] *General Invalid Traffic (GIVT),* Bidscube, consulté le 27 novembre 2024. https://bidscube.com/blog/glossary/general-invalid-traffic-givt/.

[1104] *Digital Advertising Spend Lost to Fraud to Reach $68 Billion Globally in 2022*, Juniper Research, 2022. consulté le 27 novembre 2024, https://www.juniperresearch.com/press/digital-advertising-spend-lost-to-fraud-68-billion/.

Technologies sophistiquées : le développement de technologies sophistiquées, telles que l'intelligence artificielle, rend les robots de plus en plus difficiles à détecter.

Absence de réglementation. L'absence de réglementation claire et de normes universelles dans le secteur de la publicité en ligne facilite l'émergence du IVT.

350. Systèmes opérationnels pour l'identification de l'IVT. La détection du IVT est une tâche complexe qui nécessite une combinaison de méthodes et de technologies. Les méthodes de détection les plus courantes sont les suivantes[1105] :

Analyse du trafic : il s'agit d'analyser les données relatives au trafic en recherchant des schémas suspects, par exemple des taux de clics anormalement élevés, un trafic provenant de sources non identifiées ou une activité concentrée à certains moments. Analyse comportementale : il s'agit d'analyser le comportement de l'utilisateur pour détecter les actions non humaines, par exemple le fait de sauter rapidement d'une page à l'autre, de ne pas interagir du tout avec le contenu ou de soumettre des formulaires en utilisant de fausses données.

Détection basée sur les signatures : détecte les robots connus grâce à leurs signatures, leurs adresses IP, y compris les adresses IP, les agents utilisateurs et les habitudes de navigation. Apprentissage automatique : ces algorithmes d'apprentissage automatique pourraient être entraînés à identifier des modèles de trafic non valides et à détecter des robots sophistiqués.

351. La lutte contre l'IVT. La prévention du IVT nécessite une approche holistique qui englobe toutes les entités : agents de publicité, éditeurs, réseaux publicitaires et fournisseurs de technologie. Les mesures de prévention les plus importantes sont les suivantes :

L'utilisation des solutions de détection du IVT : il existe sur le marché un grand nombre de solutions de détection du IVT qui permettent de détecter et de bloquer le trafic non valide. Il est également impératif de collaborer avec les éditeurs, les réseaux publicitaires et les fournisseurs de technologie, chacun adoptant une approche sévère de la prévention du IVT. En surveillant continuellement le trafic, il est possible de s'assurer que toute activité suspecte est stoppée, empêchant toute tentative de IVT. Il est possible d'empêcher cela en mettant en œuvre plusieurs mesures de sécurité, telles que l'authentification à deux facteurs et en veillant à appliquer un mot de passe fort sur les comptes, ce qui peut empêcher l'accès non autorisé aux comptes pour compromettre davantage les appareils[1106].

Le trafic non valide est l'un des problèmes les plus complexes qui nécessite une attention constante et un traitement proactif. En comprenant les causes, les types et les méthodes de

[1105] *Invalid Traffic (IVT) - Everything You Need to Know*, header bidding, consulté le 27 novembre 2024. https://headerbidding.co/invalid-traffic-ivt/.
[1106] Ibidem

détection du trafic non valide, les annonceurs et les éditeurs peuvent prendre des mesures efficaces pour éviter son impact négatif sur les campagnes de marketing numérique.

352. Clics invalides : impossibles à éliminer, mais limités par des politiques de trafic. Malgré de nombreuses tentatives pour l'éliminer, le problème de la fraude au clic - ou l'action de toucher une connexion payée avec l'attente de provoquer des préjudices - est toujours d'actualité et doit être résolue promptement par les joueurs de l'industrie de la publicité en ligne.[1107] En termes simples, la fraude au clic est le type de fraude qui se produit en raison de faux clics sur des publicités en ligne ou tout autre processus similaire, entraînant une perte d'argent ou des résultats douteux des campagnes de marketing. En particulier, elle peut impliquer de vraies personnes qui sont déployées pour cliquer sur des publicités par l'intermédiaire de fermes à clics. Il peut aussi s'agir d'un travail de robotique, d'unités programmées pour émuler la capacité humaine à effectuer des tâches cybernétiques répétitives. Une grande connaissance des facteurs humains et des intentions est nécessaire pour mener à bien une telle attaque[1108].

353. Clic frauduleux : incitations économiques, sabotage concurrentiel. Très souvent, l'objectif de ce délit est de faire surpayer les annonceurs en épuisant leur budget publicitaire et d'augmenter la rentabilité des campagnes de marketing. Dans d'autres cas, la fraude au clic est appliquée pour générer de faux revenus à des éditeurs frauduleux qui sont payés en fonction du nombre de clics sur les publicités placées sur leurs sites web. Enfin, la fraude au clic peut être exploitée comme un moyen de saboter la concurrence - il s'agit d'une méthode visant à saper la visibilité ou les performances positives de la campagne d'un concurrent, qui peut être adoptée par ce dernier[1109].

La fraude au clic peut se présenter sous de nombreuses formes, en fonction de différents facteurs : de simples clics artificiels créés par des robots qui effectuent des visionnages répétitifs d'une publicité, à des activités complexes qui incluent de grandes quantités de matériel compromis, l'utilisation de logiciels malveillants, et même des personnes réelles qui sont prises en charge pour effectuer des clics trompeurs. Par exemple, l'injection de clics fait référence à une pratique dans laquelle les utilisateurs ne sont pas conscients que des clics artificiels ou faux sont ajoutés dans une application[1110].

[1107] Fireweb, « *Qu'est-ce que la fraude au clic ou les clics invalides et comment on peut s'en protéger ?* », 2022. https://fireweb.ro/ce-este-frauda-prin-click-si-cum-ne-putem-proteja/.

[1108] *What Is Click Fraud ? Comment identifier et prévenir les clics frauduleux*, BigCommerce, consulté le 27 novembre 2024. https://www.bigcommerce.com/glossary/click-fraud/.

[1109] *What Is Click Fraud?*, Integral Ad Science, consulté le 27 novembre 2024. https://integralads.com/insider/what-is-click-fraud/.

[1110] *What Is Click Injection?*, Adjust, consulté le 27 novembre 2024, https://www.adjust.com/glossary/click-injection/.

354. Détection, sécurisation, analyse du trafic. Dans ce contexte, il est nécessaire de détecter la fraude au clic dans le secteur, car c'est le seul moyen de se protéger contre les pertes qui la principale motivation de la publicité et de parvenir à une concurrence loyale. L'analyse du trafic avant qu'il n'atterrisse sur la page couvrira certains des aspects les plus pertinents en termes de proactivité, mais très souvent sous-estimés.

355. La fraude publicitaire dite « stacking ». Le *stacking* d'annonces, une technique de fraude publicitaire souvent cachée derrière les publicités apparemment légitimes deviennent de plus en plus une nuisance dans l'écosystème de la publicité numérique. Cette méthode consiste à diffuser plusieurs publicités dans un espace publicitaire afin qu'une seule soit vue par l'utilisateur, tandis que toutes les autres sont cachées et rapportent de l'argent à l'éditeur. Cependant, cette pratique entraîne un gaspillage des budgets publicitaires, car ils sont dépensés pour des affichages qui ne peuvent pas être vus, qui ne peuvent pas atteindre l'utilisateur[1111].

Même si l'utilisateur réel peut voir une publicité et interagir avec elle, de nombreuses publicités sont enterrées les unes au-dessus des autres, générant des vues et des clics potentiels sans que les annonceurs en aient conscience. Ce phénomène érode les budgets publicitaires, obligeant les annonceurs à payer pour des affichages publicitaires invisibles et peu susceptibles d'avoir un impact sur l'utilisateur[1112].

356. Superposition publicitaire invisible. *Ad stacking* se produit principalement dans la publicité mobile, où l'espace publicitaire est limité et où les utilisateurs sont moins attentifs aux détails. Les utilisateurs qui se font passer pour des éditeurs en profitent pour gagner plus d'argent grâce à la publicité, sans apporter valeur ajoutée aux annonceurs. Cela entraîne non seulement des pertes pour les annonceurs, mais peut également altérer les niveaux de réussite des campagnes, car les données sur les vues et les clics sont erronées[1113].

357. Méthodologies de vérification et normes de visibilité. Le *stacking* de publicités peut être un *cookie* difficile à détecter, car les publicités cachées ne sont pas visibles pour les utilisateurs. Cependant, il existe un certain nombre d'approches permettant d'identifier cette pratique malveillante. Par exemple, l'analyse du code source des pages web peut révéler que plusieurs publicités ont été placées dans un espace publicitaire. En outre, le contrôle des performances de la campagne et l'analyse des données sur les vues et les clics peuvent indiquer avec précision qu'il y a empilement de publicités[1114].

[1111] *Ad Stacking*, Singular, consulté le 27 novembre 2024. https://www.singular.net/glossary/ad-stacking/.
[1112] *What Is Ad Stacking ? Ad Stacking Definition* , Bigabid (blog), consulté le 26 novembre 2024. https://www.bigabid.com/glossary/ad-stacking/.
[1113] *What is ad stacking?*, AppsFlyer mobile glossary", consulté le 26 novembre 2024. https://www.appsflyer.com/glossary/ad-stacking/.
[1114] *What Is Ad Stacking and How to Prevent It*, Opticks Security, 2021. https://blog.optickssecurity.com/what-is-ad- stacking.

358. Design manipulateur. L'approche nécessaire pour lutter contre l'*upselling* doit impliquer l'annonceur, l'éditeur et le logiciel publicitaire. Comme indiqué plus haut, les annonceurs doivent également surveiller et mesurer attentivement leurs performances. Les éditeurs doivent mettre en œuvre des stratégies de prévention de la fraude et veiller à ce que la publicité soit affichée ouvertement et avec précision. Les annonceurs ont également un rôle clé à jouer dans la détection et la prévention de l'empilement des publicités, puisqu'ils utilisent des technologies avancées pour surveiller et analyser le flux de communication[1115].

e). Cyber-harcèlement et harcèlement en ligne

359. Avec la croissance de l'accès à l'internet et le développement des plateformes de réseaux sociaux, l'environnement en ligne est devenu non seulement un espace d'interaction, mais aussi un terrain propice aux comportements abusifs. Le cyberharcèlement et le harcèlement en ligne sont deux phénomènes complexes, apparus récemment, qui touchent un nombre important de personnes, leur causant des dommages émotionnels, psychologiques et, dans certains cas, physiques.

360. L'érosion de la vie privée : les doubles numériques. L'article « Généalogie du Doppelgänger numérique » de Bernard E. Harcourt offre une perspective pertinente sur les risques des « doppelgangers » dans le contexte du harcèlement en ligne et du cyber-harcèlement.[1116] Dans un environnement numérique où l'identité de chaque individu est représentée et traitée par le biais de données, le contrôle de ses propres informations devient un défi majeur. Le double numérique, une construction numérique alimentée par des données personnelles collectées à partir de diverses sources en ligne, peut être utilisé à mauvais escient par des individus malveillants pour traquer et harceler les utilisateurs. Cette dynamique accroît la vulnérabilité des individus aux attaques numériques.[1117]

361. La lutte contre le harcèlement en ligne : stratégies combinées législatives et technologiques. Le cyberharcèlement est facilité par la disponibilité et l'accessibilité des données personnelles sur les plateformes numériques[1118]. Harcourt souligne comment les informations partagées publiquement ou collectées sans consentement peuvent être utilisées

---

[1115] *What Is Ad Stacking and How Does It Work?*, Adjust, consulté le 26 novembre 2024, https://www.adjust.com/glossary/ad-stacking/.

[1116] B.E. Harcourt, « *5. Généalogie du Doppelgänger numérique ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.125-149. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-125?lang=fr.

[1117] Ibidem

[1118] V. Mind, "*How to Protect Yourself From Cyberstalking*", verywell mind, 2024. consulté le 27 novembre 2024. https://www.verywellmind.com/what-is-cyberstalking-5181466.

pour surveiller les activités d'un utilisateur, créer des profils détaillés et même manipuler ou menacer les victimes. Dans un monde où le double numérique devient une extension de l'identité réelle, les risques associés à ce phénomène sont amplifiés, en particulier dans le contexte des réseaux sociaux, où les frontières entre le public et le privé sont souvent floues.[1119] Un autre aspect important est lié à la difficulté juridique et technologique de protéger les utilisateurs contre le cyber-harcèlement. Dans le travail on mentionne que bien que certaines juridictions aient mis en place une législation pour criminaliser le harcèlement en ligne, la double criminalité complique l'identification et la poursuite des auteurs[1120]. Les attaquants peuvent utiliser des outils technologiques pour cacher leur identité ou exploiter les vulnérabilités des systèmes numériques. En outre, le fait que les utilisateurs ne sachent pas comment gérer leurs propres données contribue à créer un environnement favorable au cyber-harcèlement.[1121]

À cet égard, il est essentiel d'élaborer des stratégies combinant des mesures législatives efficaces et des solutions technologiques avancées capables de protéger les utilisateurs contre le harcèlement en ligne. Dans le même temps, l'éducation des individus à la vie privée et à la gestion des données personnelles est une étape cruciale pour réduire la vulnérabilité à de telles attaques. Le harcèlement en ligne, alimenté par l'évolution du dédoublement numérique, souligne l'urgence de réponses sociales, juridiques et technologiques intégrées.

[1119].B. E, Harcourt, « *5. Généalogie du Doppelgänger numérique ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-125?lang=fr.

[1120]B.E. Harcourt, *« 4. Notre pavillon en verre-miroir ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.101-124. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-101?lang=fr.

[1121] "*What is cyberstalking and how to prevent it*?", Tech Target, consulté le 27 novembre 2024. https://www.techtarget.com/searchsecurity/definition/cyberstalking.

Section 2. **ATTEINTES CONTEMPORAINES À LA VIE PRIVÉE : INTERCEPTION, SURVEILLANCE ET BIOMÉTRIE**

362. Dangers potentiels. Ce section se concentre sur les menaces que les pratiques illégales de surveillance et d'interception font peser sur la vie privée. Tout d'abord, il examine les moyens par lesquels les communications peuvent être interceptées illégalement, en mettant l'accent sur les techniques d'écoute et de contrôle clandestines et sur les conséquences juridiques de ces activités. En outre, la surveillance non autorisée est abordée, y compris la technologie de géolocalisation qui peut permettre de surveiller l'emplacement d'une personne sans son consentement. Le thème de la cybersécurité et du piratage informatique est abordé, explorant les façons dont les failles de sécurité et l'accès non autorisé aux systèmes informatiques peuvent menacer le droit à la vie privée. Les implications des technologies de reconnaissance faciale et biométrique, qui peuvent être utilisées pour surveiller et suivre les individus sans leur consentement, et les problèmes de protection de la vie privée liés à utilisation sont également analysés. Enfin, le chapitre se termine par une discussion sur les dispositifs IoT (Internet of Things) et la manière dont ils collectent et utilisent les données personnelles, en soulignant leurs dangers potentiels pour la protection des données et de la vie privée.

§1. INTERCEPTION ILLÉGALE DES COMMUNICATIONS

363. De la tour centrale de Foucault au réseau mondial de surveillance. L'interception des communications est devenue l'une des formes les plus sophistiquées et les plus insidieuses d'atteinte à la vie privée à l'ère numérique. Contrairement à la surveillance traditionnelle, qui impliquait une écoute directe ou un suivi physique, l'interception numérique a souvent lieu à l'insu des utilisateurs, cachée dans des flux de données complexes et des processus technologiques invisibles[1122]. Le modèle panoptique, tel qu'il est décrit par Foucault, permet de comprendre ce phénomène. Dans l'architecture numérique actuelle, la "tour centrale" est remplacée par des réseaux mondiaux de surveillance électronique, où des agences de renseignement et des acteurs privés analysent et extraient des informations de tous les recoins des interactions en ligne.[1123]

[1122] D.Ventre, P.Guillot, *Electronic Communication Interception Technologies and Issues of Power*, Wiley – ISTE, 2023.
[1123] B.E. Harcourt, *«3. Le Panoptique de Jeremy Bentham ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.77-97. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.

L'interception des communications, en particulier par le biais de programmes tels que Prism ou l'utilisation d'autres technologies de surveillance de masse, montre à quel point cette pratique a été intégrée dans les mécanismes de l'État moderne[1124]. Harcourt note que ces programmes permettent de collecter non seulement des métadonnées - révélant qui communique avec qui et quand - mais aussi le contenu même des messages.[1125] Cela soulève d'importantes questions juridiques et éthiques, d'autant plus que nombre de ces pratiques sont mises en œuvre sans base juridique solide ou sans transparence. En outre, l'utilisation d'entreprises privées comme intermédiaires dans ce processus complique encore la responsabilité juridique, en fragmentant la responsabilité entre le gouvernement et les acteurs privés.[1126]

364. Les effets de l'interception : vulnérabilité, réticence, autocensure. Les effets sociaux des interceptions illégales sont aussi alarmants que les effets juridiques. La surveillance constante des communications crée un sentiment de vulnérabilité, les utilisateurs devenant de plus en plus réticents à partager des pensées ou des informations personnelles[1127]. Cette autocensure n'affecte pas seulement la liberté d'expression, mais aussi les relations sociales et la dynamique de la confiance entre les citoyens et les institutions. En outre, comme le suggère l'auteur, ce type de surveillance peut être utilisé comme un outil de contrôle politique, où les dissidents ou les personnes gênantes pour les régimes autoritaires sont identifiés et supprimés[1128]. Dans un tel monde, l'interception illégale devient non seulement une question de sécurité nationale, mais aussi un mécanisme d'érosion des droits démocratiques.

365. L'évolution technologique impose une évolution législative. À mesure que la technologie progresse, il devient essentiel de développer des mécanismes juridiques pour protéger les communications privées contre les abus. Dans un monde de plus en plus interconnecté, la réglementation traditionnelle doit être complétée par de nouveaux instruments juridiques suivre le rythme de l'évolution technologique. En même temps, la transparence dans l'utilisation des outils d'interception doit être une priorité pour éviter leur utilisation abusive. Cette bataille entre sécurité et vie privée définit les défis juridiques du 21e siècle, à une époque où chaque conversation peut devenir un point d'accès à la surveillance.

[1124] *PRISM*, *United States Surveillance Program*, Britannica, 2024. https://www.britannica.com/topic/PRISM-United-States-surveillance-program.

[1125] B.E. Harcourt, *3. Le Panoptique de Jeremy Bentham. La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.77-97. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.

[1126] R. Quann, *Check out SS8's latest lawful & location intelligence insights*, SS8, 2024. https://www.ss8.com/lawful-interception-considerations-for-private-mobile-networks/.

[1127] Perception Survey Report, *The impact of communication surveillance on Human Rights defenders in Kenya*, Defenders Coalition, 2021. consulté le 28 novembre 2024, https://privacyinternational.org/report/4469/defenders-coalition-impact-communication-surveillance-hrds-kenya /.

[1128] B.E. Harcourt, 3. *Le Panoptique de Jeremy Bentham ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.77-97. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.

366. L'interception : une technique autoritaire dans une démocratie libérale. L'article « L'éclipse de l'humanisme » traite de la dimension invasive des technologies numériques, avec un accent particulier sur l'interception des communications. Il souligne comment le développement d'outils de surveillance de masse transforme la communication personnelle en une ressource exploitable, souvent sans le consentement explicite des utilisateurs[1129]. La surveillance numérique par l'interception des communications devient non seulement un outil de contrôle, mais aussi une menace directe pour le droit à la vie privée[1130]. Harcourt souligne que ces pratiques ne sont plus limitées aux régimes autoritaires, mais sont également intégrées dans les démocraties libérales sous le couvert de la sécurité nationale[1131].

L'une des questions centrales abordées est la banalisation de l'interception des communications dans le cadre de la société contemporaine. Grâce aux technologies modernes, telles que l'analyse des métadonnées, l'enregistrement des appels et la surveillance des messages en ligne, les frontières entre publique et privée deviennent de plus en plus floues.[1132] [1133] Harcourt souligne que les utilisateurs, bien que conscients de cette surveillance, ont tendance à l'accepter comme une norme inévitable du monde numérique. Cette intériorisation de la surveillance réduit les résistances sociales et favorise l'expansion de pratiques qui pourraient être considérées comme illégales ou contraires à l'éthique[1134].

367. La relation entre sécurité et vie privée. D'un point de vue juridique, l'interception des communications pose des problèmes importants, en particulier en l'absence de réglementations claires ou de mécanismes efficaces d'application de la loi. L'auteur attire l'attention sur la manière dont les entreprises technologiques collaborent avec les gouvernements pour faciliter l'accès aux données personnelles, souvent sous le couvert de la sécurité nationale[1135]. Dans ce contexte, le manque de transparence et de responsabilité de la part de ces entités crée un

---

[1129] B.E. Harcourt, « *6. L'éclipse de l'humanisme ». La Société d'exposition Désir et désobéissance à l'ère numérique,* Le Seuil, 2020. p.150-160. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-150?lang=fr.

[1130] *Protection des Données dans le Secteur des Communications Électroniques*, EUR-Lex, consulté le 27 novembre 2024. https://eur-lex.europa.eu/RO/legal-content/summary/data-protection-in-the-electronic-communications- sector.html.

[1131] B.E. Harcourt, *6. L'éclipse de l'humanisme ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.150-160. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-150?lang=fr.

[1132] *Spyware and Surveillance: Threats to Privacy and Human Rights Growing, UN Report Warns*, OHCHR, consulté le 27 novembre 2024 https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report.

[1133] C. Carpenter, "*Privacy and Proportionality: Examining Mass Electronic Surveillance under Article 8 and the Fourth Amendment*", International and Comparative Law Review vol.20, no.1, 2020. p.27-57 https://doi.org/10.2478/iclr-2020-0002.

[1134] B.E. Harcourt, 6. *L'éclipse de l'humanisme ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.150-160. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-150?lang=fr.

[1135] *Op. cit.*

environnement propice aux abus. En outre, la complexité des réseaux de communication mondiaux rend difficile l'identification et la sanction des auteurs de ces violations.
Pour relever ces défis, le chapitre propose de réévaluer la relation entre la sécurité et la vie privée. Un cadre juridique international plus solide est nécessaire pour limiter la collecte et l'utilisation de données personnelles sans consentement. Parallèlement, des technologies plus sûres doivent être développées pour protéger les communications privées d'un accès non autorisé, telles que décrites par Harcourt, ne sont pas seulement un problème technologique, mais une menace fondamentale pour les libertés individuelles et les principes démocratiques.

A. Analyse du délit d'« interception illégale d'une transmission de données informatiques »

368. Qualification pénale de l'interception. Selon l'article 361 du code pénal, « (1) L'interception illégale d'une transmission non publique de données informatisées destinée à un système informatique, provenant d'un tel système ou effectuée à l'intérieur d'un système informatique est passible d'une peine d'emprisonnement d'un à 5 ans. (2) La même peine s'applique à l'interception illégale d'une émission électromagnétique provenant d'un système informatique et contenant des données informatiques non publiques. »
Tout d'abord, nous tenons à souligner que cette infraction n'a pas d'équivalent dans l'ancien code pénal roumain, le texte étant repris dans son intégralité de la loi 161/2003, qui était basée sur le texte proposé par la Convention européenne sur la cybercriminalité du 23 novembre 2001, à Budapest, et ce parce que la Roumanie n'avait pas la possibilité objective de construire cette législation par elle-même, étant donné le manque d'expérience dans le sujet. Plus précisément, les infractions dans le domaine des technologies de l'information sont l'un des domaines les plus récents de la vie juridique, à la fois dans le monde entier et, en particulier, en Roumanie[1136].
369. Le régime des interceptions. De l'espionnage classique à l'environnement numérique. Pour l'essentiel, l'infraction prévue à l'article 361 du code pénal appartient à la catégorie des formes traditionnelles d'espionnage, puisque la norme juridique sanctionne à la fois l'interception de transmissions de données (article 361, paragraphe 1) et l'interception d'émissions électromagnétiques (article 361, paragraphe 2).
Ainsi, la doctrine[1137] a estimé que l'objet juridique particulier de l'infraction d'interception illégale d'une transmission de données informatiques consiste en l'ensemble des relations

[1136] G. Antoniu, T. Toader, *Explicațiile noului Cod Cod penal, vol. IV*, Universul Juridic, Bucarest, 2016, p.865.
[1137] G. Antoniu, T. Toader*, Op. cit.,* p.865-866.

sociales concernant la confidentialité des données informatiques (le droit au secret des données). La même doctrine considère que l'incrimination des activités d'interception illégale fait partie des mesures juridiques visant à protéger le droit au secret des communications, c'est-à-dire le droit à la protection de la correspondance tel qu'il est énoncé à l'article 8 de la Convention Européenne des Droits de l'Homme.

a). Éléments constitutifs du délit

370. L'objet matériel de l'infraction. En outre, l'objet matériel de l'infraction est constitué par le flux de paquets informatiques (la séquence de bits « 0 » et « 1 », c'est-à-dire la séquence d'impulsions électriques résultant de la variation contrôlée de la tension), qui sont transportés d'un équipement informatique à un autre ou à l'intérieur d'un même système informatique, et auxquels s'intéresse l'auteur de l'infraction. En particulier, l'objet matériel peut être le support technique par lequel se réalise la communication de données entre les équipements, à partir des ports de sortie des postes de travail (connecteurs de cartes réseau ou téléphoniques des modems) et en continuant avec les câbles de transport (réseau ou téléphoniques), les boîtiers de connexion (dans lesquels se trouvent les commutateurs de réseau, les répartiteurs de réseau, les routeurs, etc. Dans le cas du paragraphe 2), l'objet matériel est l'énergie électromagnétique (émission) qui rayonne ou se trouve sous forme résiduelle ou incontrôlée (incontrôlable) à proximité immédiate des équipements électroniques composant le système informatique concerné. Ainsi, l'émission électromagnétique autour d'un équipement (imprimante, moniteur, câble, etc.) ne peut être considérée comme un objet tangible si, au moment de l'interception (capture), il n'était pas connecté à un système informatique dans les conditions du paragraphe 2).[1138]

371. Sujet actif, toute personne physique responsable. Le sujet actif de l'infraction peut être toute personne pénalement responsable, la règle de droit ne prévoyant pas d'exigence particulière à cet égard, et qui utilise des équipements dédiés à la réalisation de cette activité illégale, les connaissances de l'auteur en matière de technologie informatique n'étant pas pertinentes. En outre, bien que cela ne soit pas pertinent pour l'appréhension de l'infraction, nous considérons que le sujet actif a un intérêt à espionner la personne lésée, car il est de notoriété publique, comme indiqué plus haut, que l'interception des transmissions de données

[1138] M. Dobrinoiu, *« Lois de l'Internet »*, disponible à l'adresse, https://www.legi-internet.ro/articole-drept-it/infractiunea-de-interceptare-ilegala-a-unei- transmisii-de-date-informatice.htmmlinterceptare-ilegala-a-una-transmisii-de-date-informatice.html.

informatiques ou des émissions électromagnétiques d'un système informatique est l'essence même de l'espionnage.

372. Le concept de système informatique et de biens informatiques. Avant de passer au contenu constitutif de l'infraction, composé des aspects objectifs et subjectifs, il est important de mentionner que la condition préalable de cette infraction est liée à l'existence d'un système informatique, l'infraction ne pouvant exister en l'absence d'un tel système ou de données informatiques sur lesquelles l'auteur agit de la manière prévue par l'article 361 du code pénal. Puisque nous avons parlé de la transmission de données informatiques ou d'émissions électromagnétiques provenant d'un système informatique, il est important de noter que les législations nationales définissent les concepts de « système informatique » et de « données informatiques ». Ainsi, selon l'article 181 du Code pénal, « (1) Un système informatique est tout dispositif ou ensemble de dispositifs interconnectés ou fonctionnellement liés, dont un ou plusieurs assurent le traitement automatique de données, à l'aide d'un programme informatique. (2) On entend par données informatiques toute représentation de faits, d'informations ou de concepts sous une forme susceptible d'être traitée par un système informatique ». Par ailleurs, il est important de noter que cette infraction ne peut exister en l'absence de transmissions de données informatiques ou d'émissions électromagnétiques sur lesquelles l'auteur agit dans les conditions prévues par la norme légale afin d'atteindre la finalité voulue par le législateur, à savoir les systèmes informatiques qui les contiennent ou dont ils proviennent ou qui leur sont destinés.

373. Identification de l'élément matériel de l'infraction. En ce qui concerne l'élément matériel de la partie objective de l'infraction, nous constatons que dans les deux variantes proposées par l'article 361 du Code pénal, il s'agit de l'acte d'interception. Cependant, la doctrine indique que l'acte d'interception doit remplir une série de conditions essentielles pour être soumis à l'élément matériel de la partie objective, comme suit : Interception sans droit - exigence pour les deux variantes normatives : le sujet actif n'est pas autorisé par la loi ou le contrat ou dépasse les limites de l'autorisation ; L'interception concerne une transmission non publique de données informatiques qui est destinée à un système informatisé, provient d'un tel système ou est réalisée à l'intérieur d'un système informatisé, dans le cas de la variante visée au paragraphe 1; Interception concernant une émission électromagnétique d'un système informatisé, contenant des données qui ne sont pas publiques, dans le cas de la variante visée au paragraphe 2 ;[1139]

[1139] G. Antoniu, T. Toader, *Op. cit.,* pp.867.

374. Espionnage en réseau, surveillance indiscriminée. Le détournement de paquets est l'une des infractions les plus difficiles à commettre et constitue également une menace sérieuse pour les communications Internet. Chaque paquet envoyé sur l'internet peut passer par un grand nombre d'ordinateurs et de réseaux avant d'atteindre sa destination. À l'aide d'un intercepteur de paquets, les pirates peuvent intercepter des paquets de données (y compris des messages de connexion, des transmissions d'identifiants numériques de cartes de crédit, des paquets de courrier électronique, etc. Après avoir intercepté un paquet, le pirate peut l'ouvrir et voler le nom d'hôte, le nom d'utilisateur et le mot de passe associés au paquet. Les pirates utilisent l'un des types d'interception de paquets les plus courants avant les attaques IP. Les experts en matière de sécurité appellent souvent le détournement de paquets comme de « l'espionnage en réseau » (network snooping) ou « surveillance cachée » (promiscous monitoring). En général, un dispositif ou un ordinateur intrus peut se placer à n'importe quel endroit d'un système informatique ou d'un réseau informatique dans le but d'intercepter le trafic de messages. Il existe deux types d'attaques possibles :

- les attaques passives, où l'intrus « observe » les informations qui passent par le canal, sans interférer avec le flux ou le contenu des messages ;
- les attaques actives, où l'intrus vole des messages ou modifie, rejoue ou insère de faux messages, etc.[1140]

375. Systèmes d'interception controversés : le système Carnivore. Pour que l'interception soit illégale au sens de l'article 361 du Code pénal, comme indiqué ci-dessus, elle doit être effectuée sans droit. Ainsi, l'acte d'interception ne sera pas considéré comme illicite si l'auteur a le droit de disposer des données communiquées, s'il agit sur ordre ou avec l'autorisation des participants à la communication ou si, sur la base d'une disposition légale spécifique, la surveillance est autorisée dans l'intérêt de la sécurité nationale. Au fil du temps, cette surveillance a été mise en œuvre au niveau des législations nationales, ce qui a suscité diverses controverses dans le monde entier. Par exemple, le projet de surveillance technique et d'interception le plus controversé est sans doute le Système Carnivore, développé par le Bureau Fédéral d'Investigations (FBI) des États-Unis, qui a été conçu pour permettre à l'agence d'accéder plus facilement aux cyberactivités de criminels potentiels. En termes d'évolution du projet, Carnivore a représenté la troisième génération de logiciels et d'applications de surveillance électronique utilisé par le FBI. Les informations sur la première version n'ont jamais été rendues publiques ; de nombreux experts affirment qu'elle est à la base d'un programme commercial actuel appelé Etherpeek. En 1997, le FBI a développé et mis en service

[1140] V.V. Patriciu, *Criptografia și securitatea rețelelor de calculatoare*, Editura Tehnică, Bucarest, 1994. p.22.

une deuxième génération de programmes d'interception et de surveillance des technologies de l'information sous le nom d'Omnivore. Selon les données fournies par le FBI lui-même, Omnivore a été conçu spécifiquement pour surveiller le trafic de courrier électronique arrivant (acheminé) par un ISP (Internet Service Provider) particulier et le capturer par expéditeur (source). Omnivore a été abandonné fin 1999 au profit d'un système beaucoup plus complexe appelé Dragon Ware Suite, qui permettait au FBI de reconstruire (recompiler, reconfigurer) les messages électroniques, les fichiers téléchargés sur Internet et même les pages Web[1141].

376. La conséquence immédiate de l'infraction est la création d'un danger pour la confidentialité des transmissions de données informatiques ou des émissions électromagnétiques. Il doit y avoir un lien de causalité entre l'acte d'interception et la mise en danger de la confidentialité des transmissions de données informatiques ou des émissions électromagnétiques pour que l'infraction soit établie.

377. La nécessité de l'intention. En ce qui concerne l'aspect subjectif, il est important de noter que l'infraction est commise exclusivement avec intention (directe ou indirecte), le motif et le but de l'activité criminelle ne sont pas des éléments de l'aspect subjectif, mais ils peuvent contribuer à l'individualisation de la peine par le juge magistrat.

b). Interventions de la CEDH en lien avec l'interception de conversations.

378. Au niveau du droit international et européen, la protection des communications privées découle du souci même de protéger la vie privée et est régie par des actes normatifs tels que la Déclaration universelle des droits de l'homme (1948), qui stipule que « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur ou à sa réputation »[1142]. L'Assemblée Générale des Nations Unies a adopté cette déclaration le 10 décembre 1948, proclamée le même jour, appelant les États membres des Nations Unies à faire tout leur possible pour que ce document historique « soit distribué, affiché, lu et commenté, principalement dans les écoles et autres établissements d'enseignement, quel que soit le statut politique des pays ou de leurs territoires »[1143]. L'Article 8 de la Convention Européenne des Droits de l'Homme complète la Déclaration Universelle des Droits de l'Homme en stipulant que :

[1141] L. Bird, *Internet-Ghid complet de utilizare*, Editura Corint, Bucarest, 2004, p.331.

[1142] Voir *La Déclaration universelle des droits de l'homme* , sur https://www.ohchr.org/sites/default/files/UDHR/Documents/UDHR_Translations/rum.pdf

[1143] Voir la *Déclaration universelle des droits de l'homme du 10 décembre 1948.* https://legislatie.just.ro/Public/DetaliiDocument/22751.

« 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé et de la morale, ainsi qu'à la défense des droits et libertés d'autrui. »[1144].

379. Pacte international relatif aux droits civils et politiques. Cette pratique, bien que strictement réglementée par le droit pénal et les normes internationales, continue d'utilisée par des entités étatiques et non étatiques à des fins diverses. Dans le contexte du droit international, l'interception illégale relève de l'article 17 du « Pacte international relatif aux droits civils et politiques », qui énonce la garantie contre les ingérences extérieures dans la vie privée :

1. «Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur ou à sa réputation.

2. Toute personne a droit à la protection de la loi contre de telles ingérences ou interventions.»[1145]

380. Assurer la sécurité, respecter la vie privée. Un certain nombre d'affaires ont été portées devant la Cour Européenne des Droits de l'Homme (CEDH) en raison du manque d'équilibre entre la nécessité d'une intrusion de l'État dans la vie privée des individus à des fins de sécurité nationale ou de lutte contre la criminalité et la protection de la vie privée. Klass et autres vs. Allemagne (1978[1146]) est une affaire historique dans laquelle la CEDH s'est prononcée pour la première fois sur la compatibilité des mesures de surveillance nationale avec les dispositions de la Convention Européenne des Droits de l'Homme, avec l'Article 8 (respect du droit à la vie privée et familiale, au domicile et à la correspondance). Les plaignants étaient des citoyens allemands qui contestaient la légalité d'une loi allemande, la Loi G10, qui autorise la surveillance secrète des services postaux et des télécommunications dans l'intérêt de la sécurité nationale, en faisant valoir que la loi allemande violait leurs droits au titre de l'Article 8 de la Convention. Le gouvernement allemand a contesté l'accusation en faisant valoir que cette surveillance est nécessaire pour lutter contre les menaces terroristes et les activités d'espionnage. Les questions clés dans l'affaire Klass et autres vs. Allemagne sont les suivantes : 1. la surveillance secrète viole-t-elle l'article 8 de la Convention Européenne des Droits de

---

[1144] Voir *La Déclaration universelle des droits de l'homme*, p.10. https://www.echr.coe.int/documents/d/echr/convention_ron,

[1145] Voir le *Pacte international relatif aux droits civils et politiques, adopté le 16 décembre 1966 ; ratifié par la Roumanie le 31 octobre 1974*, p.6. https://avp.ro/wp-content/uploads/2020/07/pact_mnp.pdf,

[1146]Voir CEDH, *Case of Klass and others v. Germany*, no 5029/71, Strasbourg, 1978 https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}.

l'Homme ? Et 2. Si une telle ingérence existe, est-elle justifiée comme étant « nécessaire dans une société démocratique » à des fins de sécurité nationale et de sûreté publique ? La CEDH a rendu son arrêt dans cette affaire le 6 septembre 1978, statuant que, en ce qui concerne la violation de l'Article 8, la Cour admet que la surveillance secrète constitue une ingérence dans le droit à la vie privée et à la correspondance. Toutefois, elle admet qu'une telle ingérence peut être justifiée si elle remplit certaines conditions.

381. Justification de la surveillance. En ce qui concerne la justification de l'ingérence, la CEDH a reconnu que les états européens sont confrontés à un certain nombre de défis nécessitant des mesures de surveillance secrète, tout en reconnaissant que les états nationaux doivent trouver un équilibre entre ces mesures et le droit au respect de la vie privée de leurs citoyens. La Cour a estimé dans cette affaire que la législation allemande était suffisamment équilibrée dans sa protection contre les abus, en prévoyant des garanties raisonnables pour protéger la vie privée, telles que des limitations du champ d'application de la surveillance et une réglementation visant à prévenir les mesures arbitraires ou disproportionnées. En conclusion, la CEDH a jugé dans cette affaire que l'Allemagne n'avait pas violé l'Article 8 de la Convention, car les mesures ordonnées étaient proportionnées et contrôlées pour prévenir l'abus des droits individuels[1147].

En conclusion, l'affaire Kass et autres vs. Allemagne, en plus d'être la première affaire jugée par la CEDH, a établi des principes importants en ce qui concerne la vie privée des citoyens et la surveillance justifiée.

382. La compatibilité de la surveillance de l'État avec le respect de la vie privée. La deuxième affaire que nous mentionnons dans cette section en rapport avec l'interception illégale des communications est l'affaire Roman Saharov vs. Russie, une autre affaire historique dans laquelle la CEDH s'est prononcée sur la compatibilité des pratiques de surveillance secrète de la Russie avec les droits individuels en vertu de l'Article 8 de la Convention Européenne des Droits de l'Homme. Les informations relatives à cette affaire remontent à décembre 2003, lorsque Roman Saharov, journaliste et président de la section de Saint-Pétersbourg de la Fondation pour la Défense de la Glasnost, a engagé une procédure judiciaire contre trois opérateurs de téléphonie mobile russes, affirmant qu'ils avaient violé le droit au respect de la vie privée dans les communications téléphoniques. Il reprochait notamment aux opérateurs d'avoir permis aux agences de sécurité d'intercepter des conversations sans autorisation ou mandat judiciaire, ce qui a conduit à une surveillance illimitée de toutes les communications téléphoniques.

[1147]Voir Conseil de l'Europe, *Case law of the European Court of Human Rights concerning the protection of personal data, Starsbourg, 2017*, p.18. https://rm.coe.int/case-law-on-data-protection/1680766992

Le tribunal national a rejeté la plainte de Saharov, estimant qu'il n'avait pas fourni de preuves selon lesquelles ses conversations avaient été interceptées ou que les opérateurs de communications mobiles avaient transmis illégalement des informations à des entités non autorisées. Dans cette affaire, la Cour a estimé que la simple installation d'équipements de surveillance ne constituait pas une atteinte à la vie privée. Trois ans plus tard, en 2006, Saharov a déposé une plainte auprès de la CEDH, alléguant que l'interception de communications sans contrôle adéquat contre les abus des services de sécurité violait son droit à la vie privée en vertu de l'Article 8. Saharov se plaignait également de l'absence de recours effectif au niveau national pour se protéger contre de telles pratiques, invoquant l'Article 13[1148] de la Convention[1149]. Ainsi, le 4 décembre 2015, la CEDH a jugé que le système juridique de la Fédération de Russie n'offrait pas de garanties suffisantes contre l'application arbitraire de la surveillance et les abus[1150], la Cour identifiant un certain nombre de lacunes, telles que les vastes pouvoirs discrétionnaires des autorités pour intercepter des communications pour un large éventail d'infractions sans limites claires ; l'absence de surveillance ciblée, les mesures de surveillance n'étant pas limitées à une seule personne soupçonnée d'activité criminelle, ce qui permet d'étendre éventuellement la surveillance à d'autres personnes ; des critères de surveillance non définis, la législation de la Fédération de Russie ne définissant pas très clairement les conditions dans lesquelles les opérations de surveillance sont lancées, menées et achevées ; un contrôle indépendant insuffisant. En conclusion, la Cour a jugé que le système d'interception secrète des communications mobiles de la Fédération de Russie violait l'Article 8 de la Convention Européenne des Droits de l'Homme dans l'affaire Saharov vs. Russie[1151].

B. Surveillance non autorisée et géolocalisation

383. Réglementation de la surveillance non autorisée et de la géolocalisation. En définissant la terminologie et le cadre théorique, nous fournissons une base pour analyser la manière dont la surveillance non autorisée et la géolocalisation sont réglementées au niveau international. En même temps, les études de cas présentées dans ce chapitre contribuent à étayer

[1148] Voir CEDH, texte de la Convention pour la protection des droits de l'homme et des libertés fondamentales, p.12 https://www.echr.coe.int/documents/d/echr/convention_ron.
[1149] Voir CEDH, *Case of Roman Zakharov v. Russia*, no.47143/06, 2015 (Application no. 47143/06) consulté sur https://hudoc.echr.coe.int/eng?i=001-159324.
[1150] Voir M. Milanovic *Blockbuster Strasbourg Judgment on Surveillance in Russia*, 2015 consulté sur https://www.ejiltalk.org/blockbuster-strasbourg-judgment-on-surveillance-in-russia/.
[1151] Voir European Human Rights Advocacy Centre., *Journalist wins decision establishing « arbitrary and abusive » secret mobile phone surveillance in Russia, 2015* consulté à l'adresse https://ehrac.org.uk/en_gb/journalist-wins-decision-establishing-arbitrary-and-abusive-secret-mobile-phone-surveillance-in-russia/.

les conclusions sur la nécessité de garanties juridiques solides qui protègent les droits fondamentaux des individus dans une société technologiquement avancée. Depuis le début des études sur la personnalité numérique (*digital persona*) et l'utilisation des données à des fins de surveillance, la littérature indique que l'information, pour être utile, doit être attribuable à une personne qui peut être localisée[1152].

384. La surveillance non autorisée, caractéristique des régimes totalitaires. La surveillance non autorisée est définie comme la collecte, le stockage et le contrôle des données et des activités d'une personne sans son consentement. La surveillance non autorisée se réfère également à la situation où les communications sont interceptées, où un contrôle visuel est appliqué et où les données collectées n'ont pas de base juridique claire. L'un des arguments les plus éloquents sur l'importance du respect de la vie privée dans les sociétés démocratiques est celui de Westin apud Benett et Raab, qui, contrairement aux sociétés totalitaires, garantit l'espace individuel et collectif, et la divulgation d'informations et la surveillance sont des conditions préalables aux sociétés démocratiques, où la vie privée est respectée et où l'autorité est responsable devant la société[1153].

385. La géolocalisation, conséquence de l'évolution numérique. En ce qui concerne les définitions de la géolocalisation, la littérature s'accorde sur le fait que la géolocalisation implique l'utilisation des technologies GPS, Wi-Fi ou des tours de téléphonie mobile pour identifier la position d'une personne, d'un groupe ou d'un appareil. La géolocalisation est utilisée dans différents contextes et secteurs, dans le marketing numérique, pour réduire la portée du contenu numérique dans les réseaux sociaux, mais aussi dans la sphère médico-légale, dans le cadre d'enquêtes. La géolocalisation soulève la question du consentement de l'utilisateur.[1154]

386. Protection internationale contre la surveillance et la géolocalisation illégales. Le cadre juridique actuel, tant international que national, offre une protection significative et importante contre la surveillance et l'utilisation illégales de la géolocalisation, mais le rythme rapide de l'évolution technologique exige des mises à jour tout aussi rapides et constantes. Les règlements de la CEDH et les dispositions du GDPR, en tant que mécanismes internationaux, constituent un point de départ solide, mais le succès d'une telle entreprise tient également compte des mises en œuvre nationales. Ainsi, à l'ère numérique, le souci de renforcer le cadre juridique est constant. Les lois internationales et nationales tendent à s'harmoniser et à offrir la meilleure protection de la vie privée des citoyens.

[1152] Voir R.A Clarke, *The Digital Persona and Its Application to Data Surveillance (La personne numérique et son application à la surveillance des données).* Inf. Soc*, 10*, 1994. p.6.

[1153] Voir C.J. Bennett, C.D Raab, C. *The Governance of Privacy : Policy Instruments in Global Perspective*, MIT Press, 2006. p.61-77

[1154] H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2010, p 110.

Le même Article 8 de la Convention Européenne des Droits de l'Homme énonce des principes internationaux clés en matière de protection de la vie privée des citoyens. À cet égard, nous prenons note de la jurisprudence pertinente, telle que l'affaire Malone vs. Royaume-Uni (1984), dans laquelle la CEDH a statué que l'interception sans cadre juridique clair violait l'article 8. Il s'agit de l'une des premières affaires importantes dans lesquelles les juges de la Cour européenne des droits de l'homme ont examiné la question de l'interception illégale des communications et l'impact qu'elle a sur la vie privée de l'individu.

387. Le comptage du trafic de données, une action illégale. L'affaire a été réglée par la CEDH le 2 août 1984 - James Malone, un antiquaire, a découvert que ses conversations téléphoniques avaient été mises sur écoute par les autorités enquêtant sur une affaire criminelle sans base juridique claire. Malone s'est plaint que ces interceptions violaient son droit à la vie privée, garanti par l'article 8 de la Convention européenne des droits de l'homme. Malone s'est également plaint de la pratique du *metering*, par laquelle les autorités collectaient des données sur les appels passés, les numéros de téléphone utilisés et la durée des appels sans mandat clair[1155]. Dans cette affaire, la CEDH a reconnu que la législation britannique de l'époque n'offrait pas de garanties suffisantes contre les ingérences arbitraires dans les communications et que les interceptions n'étaient pas réglementées au sens de la Convention, à savoir qu'elles étaient nécessaires et proportionnées au but légitime poursuivi.[1156]

La CEDH a estimé que la législation britannique n'offrait pas de garanties suffisantes contre les ingérences arbitraires dans les communications et que les interceptions n'étaient pas « prévues par la loi » au sens de la Convention. La Cour a donc conclu à une violation de l'article 8 et a jugé que le comptage et l'interception des appels constituaient une ingérence dans le droit au respect de la vie privée et que la justification des circonstances dans lesquelles ils étaient autorisés n'était pas présente dans la loi.

388. Document RIPA 2000. Cette affaire a eu un impact majeur au Royaume-Uni, mais aussi en Europe. La décision de la CEDH ayant souligné la nécessité d'un cadre juridique clair assorti de garanties contre l'utilisation abusive des tactiques, le Royaume-Uni a adopté un document supplémentaire, le Regulation of Investigatory Powers Act 2000 (RIPA)[1157], un instrument statutaire publié à l'origine le 28 juillet 2000, mis à jour par des ajouts ultérieurs, qui réglemente le pouvoir des organismes publics de procéder à des surveillances et à des enquêtes, y compris dans le domaine de l'interception des communications. Le document a été introduit

[1155] Voir G.T Marx, *What's New About the « New Surveillance » ? Classifying for Change and Continuity*. Surveillance & Society, *1*(1), 2002 p.24.
[1156] Voir P. De Hert, S. Gutwirth, *Data protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in action.* Reinventing data protection *2009*. p.14.
[1157]Voir *Regulation of investigatory powers act 2000*, GOV.UK, 2017.

par le gouvernement travailliste de Tony Blair en réponse aux avancées technologiques, au pouvoir croissant d'Internet et aux dispositifs de cryptage. La loi a été introduite à l'origine à la Chambre des Communes le 9 février 2000, puis adoptée par le Parlement le 26 juillet, avec des ajouts ultérieurs en décembre 2003, avril 2005, juillet 2006, février 2010 et une toute nouvelle loi a été introduite en novembre 2015. La loi a été révisée en 2023 et la prochaine mise à jour est prévue pour 2025[1158].

389. Surveillance d'une personne impliquée dans le trafic de stupéfiants. L'une des affaires les plus connues traitant de l'utilisation de la technologie GPS pour la géolocalisation est l'affaire Ben Faiza vs. France (2018)[1159], qui a été entendue par la CEDH après le dépôt d'une plainte alléguant la violation du droit au respect de la vie privée garanti par l'Article 8 de la Convention Européenne des Droits de l'Homme. L'affaire a été réglée le 8 février 2018 et concernait les mesures de surveillance appliquées à Mohamed Ben Faiza, un citoyen soupçonné d'être impliqué dans des opérations de trafic de stupéfiants. Le dossier public de l'affaire sur le portail de la CEDH indique que les autorités françaises ont ordonné des mesures de surveillance de Ben Faiza entre 2009 et 2010, montrant que des données téléphoniques ont été réquisitionnées le 24 juillet 2009 par la police avec l'autorisation du procureur de la République dans le cadre d'un mandat délivré à un opérateur mobile par la police avec l'autorisation du procureur de la République dans une affaire, afin d'obtenir la liste des appels émis et reçus sur quatre lignes téléphoniques appartenant au requérant, ainsi que les données de localisation de l'appelant associées à ces appels. Le dossier indique également que le 10 mai 2010, la police a reçu l'autorisation verbale du juge d'instruction d'installer un dispositif de repérage sur l'une des voitures utilisées par le requérant afin de surveiller ses déplacements. Cette mesure a été prise sans autorisation judiciaire, l'action étant justifiée par la nature urgente de l'enquête.

Plus tard, le 3 juin 2010, le juge a ordonné l'installation d'un dispositif permettant la réception et l'enregistrement des conversations dans le véhicule, ainsi que sa géolocalisation pendant un mois en juin 2010.

La Cour Européenne des Droits de l'Homme a analysé la documentation de l'affaire pour voir si les mesures ordonnées par les autorités françaises constituaient une violation du droit à la vie privée comme le prétendait Ben Faiza, et si ces mesures étaient conformes à la loi et nécessaires dans une société démocratique[1160]. En ce qui concerne la réquisition des données téléphoniques, la CEDH a jugé que cette mesure constituait une ingérence dans la vie privée, mais conforme à la loi, poursuivant un but légitime, aux fins du démantèlement d'un important réseau de trafic

[1158]Ibidem

[1159]CEDH, *Ben Faiza v Frace*, no.31446/12, 2018.

[1160] Voir ALT Advisory, European Court rules on the use of real-time geolocalion, 2018. https://altadvisory.africa/2018/02/09/european-court-rules-use-surveillance-measures-criminal- proceedings/.

de stupéfiants. S'agissant du grief contre la mesure de géolocalisation, en temps réel, la Cour a relevé qu'à l'époque, la législation française n'offrait pas une protection et des garanties suffisantes contre les abus, et a donc conclu à la violation de l'Article 8 dans l'application de cette mesure[1161].

390. Géolocalisation, interdite sans autorisation judiciaire. En résumé, dans cette affaire, la Cour a statué en faveur de Ben Faiza, estimant que la mesure appliquée sans autorisation judiciaire violait la CEDH, pour les motifs suivants : 1) la violation de l'Article 8 de la Convention Européenne des Droits de l'Homme s'est produite par le biais d'une ingérence dans la vie privée d'une personne au moyen de la géolocalisation, et pour qu'une telle ingérence soit justifiée, elle doit être prévue par la loi, nécessaire et proportionnée au but poursuivi ; 2) la Cour a établi qu'en l'absence d'autorisation judiciaire préalable, la géolocalisation est contraire aux principes fondamentaux garantissant la protection contre l'utilisation abusive des techniques ; et 3) la géolocalisation suit en détail les mouvements et les itinéraires quotidiens d'une personne, exposant ainsi également des détails sensibles de sa vie privée[1162].

391. Enfin, la littérature suggère qu'avec l'avènement des nouvelles technologies de surveillance, l'idée que des problèmes et des risques sociaux majeurs peuvent être résolus par cette technologie a également émergé. Comme l'analysent Kroener et Neyland, mais en parallèle, des risques dans la sphère du respect des droits de l'homme apparaissent et doivent être pris en compte[1163].

C. Violation de la cybersécurité et piratage

a). Définition et classification des atteintes à la cybersécurité

392. Types d'attaques informatiques, types de pirates informatiques. La cybercriminalité est en augmentation au niveau mondial, comme l'indiquent les dernières études.[1164] Une atteinte à la cybersécurité est définie comme l'accès non autorisé, la destruction, la modification ou l'utilisation illégale de données informatiques. Les méthodes de violation de la cybersécurité comprennent le *piratage*, les *ransomwares*, les attaques par *hameçonnage* ainsi que les

[1161] Voir CEDH, *Ben Faiza vs. France,* 2018. *Surveillance measures in drug trafficking investigation.* disponible à l'adresse suivante : http://hudoc.echr.coe.int/eng?i=001-180657.
[1162] Voir D. Lyon, D. *Surveillance studies : An overview*, Polity Press. Chapitre 6, "Privacy and Resistance", 2007. p.120.
[1163] Voir I. Kroener, D. Neyland, *New technologies, security and surveillance*. Dans K. Ball, K. D. Haggerty, D. Lyon (eds.), *Routledge Handbook of Surveillance Studies ,* Routledge, 2012*,* p. 143.
[1164] Voir S. Chng, Lu, H. Y., Kumar, A., & Yau, D. *Hacker types, motivations and strategies : A comprehensive framework*. Computers in Human Behaviour Reports*, 5*, 2022. 100167. https://doi.org/10.1016/j.chbr.2022.100167.

méthodes conçues pour compromettre la confidentialité, l'intégrité ou la disponibilité des systèmes d'information. Selon l'étude citée[1165], comme le nombre et la complexité des cyber-attaques augmentent et se développent continuellement, il est essentiel de connaître les motivations, les typologies et les stratégies des pirates informatiques dans un cadre qui englobe les recherches des 30 dernières années. Ainsi, les résultats de l'étude indiquent les classifications suivantes : par types de pirates informatiques, une taxonomie des motivations derrière les actions et une classification des stratégies d'attaque utilisées. En termes de types de hackers, l'étude identifie 13 catégories (Figure 1), classées selon leur niveau de compétences, leurs intentions et leurs comportements (hackers novices, chapeaux blancs éthiques, hacktivistes, pirates numériques, etc); en termes de motivations des hackers (Figure 2), l'étude identifie 7 motivations spécifiques, curiosité, le gain financier, la notoriété, la vengeance, l'amusement, la motivation idéologique ou sexuelle ; chaque catégorie de hacker a des tactiques spécifiques et des méthodes distinctes (Figure 3) par lesquelles ils appliquent des cyberattaques (attaques de code ou attaques complexes).

Type de hackers	Définition	Noms alternatifs
Novices	Des pirates informatiques mal formés qui s'appuient fortement sur des outils en ligne	Script Kiddies, Newbies
Cyberpunks	Pirates informatiques peu ou moyennement qualifiés créant le chaos pour le plaisir	Crashers, Thugs, Crackers
Insiders	Les employés actuels ou mécontents qui abusent de leur accès pour obtenir ce qu'ils veulent	Internals, User Malcontents, Corporate Raiders
Old Guards (Anciens Gardiens)	Les pirates informatiques qui n'agissent pas pour des raisons malveillantes mais qui ne respectent pas la vie privée.	White Hats, Sneakers, Grey Hats, Tourists

[1165] Ibidem

Professionnels	Pirates informatiques hautement qualifiés agissant pour étendre leur empire criminel ou recrutés pour des cyberattaques	Black Hats, Elites, Criminals, Organized Crime, Information Brokers
Pirates activistes	Les pirates informatiques qui utilisent leurs compétences techniques pour promouvoir des programmes politiques ou provoquer des changements politiques.	Political Activists, Ideologists
Nations statales	Des pirates informatiques hautement qualifiés qui travaillent pour des gouvernements afin de déstabiliser, perturber ou détruire les réseaux d'autres pays.	Information Warriors, Cyber Terrorists, Cyber Warriors, State Actors, State-Sponsored Networks
Étudiants	Les hackers pas malveillants qui piratent uniquement pour acquérir des connaissances	-
Petits voleurs	Les criminels qui exercent leurs activités en ligne en utilisant des compétences faibles ou moyennes	Extortionists, Scammers, Fraudsters, Thieves
Pirates numériques	Les pirates informatiques qui dupliquent, distribuent, téléchargent ou vendent illégalement du matériel protégé par des droits d'auteur.	Copyright Infringers
Infracteurs sexuels en ligne	Des pirates informatiques utilisent l'internet pour se livrer à des comportements	Cyber Predators, Pedophiles

	sexuels déviants à l'égard des enfants	
Collaborateurs (Crowdsourcers)	Les collaborateurs sont des personnes qui se réunissent pour résoudre un problème, souvent en utilisant des méthodes discutables ou en poursuivant des objectifs douteux.	-
Facilitateurs de la criminalité (Crime Facilitators)	Les pirates informatiques qui fournissent les outils et le savoir-faire technique nécessaires aux cybercriminels pour lancer des attaques sophistiquées.	Supporters

Figure 1 Types de pirates informatiques, définitions et noms alternatifs. S. Chng., Lu, H. Y., Kumar, A., Yau, D. (2022) *Hacker types, motivations and strategies: A comprehensive framework.* Computers in Human Behaviour Reports*, 5*, 2022, p.5

Type de hackers	Curiosité	Gain financier	Notoriété	Vengeance	Amusement	Idéologie	Motivation sexuelle
Novices	√	-	√	-	√	-	-
Cyberpunks	-	√	√	√	√	-	-
Insiders	-	√	-	√	-	√	-
Old Guards (Anciens Gardiens)	√	-	√	-	√	√	-
Professionnels	-	√	-	√	-	-	-
Pirates	-	-	√	√	√	√	-
activistes	-	√	-	√	-	√	-
Nations	√	-	-	-	-	-	-
statales	-	√	-	√	-	-	-

Étudiants Petits voleurs	-	√	-	-	-	-	-
Pirates numériques	-	-	-	-	-	-	√
Infracteurs sexuels en ligne	-	-	√	√	√	√	-
Collaborateurs (Crowdsourcers)	-	√	-	-	-	-	-
Facilitateurs de la criminalité (Crime Facilitators)							

Figure 2 Types de pirates informatiques et leurs motivations S. Chng., Lu, H. Y., Kumar, A., Yau, D. (2022) *Hacker types, motivations and strategies : A comprehensive framework.* Computers in Human Behaviour Reports*, 5*, 2022, p.6

Type de hackers	Stratégies
Novices	Réutilisent des codes/scripts/logiciels malveillants trouvés sur l'internet. Ils n'ont pas de plan d'action clair en ce qui concerne les étapes de l'attaque ne sont pas assez prudents pour dissimuler leurs traces en ligne.
Cyberpunks	Ils peuvent utiliser des codes/scripts existants en les modifiant ou écrire leurs propres codes/scripts. Les vecteurs d'attaque comprennent l'endommagement des appareils des victimes, l'exploitation de bogues dans le logiciel et les attaques par déni de service (DoS). Ils cherchent à attirer l'attention du public et des médias.
Insiders	Ils utilisent des connaissances confidentielles sur l'infrastructure cybernétique d'une entreprise pour lancer des attaques ou vendre ces informations. Ils peuvent transférer des données sensibles sur leurs

	propres appareils ou accéder aux bases de données et aux services en nuage de l'entreprise.
Old Guards (Anciens Gardiens)	Ils utilisent des codes/scripts personnalisés ou des outils de test de pénétration pour révéler les vulnérabilités des systèmes existants. Ils découvrent de nouveaux logiciels malveillants à l'aide de honeyspots professionnels et traquent les pirates malveillants grâce à des techniques de cybercriminalité. Ils Incluent les hackers « white hat » et « grey hat ».
Professionnels	Ils effectuent des attaques sophistiquées en utilisant un répertoire complet de vecteurs d'attaque et de codes/scripts personnalisés. Ils veillent à ne pas laisser de traces en ligne.
Pirates activistes	Ils utilisent des vecteurs d'attaque tels que les injections SQL, la mauvaise configuration des serveurs web pour détourner des bases de données, le détournement de sites web de premier plan, la désactivation de services publics, etc.
Nations statales	Elles mènent des attaques sophistiquées en plusieurs étapes : elles accèdent aux réseaux cibles, installent des logiciels malveillants, obtiennent des droits d'administration, identifient et préparent des données précieuses en vue de leur exfiltration, et poursuivent le processus à long terme.
Étudiants	Ils peuvent utiliser des codes/scripts existants, comme les novices, mais en les modifiant pour expérimenter et étudier les vulnérabilités des systèmes. Ils sont susceptibles de signaler les failles.
Petits voleurs	Ils utilisent des vecteurs d'attaque tels que les chevaux de Troie, les ransomwares disponibles en ligne pour obtenir des informations sur les comptes bancaires ou les cartes de crédit.
Pirates numériques	Ils volent directement ou indirectement des contenus protégés par des droits d'auteur et les publient.
Infracteurs sexuels en ligne	Ils se lient d'amitié avec des victimes vulnérables sur les réseaux sociaux et obtiennent des images/vidéos compromettantes par le biais de courriels/chats accompagnés de pièces jointes malveillantes.

Collaborateurs (Crowdsourcers)	Ils unissent leurs forces et leurs compétences pour des tâches telles que le développement de nouveaux logiciels malveillants, la gestion de réseaux de zombies, etc.
Facilitateurs de la criminalité (Crime Facilitators)	Ils fournissent des services de cybercriminalité, aidant les criminels à mener des campagnes de phishing, à louer des logiciels malveillants et des réseaux de zombies, etc.

Figure 3 Stratégies des pirates informatiques S. Chng., Lu, H. Y., Kumar, A., Yau, D. (2022) *Hacker types, motivations and strategies : A comprehensive framework.* Computers in Human Behaviour Reports*, 5*, 2022 p.7)

b). Le piratage devient une méthode invisible d'exercice du pouvoir

393. Les technologies numériques ont inauguré une nouvelle ère dans laquelle les atteintes à la cybersécurité et le piratage informatique sont devenus non seulement des phénomènes courants, mais aussi des outils sophistiqués d'influence géopolitique, économique et sociale. L'article « L'État de surveillance » souligne comment les programmes avancés des agences de renseignement, tels que ceux développés par la NSA, utilisent l'infrastructure numérique mondiale pour accéder aux données personnelles des utilisateurs et surveiller les communications sensibles[1166]. Toutefois, ces capacités s'accompagnent de risques majeurs, car les failles de sécurité créées au nom de la surveillance peuvent être exploitées ultérieurement par des pirates informatiques indépendants ou par d'autres états.

394. Programmes d'interception des données numériques : Upstream. Un exemple notable est le programme Upstream de la NSA, qui intercepte les données directement à partir des fibres optiques reliant les continents. Bien que l'objectif déclaré soit la sécurité nationale, de telles pratiques soulèvent des questions cruciales en matière de protection des données et l'exposition involontaire d'infrastructures mondiales[1167]. Ces vulnérabilités ne sont pas seulement théoriques : une fois créées, elles deviennent des cibles pour les pirates informatiques ou d'autres agences de renseignement qui cherchent à accéder aux mêmes informations. Par exemple, l'infiltration de serveurs ou de systèmes financiers par le biais de réseaux compromis

[1166] B.E Harcourt « 2. *L'État de surveillance* ». *La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.59-76. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-59?lang=fr.Harcourt.
[1167] Ibidem.

s'est avérée avoir des effets dévastateurs, comme en témoignent les attaques à grande échelle contre des entreprises internationales telles que Target ou Neiman Marcus[1168].

395. Le piratage moderne : interception, manipulation, désinformation. En outre, le piratage moderne va au-delà de la simple interception de données pour inclure la manipulation et la désinformation. L'auteur analyse également la manière dont les agences gouvernementales ou les acteurs privés utilisent des méthodes avancées pour influencer le comportement du public, soit en accédant et en distribuant des informations personnelles, soit en manipulant les flux d'informations en ligne[1169]. Le piratage informatique devient ainsi un outil puissant pour créer une instabilité économique ou politique, avec un impact direct sur la confiance des utilisateurs dans la technologie et sur l'intégrité des institutions démocratiques[1170].

396. Minimiser l'impact du piratage. Cette situation complexe appelle à repenser la cybersécurité et les réglementations associées. La législation internationale, ainsi que les cadres nationaux, doivent être adaptés pour prévenir l'utilisation abusive des technologies numériques et assurer un équilibre entre la protection de la vie privée et les besoins en matière de sécurité. En outre, il est essentiel de développer des solutions techniques pour minimiser l'impact du piratage sur les infrastructures critiques telles que les réseaux financiers ou les systèmes de santé. Ces mesures sont non seulement nécessaires pour contrer les menaces actuelles, mais aussi pour rétablir la confiance du public dans le monde numérique, une ressource essentielle dans une société interconnectée.

397. Apparition de la vulnérabilité. L'article « Le Panoptique » fournit un cadre théorique permettant de comprendre ce phénomène, en décrivant comment les architectures de surveillance et de contrôle, conçues à l'origine pour la discipline, peuvent être exploitées pour générer des vulnérabilités[1171]. Dans un contexte numérique, les réseaux et les bases de données deviennent des points sensibles, et des acteurs étatiques ou non étatiques utilisent ces brèches pour accéder à des informations sensibles, les manipuler ou les détruire.

398. Instruments d'influence géopolitique. Le piratage moderne va au-delà du simple accès non autorisé à des informations et comprend des formes d'attaques plus sophistiquées telles que le ramsonware, le phishing avancé et l'exploitation des vulnérabilités critiques de l'infrastructure.[1172] Par exemple, les attaques contre les systèmes financiers mondiaux ou les

[1168]Ibidem.
[1169]Ibidem.
[1170]M. Nkongolo, "*Navigating the complex nexus : cybersecurity in political landscapes*", arXiv, 2023 https://doi.org/10.48550/arXiv.2308.08005.
[1171]G Tusseau, « *Sur le panoptisme de Jeremy Bentham* », Revue Française d'Histoire des Idées Politiques 19, nr. 1, 2004: 3-38, https://doi.org/10.3917/rfhip.019.0003.
[1172] Mitnick Security, "*Common Hacking Techniques in 2023 and Predictions for 2024*", consulté le 27 novembre 2024, https://www.mitnicksecurity.com/blog/common-hacking-techniques-2023.

infrastructures critiques, telles que la santé ou les transports, sont utilisées non seulement à des fins lucratives, mais aussi comme outils d'influence géopolitique. En ce sens, le piratage informatique devient une méthode d'exercice du pouvoir[1173], similaire à la surveillance décrite dans le panoptique de Bentham - un mécanisme par lequel ceux qui contrôlent l'information peuvent contrôler l'ensemble de la structure sociale[1174].

399. Failles de sécurité, incertitude, environnement de méfiance. Au-delà de la dimension technique, le piratage a également de profondes implications sociales et juridiques. Harcourt suggère que la nature invisible du piratage - dans laquelle les victimes ne sont pas toujours conscientes des failles de sécurité - renforce le sentiment d'insécurité cybernétique[1175]. Cette incertitude contribue à un environnement de méfiance, les utilisateurs devenant de plus en plus prudents dans leurs interactions numériques et les entreprises investissant des sommes considérables pour protéger leurs données. Cependant, la législation internationale est à la traîne et le manque de coordination mondiale en matière de cybersécurité permet aux pirates de profiter des lacunes existantes[1176]. Les états doivent non seulement prévenir les attaques, mais aussi réagir de manière éthique et légale lorsqu'ils sont impliqués dans des opérations de piratage offensives[1177].

400. L'effet sur les relations internationales. Un autre aspect critique des atteintes à la cybersécurité est leur effet sur les relations internationales. Les cyber-attaques, souvent utilisées comme arme dans les conflits entre États, sapent non seulement les infrastructures et l'économie, mais créent également des tensions diplomatiques ingérables[1178]. Dans un monde interconnecté où les données sont au cœur du fonctionnement social, le piratage informatique devient une arme qui transforme complètement les règles traditionnelles de la sécurité. Harcourt indique que les solutions futures doivent comprendre à la fois des mesures préventives et des

---

[1173] D&AD "*Harness the Power of Hacking*", consulté le 27 novembre 2024, https://www.dandad.org/en/d- ad-harness-power-hacking-new-blood-advice/.

[1174]G. Tusseau, « *Sur le panoptisme de Jeremy Bentham* », revue française d'historie des idées politiques, nº 19, 2024, p.3-38.

[1175]B.E Harcourt,« *3. Le Panoptique de Jeremy Bentham ». La Société d'exposition Désir et désobéissance à l'ère numérique,* Le Seuil, 2020. p.77-97. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.

[1176] EUR-Lex, *« Cybersécurité des réseaux et des systèmes d'information, 2022 »,* consulté le 27 novembre 2024, https://eur-lex.europa.eu/RO/legal-content/summary/cybersecurity-of-network-and-information- systems-2022.html.

[1177] Gouvernement roumain, Stratégie militaire de la Roumanie du 11 août 2021, Journal officiel, n° 781, 2021. consulté le 27 novembre 2024, https://legislatie.just.ro/Public/DetaliiDocument/245326?

[1178] DefenseRomania Team, « *Le manuel des cybermenaces* – Thales, 2022 ». Tout ce qu'il faut savoir sur la nouvelle vague de menaces invisibles, 2022. https://www.defenseromania.ro/manualul-amenintarilor-cibernetice-thales-2022-tot-ce-trebuie-sa-stiti-despre-noul-val-de-amenintari-invizibile_616697.html.

sanctions mondiales efficaces pour dissuader l'utilisation abusive de la technologie comme outil de contrôle ou de destruction[1179].

401. Le phénomène de l'interconnexion mondiale. Le chapitre « La disparition des frontières entre l'État, l'économie et la société » analyse comment la dissolution des frontières traditionnelles entre l'état, l'économie et la société amplifie les risques associés à la violation de la cybersécurité et au piratage.[1180] Dans un contexte où les données personnelles et l'infrastructure numérique deviennent des éléments centraux du pouvoir et du contrôle, le piratage n'est plus seulement une menace technologique, mais aussi une manifestation des vulnérabilités générées par cette interconnexion mondiale.[1181] Harcourt souligne que les acteurs étatiques et non étatiques utilisent ces violations pour étendre leur influence économique, politique et sociale.[1182]

402. Lacunes normatives en matière de piratage. Le piratage informatique moderne est alimenté par un manque de réglementation efficace et une collaboration opaque entre l'État et les entreprises privées. Le document explore la manière dont l'infrastructure numérique est rendue vulnérable par le besoin d'un accès rapide aux données et l'intégration incontrôlée des technologies émergentes[1183]. Par exemple, les systèmes financiers ou les plateformes de communication deviennent la cible de cyber-attaques, des acteurs malveillants exploitant l'absence de normes de sécurité unifiées pour accéder à des informations sensibles. Ces attaques peuvent aller du vol de données personnelles à la compromission d'infrastructures critiques, avec des effets dévastateurs sur la société et l'économie[1184].

403. L'importance de la notion de responsabilité. Un aspect important souligné dans ce chapitre est la relation entre le piratage informatique et la notion de responsabilité. Dans un écosystème numérique où l'État, l'économie et la société sont interconnectés, il devient

---

[1179] B.E. Harcourt, «3. Le Panoptique de Jeremy Bentham». *La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.77-97. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-77?lang=fr.

[1180] B.E. Harcourt,«*7. La disparition des frontières entre l'État, l'économie et la société». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.163-184. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-163?lang=fr.

[1181] R.Chen, S. Xu, N.Harris, "*Digital infrastructure as essential as power, water, and roads"* | RC Global FM Insights",2021. consulté le 27 novembre 2024, https://rcglobalfm.com.au/insights/digital-infrastructure-as-essential-as-power-water-and-roads.html

[1182] B.E. Harcourt,«*7.La disparition des frontières entre l'État, l'économie et la société ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.163-184. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-163?lang=fr.

[1183]B.E. Harcourt, *La Société d'Exposition: Désir et Désobéissance à l'Ère Numérique.* Le Seuil, 2020. https://shs-cairn-info.docelec.u-bordeaux.fr/la-societe-dexposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page39?lang=fr.

[1184]T.Maurer, A.Nelson, "*The Global Cyber Threat to Financial Systems"*, IMF F&D, 2021. consulté le 27 novembre 2024, https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.

extrêmement difficile d'identifier et de punir les coupables[1185]. Par exemple, le piratage informatique parrainé par un État peut être utilisé comme un outil géopolitique pour déstabiliser d'autres pays ou pour obtenir un avantage économique. Dans le même temps, les entreprises qui collectent et gèrent les données personnelles des utilisateurs peuvent devenir des cibles, et la responsabilité des atteintes à la sécurité est souvent dispersée entre différents acteurscomplique l'application de la loi et l'obtention de réparations[1186].

404. La nécessité d'un cadre réglementaire international. Harcourt suggère que les solutions pour combattre ces menaces doivent être multidimensionnelles. Un cadre juridique international plus strict est nécessaire pour imposer des normes claires en matière de cybersécurité et sanctionner les abus, quelle que soit leur origine. En outre, des technologies plus sûres doivent être développées pour protéger les infrastructures critiques et les données personnelles contre les attaques. Dans le même temps, l'éducation du public sur les bonnes pratiques numériques sont essentielles pour minimiser les vulnérabilités créées par des utilisateurs négligents. Le piratage, tel qu'il est décrit dans ce chapitre, met en évidence non seulement les défis technologiques, mais aussi juridiques et sociaux d'un monde de plus en plus numérisé et interconnecté[1187].

§2. APPROCHE JURIDIQUE DES ATTEINTES À LA CYBERSÉCURITÉ : ANALYSE DES AFFAIRES ET RÉGLEMENTATIONS INTERNATIONALES

405. Un autre cas pertinent de la jurisprudence américaine est United States vs. Morris (1991). Il s'agit du premier procès pénal en vertu de la loi sur la fraude et l'abus informatiques[1188] de 1986. Robert Tappan Morris, étudiant à l'université de Cornell, a été accusé d'avoir lancé un programme informatique de type « worm » (vers) qui a affecté plus de 6.000 ordinateurs connectés à l'Internet en novembre 1988. Les systèmes ont été endommagés et des dégâts importants ont été causés par Morris, qui a créé et distribué le programme dans le but déclaré d'évaluer la taille du réseau d'ordinateurs connectés à l'Internet. Cependant, le code source du programme de Morris était défectueux et le programme s'est répliqué de manière incontrôlée,

[1185] B.E. Harcourt, «*7.La disparition des frontières entre l'État, l'économie et la société ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.163-184. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-163?lang=fr.

[1186] K. Smith, "*Understanding State-Sponsored Cyber Attacks*", Phoenix Software,2024. consulté le 27 novembre 2024, https://www.phoenixs.co.uk/resources/blog/understanding-state-sponsored-cyber-attacks/.

[1187] B.E. Harcourt, *«7. La disparition des frontières entre l'État, l'économie et la société ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.163-184. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-163?lang=fr.

[1188] U.S. Government, *18 U.S. Code 1030 – Fraud and related activity on connection with computers* , Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/1030#.

avec des conséquences importantes sur le système ciblé. Morris a affirmé que son but n'était pas de causer des dommages, mais simplement de mettre en évidence les vulnérabilités des réseaux informatiques. L'affaire a été poursuivie sur la base des informations suivantes concernant l'infraction : Morris a été accusé d'avoir accédé sans autorisation à des systèmes informatiques gouvernementaux et privés en violation de la loi sur la fraude et l'abus informatiques[1189]. Le tribunal a également examiné si les actions de Morris étaient intentionnelles et relevaient de la définition de l'accès non autorisé. Morris a été condamné à 3 ans de mise à l'épreuve sous surveillance, à 400 heures de travaux d'intérêt général et à une amende de 10.050 dollars.

L'affaire United States vs. Morris crée un précédent important dans l'interprétation de la CFAA, en montrant qu'il existe une responsabilité pénale pour l'accès non autorisé à des systèmes informatiques, même en l'absence d'une intention claire de nuire.

406. Le service Yahoo, cible des cyberattaques. Un autre cas de piratage notoire est la violation des données de Yahoo ! (Yahoo Data Breach) (2013-2014), au cours de laquelle le service Yahoo ! a été la cible de cyber-attaquants dont les actions ont eu une grande portée et ont révélé des vulnérabilités importantes dans l'infrastructure de sécurité. Les failles de sécurité ont touché des milliards de comptes et d'utilisateurs, et les attaques de 2013 et 2014 sont considérées comme parmi les pires de l'histoire - elles ont eu un impact significatif sur l'entreprise, tant sur le plan de la réputation que sur le plan commercial, ainsi que sur les utilisateurs.

En août 2013, la cyberattaque a touché les trois milliards de comptes Yahoo ! actifs à l'époque[1190]. Les attaquants ont collecté des données sensibles, y compris les noms complets, les adresses électroniques, numéros de téléphone, dates de naissance, mots de passe cryptés à l'aide d'algorithmes faibles (MD5) et questions et réponses de sécurité, dont certaines étaient stockées en clair. La gravité de cette violation a été amplifiée par le fait que Yahoo ! a admis le problème trois ans plus tard, en 2016. L'entreprise a d'abord affirmé que seuls 500 millions de comptes avaient été compromis, et ce n'est qu'en 2016 qu'elle a reconnu que l'ensemble de sa base d'utilisateurs avait été touchée.

Ce n'était pas le seul incident grave survenu sur Yahoo ! Un an après la première attaque, en 2014, une autre attaque tout aussi importante a touché plus de 500 millions de comptes. Contrairement à l'attaque de 2013, cette violation a été imputée à des pirates soutenus par un gouvernement étranger, qui ont utilisé des techniques sophistiquées pour accéder aux données

[1189] *Ibidem*.

[1190] Voir N. Perlroth, *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, The New York Times, 2016. Accédé à l'adresse suivante : https://www.nytimes.com.

des utilisateurs, aux mots de passe cryptés et aux informations personnelles. Cette attaque a été révélée plus tôt en septembre 2016 et a nécessité une enquête du Bureau Fédéral du Renseignement (FBI)[1191].

L'impact sur Yahoo ! a été important - principalement en termes de crédibilité. La divulgation tardive des faits a remis en cause la transparence de Yahoo ! et sa capacité à gérer correctement les cyberattaques et la sécurité des données personnelles des utilisateurs. En 2017, dans le cadre de son acquisition par Verizon Communications, Yahoo ! a été contraint d'accepter une transaction réduite de 350 millions USD par rapport à sa valeur initiale en raison des risques associés et de l'impact sur la réputation subis à la suite des attaques (Riley et Robertson, 2017)[1192]. L'impact sur les activités de Yahoo ! ne s'est pas arrêté là, mais l'entreprise a également été la cible de plusieurs recours collectifs de la part d'utilisateurs, qui accusaient les services de Yahoo ! de négligence dans la protection de leurs données et de retard dans le signalement des cyberincidents. À la suite du règlement de actions collectives, Yahoo ! a versé 117,5 millions de dollars de dommages et intérêts pour régler les poursuites, ont rapporté les médias (Reuters, 2019)[1193]. Les autorités américaines ont fait savoir qu'elles avaient inculpé quatre personnes, dont deux agents russes du FSB (Service Fédéral de Sécurité de Russie), pour leur rôle dans l'attaque de 2014. Ils ont été inculpés de cyberespionnage, de fraude et d'utilisation abusive de données. Les enquêtes ont révélé l'ampleur et la complexité affaires, mettant en évidence ce que l'on soupçonnait initialement, à savoir que des entités étatiques étrangères dotées de compétences avancées en matière de piratage informatique étaient impliquées dans au moins l'une des attaques. L'affaire Yahoo ! a mis en évidence l'importance de la mise en œuvre de normes élevées en matière de cybersécurité, en particulier pour les entreprises qui traitent d'énormes quantités de données personnelles. Mais l'affaire fait encore aujourd'hui l'objet d'un examen minutieux, car elle montre qu'une mauvaise gestion des incidents peut détruire la confiance des utilisateurs, avec des conséquences financières et juridiques majeures.

A. Vulnérabilités des systèmes d'information mondiaux

407. Cyberattaques récentes. Le piratage de SolarWinds est l'un des cas récents de cyberattaque, qui s'est produit en 2020 et qui présente certaines des caractéristiques les plus

[1191] M. Riley, J. Robertson, *Inside the Billion-Dollar Hack of Yahoo : The Internet Heist That Keeps On Hurting*. Bloomberg, 2017. Accédé à l'adresse suivante : https://www.bloomberg.com.
[1192] *Ibidem*.
[1193] Voir Reuters. *Yahoo data breach settlement gets preliminary approval from U.S. judge*. Reuters, 2019. accédé à l'adresse https://www.reuters.com.

sophistiquées d'une cyberattaque dans l'histoire, impliquant de nombreuses organisations internationales et entreprises privées dans le monde entier. La compromission de la chaîne de fournisseurs SolarWinds, une importante société de logiciels qui fournit des produits de gestion de réseaux informatiques, a eu un effet considérable. Les pirates ont introduit un code malveillant dans une mise à jour de la plateforme Orion, qui est utilisée par plus de 18.000 organisations, dont des agences gouvernementales américaines telles que les départements du Trésor, du Commerce et de l'Énergie, ainsi que d'autres institutions critiques (Constantin, 2020)[1194].

L'attaque a été découverte par la société de cybersécurité FireEye, qui a constaté que les attaquants malveillants avaient un accès non détecté aux réseaux compromis pendant plusieurs mois. Le groupe responsable de l'attaque, surnommé « Cozy Bear » ou APT29, est associé aux services de renseignement russes[1195]. Cet incident a soulevé de sérieuses questions sur la sécurité des chaînes d'approvisionnement et a révélé les vulnérabilités des systèmes d'information mondiaux.

408. Impact juridique. D'un point de vue juridique, l'attaque a conduit à une révision de la législation américaine en matière de cybersécurité, y compris la mise en œuvre du décret sur le renforcement des infrastructures critiques et l'amélioration des procédures de détection et de réponse aux incidents. Elle a également mis l'accent sur la collaboration internationale afin de prévenir des attaques similaires à lavenir. L'affaire SolarWinds reste un exemple alarmant des risques associés à la sécurité numérique dans un monde interconnecté.

a). Kevin Mitnick, le hacker le plus recherché au monde

409. Il convient également de mentionner dans ce chapitre le cas de Kevin Mitnick[1196], l'un des pirates informatiques les plus célèbres de l'histoire. Kevin Mitnick, également connu sous le nom de « The Condor » ou « The World's Most Wanted Hacker », était un pirate informatique américain célèbre pour sa capacité à accéder illégalement à des systèmes informatiques et à des réseaux de télécommunications. Mitnick a fait ses premiers pas à l'adolescence en piratant des réseaux informatiques et a commis divers délits informatiques, y compris l'accès non autorisé aux systèmes de grandes entreprises. Mitnick est né le 6 août 1963 à Los Angeles, en Californie,

[1194] L. Constantin, *SolarWinds attack explained : And why itw as so hard to detect*, CSO, 2020. https://www.csoonline.com/article/570191/solarwinds-supply-chain-attack-explained-why-organisations-were-not-prepared.html.

[1195] EuRepoC. *Advanced Persistent Threat Profile : APT29*, 2023. https://eurepoc.eu/advanced-persistent-threats-apts/

[1196]J.Walsh, *Kevin Mitnick, founder of Mitnick Security*, EBSCO Knowledge Advantage, 2024.. https://www.ebsco.com/research-starters/biography/kevin-mitnick

et s'est intéressé à la technologie et aux communications dès son enfance. Il a commencé à s'intéresser à la technologie et aux communications dès son enfance. Ses premiers délits concernaient le *phone phreaking*, une méthode consistant à manipuler les systèmes téléphoniques pour obtenir des appels gratuits. Plus tard, il s'est lancé dans le piratage de réseaux informatiques, accédant aux systèmes d'entreprises telles que Digital Equipment Corporation (DEC), Nokia, Motorola et Sun Microsystems.

La motivation de Mitnick n'a jamais été financière, mais il s'intéressait plutôt à la technologie et à ses défis, en particulier à l'obtention d'informations sensibles, de codes sources et de logiciels propriétaires. L'ingénierie sociale était l'une des méthodes utilisées par Mitnick pour persuader les gens de lui fournir des données sensibles. Il a été arrêté à plusieurs reprises pour cybercriminalité, notamment dans une affaire impliquant le FBI en 1995, et n'a été appréhendé qu'après un an et demi de recherches. Il a été accusé de vol d'informations sensibles et responsable de millions de dollars de préjudice financier. Il a passé quatre ans en détention et, après sa libération, il est devenu consultant en cybersécurité et a fondé sa propre entreprise, a publié des ouvrages considérés comme des références en matière de cybersécurité - « L'art de la tromperie » et « Ghost in the Wires ». Ces ouvrages sont considérés comme des ressources essentielles pour comprendre la cybersécurité. Kevin Mitnick est décédé le 16 juillet 2023. Il est considéré comme un pionnier dans le domaine de la cybersécurité, et son histoire illustre à la fois les vulnérabilités des systèmes informatiques et la possibilité de transformer les compétences en matière de piratage informatique en un outil constructif.

b). Convention de Budapest sur la cybercriminalité

410. Instruments législatifs de l'UE. En termes de législation contre les cyberattaques, l'Union Européenne a adopté un certain nombre de textes législatifs clés pour renforcer la cybersécurité et la protection des données. La directive NIS (2016/1148)[1197] est un cadre de référence, obligeant les États membres à assurer un niveau élevé de protection des réseaux et systèmes d'information critiques. La directive se concentre sur la prévention et la gestion des cyberincidents, soulignant que la résilience des structures critiques ne peut être accrue que par une bonne coopération entre les États membres.

Parallèlement, le Règlement Général sur la Protection des Données (RGPD) a fixé des normes strictes en matière de sécurité des données, imposant des sanctions sévères en cas de violation.

[1197] Directive (UE) *2016/1148* du Parlament Europeen et du Conseil *concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*, Journal officiel de l'Union européenne, L194, 2016.https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L1148.

Le RGPD souligne l'importance de notifier les incidents de cybersécurité dans les 72 heures, ainsi que la mise en œuvre de mesures préventives appropriées pour protéger les données à caractère personnel.

Au niveau international, la Convention de Budapest sur la cybercriminalité (2001)[1198] reste un instrument législatif central. La Convention fournit un cadre commun pour la criminalisation d'activités illégales telles que l'accès non autorisé à des systèmes informatiques, l'interception illégale de données et l'utilisation abusive d'informations. Elle encourage également la coopération transfrontalière entre les États pour enquêter sur la cybercriminalité et la combattre, soulignant ainsi l'importance d'une collaboration à l'échelle mondiale.

c).Ransomware : taxonomie et impact

411. Le cryptage abusif des données personnelles. Une attaque par ransomware[1199] se définit comme l'utilisation d'un logiciel malveillant (malware) par des cyber-attaquants qui bloquent l'accès des utilisateurs à leurs propres données ou systèmes informatiques en échange du paiement d'une rançon (« ransom », en anglais). Cette attaque fonctionne en chiffrant les données de la victime de l'attaque, qui peut récupérer les informations une fois qu'elle a accès à la clé de chiffrement, et évidemment seulement après avoir payé la rançon. Dans de nombreux cas, cependant, le paiement de la rançon ne garantit pas la récupération des données.

Les attaques ont considérablement évolué, utilisant des tactiques, des techniques et des procédures (TTP) complexes qui maximisent leur impact et génèrent des profits difficilement imaginables il y a quelques années. Pour mettre les choses en perspective, les profits des attaques et de l'extorsion publiés donnent aux attaquants des budgets comparables à ceux d'organisations de cyber-attaques au niveau de l'État, sans compter les profits des attaques qui n'ont pas été rendues publiques.

412. Instruction contre le r*ansomware*. La lutte contre les *ransomwares* nécessite un effort de collaboration mondial entre le secteur privé, les autorités chargées de l'application de la loi et les gouvernements. Microsoft contribue activement au rapport du groupe de travail (Task Force Report)[1200], un cadre complet de propositions d'actions pour lutter contre les *ransomwares*. Microsoft publie également régulièrement un plan de projet avec des conseils

---

[1198] Voir la *Convention du Conseil de l'Europe sur la cybercriminalité*, Budapeste, 2001. https://rm.coe.int/16802fa41f.

[1199] N. Gourav, *The Evolution of Ransomware : Tactics, Techniques, and Mitigation Strategies*, SSRN, 2024.https://ssrn.com/abstract=4881213 ou http://dx.doi.org/10.2139/ssrn.4881213.

[1200] Voir *Microsoft Digital Report* 2024, https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/FY21-Microsoft-Digital-Defense-Report.pdf.

techniques pour aider les organisations à mieux se préparer et à répondre plus efficacement à ces attaques. En outre, l'entreprise participe à l'élaboration d'une publication de l'Institut National pour Standards et Technologie (NIST)[1201] qui conseille les entreprises sur la manière de prévenir les risques d'une telle attaque.

413. Développement de l'écosystème *ransomware*. Le mécanisme utilise, comme décrit dans la littérature, des logiciels malveillants pour chiffrer et exfiltrer des données, qu'il conserve ensuite en échange d'une rançon, généralement demandée en crypto-monnaies. Plutôt que de se contenter de chiffrer les fichiers de la victime et de demander une rançon en échange de la clé de déchiffrement, les attaquants exfiltrent également les données sensibles avant de déployer le *ransomware*. Cette pratique empêche la victime de faire marche arrière dans les négociations et augmente les coûts de réputation pour la victime en cas de non-paiement, car les attaquants peuvent à la fois conserver les données cryptées et divulguer des informations sensibles.

Derrière le déploiement d'un *ransomware*, une série d'activités criminelles se déroulent pour préparer le terrain à l'attaque finale. Dans ce contexte, une taxonomie a été créée pour analyser les relations entre les entités de l'écosystème des *ransomwares*, chaque entité pouvant jouer un rôle différent à un moment donné. Les attaques sont devenues manuelles, également connues sous le nom de « *ransomware* du grand *jeu* ». Ce type d'attaque est très rentable mais peu coûteux, avec un impact dévastateur sur les organisations ciblées, la sécurité nationale, l'économie, la santé publique et la sécurité.

Ce qui était à l'origine simple, affectant un seul ordinateur, a évolué pour inclure des techniques d'extorsion variées, basées sur l'intelligence humaine, ciblant des réseaux d'organisations dans le monde entier. Cette combinaison de renseignements en temps réel et de tactiques criminelles complexes contribue au succès des attaques par ransomware, ce qui en fait une menace majeure pour la cybersécurité mondiale.

414. Attaques transfrontalières à grande échelle. Un exemple pertinent est l'attaque du type WannaCry (2017)[1202], qui a compromis plus de 200.000 ordinateurs dans 150 pays, paralysant des hôpitaux, des banques et d'autres institutions critiques. Cette attaque a démontré la vulnérabilité des infrastructures numériques et la nécessité de prendre des mesures de sécurité proactives.

Les attaques contre les réseaux d'infrastructures critiques sont régulièrement évaluées dans des rapports mondiaux et les dernières données montrent des tendances spécifiques, en particulier

---

[1201] Voir *Small business cybersecuriturity corner : ransomware*, NIST. https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware.

[1202] M. Akbanov, V.G. Vassilakis, M.D. Logothetis, *WannaCry ransomware : Analysis of infection, persistence, recovery prevention and propagation mechanisms*. Journal of Telecommunications and Information Technology, (1), 2019, p.113-124.

après la pandémie COVID-19. Selon un rapport de la société de services de cybersécurité SOPHOS[1203], les attaques contre les infrastructures critiques telles que le pétrole et le gaz, les services financiers ou l'éducation ont augmenté en 2024, et des comportements différents ont été observés dans différents domaines par rapport à 2023. Par exemple, dans le cas des services financiers, 51% de leurs représentants étaient prêts à payer les montants demandés, contre 56% de paiements au niveau mondial dans différentes industries[1204].

Principales caractéristiques du ransomware :

- Chiffrement des données : les fichiers des victimes sont chiffrés à l'aide d'algorithmes de chiffrement avancés.
- Demande de rançon : les attaquants exigent généralement un paiement en crypto-monnaies en échange de l'anonymat.
- Tactiques d'intimidation : les attaquants menacent parfois de publier les données volées si la rançon n'est pas payée (par exemple, le ransomware de double extorsion).

415. Cryptage, vol de données, rançon. Le modèle commercial de la « double extorsion » se retrouve dans Conti Ransomware[1205], en 2020, où la victime est d'abord extorquée pour obtenir une rançon et menacée de publier les données volées. Conti fonctionne également sur la base d'un abonnement en tant que service As A Service (RaaS), qui permet aux affiliés d'accéder directement à la création d'outils de ransomware. Ceux qui accèdent à ce service acceptent de percevoir un pourcentage de la rançon demandée par l'attaquant et la victime. Conti accède aux réseaux des victimes par le biais d'autres cybermenaces telles que Trickbot, IcedID ou Zloader. Une fois qu'il a accédé au réseau de la victime, Conti utilise un module de reconnaissance pour scanner le réseau à la recherche d'informations précieuses. Celles-ci sont ensuite chiffrées et, à la fin du processus, le système applique une « note de rançon » dans chaque répertoire affecté, avec des instructions sur la manière de contacter initiateurs de l'attaque.

B. Technologies de reconnaissance et d'authentification biométriques

416. Authentification par reconnaissance faciale. Les technologies biométriques, en particulier les technologies de reconnaissance faciale, sont de plus en plus utilisées dans un

[1203]P. Mahendu, *The State of Ransomware in Education*, Sophos, 2024.https://news.sophos.com/en-us/2024/07/11/the-state-of-ransomware-in-education-2024/.
[1204]P. Mahendu, *The State of Ransomware in Financial Services* , Sophos, 2024. https://news.sophos.com/en-us/2024/06/24/the-state-of-ransomware-in-financial-services-2024/.

[1205] Voir *Microsoft Digital Defence Report*, 2024. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft- brand/documents/FY21-Microsoft-Digital-Defense-Report.pdf, p. 15.

large éventail de domaines tels que la sécurité publique, le secteur privé et l'administration de la justice. Les technologies biométriques, y compris la reconnaissance faciale, sont un outil très important dans la gestion de l'identité personnelle et de l'authentification et sont utilisées dans une grande variété de contextes multiples tels que la sécurité nationale, l'accès aux services publics ou les applications commerciales. Les systèmes d'identification biométrique reposent sur l'analyse de caractéristiques uniques des individus[1206] - empreintes digitales, structure et géométrie du visage ou spécificité de l'iris - et sont présentés comme des solutions efficaces et rapides pour l'identification et la vérification des individus[1207]. Toutefois, à mesure que ces technologies deviennent de plus en plus répandues, d'importantes questions relatives à la vie privée, à l'utilisation éthique des données et aux droits de l'homme fondamentaux se posent également[1208].

417. Situation législative. D'un point de vue juridique, l'utilisation des données biométriques est strictement réglementée, en particulier dans les juridictions qui adoptent des normes élevées en matière de protection des données.

Au niveau international, la Convention 108[1209] du Conseil de l'Europe étend la protection des données biométriques, en exigeant des analyses d'impact et des mesures techniques robustes.

Au sein de l'Union Européenne, le Règlement Général sur la Protection des Données (RGPD)[1210] définit les données biométriques comme des « catégories particulières » de données qui nécessitent un niveau de protection élevé. Selon l'Article 9 du RGPD[1211], le traitement de ce type de données n'est autorisé que dans des conditions strictes, telles que le consentement explicite de la personne concernée ou l'existence de motifs d'intérêt public.

(1) Le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques permettant l'identification unique d'une personne physique, des données relatives à la santé ou à la vie sexuelle ou à l'orientation sexuelle d'une personne physique sont interdits.[1212]

[1206]S. Kloppenburg, I van der Ploeg, *Security Identities: Biometric Technologies and the Enactment of Human Bodily Differences*, Science as Culture, 2020, p.57-76.
[1207]A.Jain, A.Ross, S.Prabhakar, *An Introduction to Biometric Recognition*, IEEE Xplore, 2004.
[1208]A. North-Samardzic. *Biometric Technology and Ethics: Beyond Security Applications*. Journal of Business Ethics vol.167, no. 3, 2020. http://www.jstor.org/stable/45386904.
[1209]Voir Conseil de l'Europe Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), connue sous le nom de Convention n° 108, ANS PDCP, 2018.https://www.dataprotection.ro/?page=europa_council&lang=ro.
[1210]Voir Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[1211]Voir la Loi GDPR 2025 mise à jour. https://www.legeagdpr.ro/titlu-1/capitol-2/articol-9.html.
[1212]Ibidem.

a). Données biométriques, zone grise aux États-Unis

418. Aux États-Unis, par comparaison, la réglementation de l'utilisation des données biométriques n'est pas uniforme, mais il existe des exemples de législation dans certains États qui traitent de l'utilisation éthique des données biométriques. Le California Privacy Rights Act (CPRA)[1213] est un exemple de ce type de législation, mais l'absence de réglementation fédérale unitaire crée des « zones grises » qui peuvent affecter la protection des personnes[1214].

419. **Le concept d'intégrité contextuelle**. Les technologies de collecte et de stockage des données biométriques soulèvent des questions fondamentales en matière d'autonomie individuelle et de respect de la vie privée. Le concept d'« intégrité contextuelle », développé par Helen Nissenbaum[1215], souligne l'importance du respect des normes sociales et contextuelles dans le traitement des informations personnelles. Ce cadre (*framework*) suggère que toute utilisation de données biométriques doit être évaluée non seulement en termes de légalité, mais aussi en termes de respect des normes morales et sociales qui régissent les relations entre les individus et les institutions[1216].

b). La reconnaissance faciale augmente la sécurité dans l'espace public

420. Il ne fait aucun doute que les progrès technologiques et la mise en œuvre de techniques biométriques présentent d'importants avantages pour la société, mais ils comportent également des risques significatifs concernant la protection des droits de l'homme. D'une part, la technologie biométrique contribue grandement à renforcer la sécurité dans l'espace public en identifiant rapidement les suspects, ce qui permet d'éviter les fraudes.

421. **Risque pour les droits fondamentaux**. D'autre part, l'utilisation de la technologie biométrique sans le consentement explicite des personnes et d'une manière disproportionnée par rapport à l'objectif visé peut conduire à des violations des droits de l'homme fondamentaux. Les failles de sécurité dans les systèmes de stockage des données biométriques constituent un risque majeur à cet égard. De même, l'utilisation excessive des données biométriques à des fins

---

[1213]Le California Privacy Rights Act , 2020. voir https://thecpra.org.
[1214]H.Nissenbaum, „*Privacy in Context, Technology, Policy and the Integrity of Social Life*", Standford University Press, 2010.
[1215] M.A. Paveau, *Intégrité contextuelle*. Technologies discursives*, 2015, p.129.*
[1216] H.Nissenbaum, „*Privacy in Context, Technology, Policy and the Integrity of Social Life*", Standford University Press, 2010, p 131.

de surveillance excessive de la population peut conduire à une transformation sociétale similaire au concept de « panoptique » introduit par Foucault à l'aide du biopouvoir.

c). Les aéroports annoncent l'exclusion de l'identification des passagers sur la base de documents

422. L'identification biométrique, accueillie avec enthousiasme. La reconnaissance faciale est importante dans le secteur des transports car elle peut être utilisée pour vérifier rapidement l'identité des passagers, ce qui permet de gagner du temps et d'améliorer la sécurité. De nombreux grands aéroports du monde ont déjà fait part de leur intention d'éliminer complètement l'utilisation de documents traditionnels pour l'identification. La dernière annonce[1217] de l'intégration complète de la biométrie pour l'identification des passagers vient des Aéroports d'Abu Dhabi, qui ont lancé le projet Smart Travel[1218], un programme qui s'appuiera uniquement sur la biométrie, c'est-à-dire la reconnaissance de l'iris et du visage, pour l'identification.

Selon des enquêtes en novembre 2024 par International Air Transport Association (IATA)[1219] le nombre de passagers qui ne souhaitent plus s'enregistrer dans les aéroports avec des documents traditionnels mais uniquement avec une identification biométrique ne cesse d'augmenter, 76% des personnes interrogées préférant cette nouvelle méthode[1220]. L'enquête menée auprès de plus de 10 000 passagers dans 2 000 pays montre également que plus de 46% des voyageurs ont déjà utilisé l'identification biométrique et que 84% d'entre eux se sont déclarés satisfaits. La même enquête montre que 50% des passagers sont préoccupés par la manière dont les données privées sont traitées et protégées[1221].

[1217] Abu Dhabi Media Office, *Abu Dhabi Airports and ICP partner to launch the world's first-of-its-kind Smart Travel project, 2024.*. https://www.mediaoffice.abudhabi/en/transport/abu-dhabi-airports-and-icp-partner-to-launch-the-worlds-first-of-its-kind-smart-travel-project/

[1218] Il s'agit d'un programme qui a signé un partenariat avec l'Autorité Fédérale pour l'Identité, la Citoyenneté, les Douanes et la Sécurité Portuaire des Émirats Arabes Unis afin d'utiliser l'intelligence artificielle pour authentifier de manière biométrique tous les passagers utilisant les services aéroportuaires. « Grâce à la mise en œuvre de ce projet, Abu Dhabi Airports vise à maintenir les protocoles de sécurité et de sûreté aérienne les plus élevés à l'aéroport, à améliorer l'expérience des voyageurs et à simplifier le processus de voyage pour les passagers », indique le communiqué officiel. L'objectif est d'éliminer complètement l'interaction directe avec le personnel de l'aéroport. Une première collecte de données biométriques est en cours, après quoi l'authentification se fera automatiquement. Les représentants de l'institution ont annoncé que le plan pour l'avenir proche est de devenir le premier aéroport au monde à disposer d'une identification entièrement biométrique.

[1219] Il s'agit d'une association professionnelle d'opérateurs de transport aérien, représentant environ 80% du marché total, avec plus de 340 entreprises enregistrées.

[1220]IATA Knowledge Hub, *Key Trends in Passenger Behavior: Insights from the IATA Global Passenger Survey* 2024 https://www.iata.org/en/publications/newsletters/iata-knowledge-hub/key-trends-in-passenger-behavior/

[1221] « Cette préférence pour la biométrie permet aux compagnies aériennes et aux exploitants d'aéroports de simplifier les voyages, à condition d'avoir des garanties de confidentialité. Les solutions biométriques soutenues par la

423. L'Europe, prudente face aux nouvelles technologies. En ce qui concerne l'intégration des nouvelles technologies d'identification biométrique dans le comportement des passagers par territoire, l'Europe semble être la plus prudente, l'adoption et la confiance dans la biométrie étant plutôt faibles. L'Asie-Pacifique est à la pointe de l'intégration de l'identification biométrique dans les aéroports, en Afrique le potentiel des nouvelles technologies n'est pas exploité (les passagers n'utilisent pas encore suffisamment les applications de réservation, préférant les agences de voyage classiques), et en Amérique du Nord l'ouverture au partage des données privées provient du besoin de commodité et de rapidité des procédures. La reconnaissance faciale ou de l'iris a déjà été mise en œuvre dans plusieurs aéroports à travers le monde, et l'objectif est que le processus soit entièrement achevé dans un avenir proche, étant donné que le nombre de passagers doublera d'ici 2041[1222]. Le visa, le passeport, la réservation, le billet électronique et l'e-ticket seront stockés dans un simple portefeuille numérique, accessible grâce à l'identification biométrique.

424. Singapour, leader en matière de mise en œuvre. L'aéroport de Singapour est à la pointe de la mise en œuvre de cette technologie. Selon un communiqué de presse daté du 24 octobre 2024, il est le premier au monde à disposer d'une reconnaissance biométrique entièrement intégrée, sans qu'il soit nécessaire d'avoir un passeport traditionnel pour autoriser le voyage. Les procédures d'identification ne prennent que 10 secondes et l'ensemble du processus est relié aux bases de données gouvernementales. De cette manière, l'État s'immisce également dans la vie privée des voyageurs d'une manière moins visible.

d). Critiques de l'utilisation par le gouvernement chinois de la reconnaissance faciale

425. Technologie biométrique, mécanisme de surveillance. Le système de surveillance chinois basé sur la reconnaissance faciale[1223] est un exemple éloquent de l'utilisation extensive des technologies biométriques. Le gouvernement chinois a été fortement critiqué pour la mise en œuvre de ce système qui, selon les organisations de défense des droits de l'homme, intègre des millions de caméras de surveillance avec des logiciels avancés pour surveiller les citoyens en temps réel, mais aussi pour établir le profil d'une des populations minoritaires de Chine, les

protection des données peuvent améliorer l'expérience tout en répondant aux préoccupations des passagers en matière de respect de la vie privée ».

[1222]IATA, *One ID for a Seamless & Contactless Passenger Journey* https://www.iata.org/en/programs/passenger/one-id/.

[1223]Voir New York Times, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority, 2019.* https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial- profiling.html

Ouïgours[1224]. Les autorités chinoises affirment que ces technologies sont indispensables au maintien de l'ordre public et à la lutte contre la criminalité. Cet exemple met en évidence le risque que les technologies avancées soient utilisées non seulement pour la sécurité, mais aussi comme outil de contrôle social, mettant ainsi en péril la liberté et la dignité humaines.[12251226].

426. Avantages et risques. Selon un rapport du Biometric Research Group (2021)[1227], le marché mondial des technologies biométriques a été évalué à plus de 40 milliards de dollars, avec une croissance annuelle significative due au déploiement dans les secteurs public et privé. En résumé, les technologies biométriques présentent des avantages, mais aussi des risques, notamment une sécurité accrue et une meilleure efficacité de l'authentification dans les systèmes complexes, mais aussi des risques pour la sécurité, car les atteintes à la sécurité sont irréversibles, les caractéristiques personnelles ne pouvant être modifiées de la même manière que les mots de passe, et l'absence de consentement explicite est problématique et fréquente.

427. Jurisprudences notables. L'une des affaires les plus médiatisées soumises aux juges de la CEDH est l'affaire Lopez Ribalda vs. Espagne (2019), dans laquelle cinq employés licenciés d'une entreprise espagnole ont affirmé que les enregistrements vidéo de sécurité violaient leur droit à la vie privée en vertu de l'Article 8 de la Convention Européenne des Droits de l'Homme. Les tribunaux nationaux et la CEDH ont statué que, bien que l'employeur ait le droit de se protéger au moyen d'enregistrements vidéo de sécurité, en l'absence de notification préalable, le droit à la vie privée est violé. Cette affaire illustre la nécessité de respecter la proportionnalité et l'intérêt légitime dans l'application de la vidéosurveillance.

Une autre étude de cas des États-Unis, Patel et al vs. Facebook (2020)[1228], a abouti à un montant record de 650 millions de dollars de dommages et intérêts pour les plaignants dans une affaire concernant l'utilisation d'une technologie biométrique de reconnaissance faciale sans le consentement de l'utilisateur. Le tribunal a statué en faveur des plaignants, admettant que le réseau social avait violé le Biometric Information Privacy Act (BIPA) de l'Illinois[1229].

[1224] Human Rights Watch *Chine: Collecte de l'ADN de millions d'habitants du Xinjiang, 2017.* Voir https://www.hrw.org/news/2017/12/13/china-minority-region-collects-dna-millions.

[1225] Marx et al., *Marx and Engels Anthology*. vol.5, People's Publishing House, 2004.

[1226] J. Q. Quach et al*., Superabsorption in an organic microcavity: Toward a quantum battery.* Sci. Adv**.**, 2022.

[1227] Voir Global Biometrics Market Report 2021: *Market to Reach $44.1 Billion by 2026 - Increasing Significance of Biometrics Technology in Facilitating Contactless Passenger Journey Post-COVID-19 Pandemic*, Research and Markets*, 2021.*

[1228] M.Rotenberg, A.Butler, J.Davissom, *Brief of Amicus Curiae electronic privacy information center (EPIC)in suport of plaintiffs-appellees*, EPIC 2018. https://epic.org/wp-content/uploads/amicus/bipa/patel-v-facebook/Patel-v-FB-9th-Cir- Opinion.pdf

[1229] R.Pester *Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit,* Harvard Law School, 2020.https://jolt.law.harvard.edu/digest/patel-v-facebook-facebook-settles-illinois-biometric-information-privacy-act-bipa-violation-suit

e). Technologies de reconnaissance faciale et acceptation de la surveillance

428. Surveillance invasive, mais invisible. La reconnaissance faciale et les technologies biométriques sont devenues des symboles du pouvoir de la surveillance moderne, transformant chaque interaction numérique ou physique en une opportunité de surveillance et de contrôle. Le chapitre « Notre pavillon en verre-miroir » de Bernard E. Harcourt offre une perspective critique sur ces technologies, soulignant comment elles étendent l'architecture de la surveillance à une forme plus invasive, mais presque invisible[1230]. Alors que dans le passé, la surveillance était associée à la présence manifeste de caméras ou d'autres dispositifs, les technologies biométriques apportent une nouvelle dimension : la capacité d'identifier et de suivre les individus sans leur consentement ou sans qu'ils en soient conscients.

429. Programme Optic Nerve. Un exemple pertinent est le programme Optic Nerve, développé par des agences gouvernementales, qui a utilisé des caméras sur des plateformes telles que Yahoo pour collecter des images faciales d'utilisateurs à leur insu[1231]. Ce type d'utilisation des technologies biométriques va au-delà de la simple collecte de données, devenant une forme de surveillance systémique qui peut éroder la confiance des utilisateurs dans les plateformes numériques. En outre, ces technologies ne se limitent pas à l'identification, mais sont intégrées dans divers contextes, de la sécurité nationale au marketing personnalisé, créant un environnement dans lequel chaque expression faciale ou caractéristique biométrique devient un outil exploitable[1232].

Les conséquences sociales et juridiques de ces technologies sont considérables. Dans une « société d'exposition », comme la décrit Harcourt, les utilisateurs intériorisent l'idée qu'ils sont constamment surveillés et finissent par l'accepter comme la norme[1233]. Par exemple, les systèmes de reconnaissance faciale déployés dans les espaces publics, tels que les aéroports ou les stations de métro, sont présentés comme des mesures de sécurité. Cependant, ils soulèvent de sérieuses questions éthiques et juridiques, en particulier en l'absence d'un cadre juridique clair pour empêcher l'utilisation abusive des données biométriques. Le document souligne qu'une fois collectées, ces données sont presque impossibles à protéger de manière absolue, et

---

[1230]B.E. Harcourt, « *4. Notre pavillon en verre-miroir ». La Société d'exposition Désir et désobéissance à l'ère numérique,* Le Seuil, 2020. p.101-124. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-101?lang=fr.

[1231] Ibidem.

[1232]A. Spencer, J. Ball, "*Optic Nerve : Millions of Yahoo Webcam Images Intercepted by GCHQ*", The Guardian, 2014. https://www.theguardian.com/world/2014/feb/27/gchq-nsa- webcam-images-internet-yahoo.

[1233]B.E. Harcourt. «*4. Notre pavillon en verre-miroir ». La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p.101-124. CAIRN.INFO, shs.cairn.info/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-101?lang=fr.

que les utilisations ultérieures - que ce soit par les gouvernements ou les entreprises - peuvent être difficiles à contrôler[1234].

f). Nécessité de réglementer les technologies biométriques

430. Atteinte aux droits fondamentaux. Un autre aspect critique est le potentiel discriminatoire de ces technologies. Les algorithmes qui sous-tendent la reconnaissance faciale sont souvent biaisés, avec des taux d'erreur plus élevés pour certains groupes ethniques ou de sexe. Non seulement cela affecte les individus marginalisés, mais cela amplifie les inégalités sociales et soulève des questions sur l'éthique de l'utilisation de ces systèmes. Le document suggère que l'intégration des technologies biométriques dans la vie quotidienne crée une dynamique dans laquelle les droits fondamentaux des utilisateurs sont sapés sous couvert de sécurité ou d'efficacité[1235].

Dans un tel contexte, une réglementation claire et complète de l'utilisation des technologies biométriques devient essentielle. Celles-ci ne doivent pas être considérées comme une simple avancée technologique, mais comme un élément qui transforme la relation entre les individus, les institutions et la vie privée. Protéger les données biométriques et imposer des limites strictes à leur utilisation sont des impératifs non seulement juridiques mais aussi sociaux pour éviter que la vie privée ne devienne une simple marchandise à exploiter dans un monde hypertechnologisé.

g). Éthique et avenir de la biométrie

431. Protection de la confidentialité, prévention des abus. L'utilisation de la biométrie nécessite une approche éthique qui protège la vie privée et prévient les abus. Il est essentiel que les pays mettent en œuvre des règles claires pour une utilisation responsable technologies biométriques :

- Garantir le consentement éclairé.
- Limiter les finalités pour lesquelles les données biométriques peuvent être utilisées.
- Mettre en œuvre des mécanismes de vérification indépendante de l'utilisation.

Les technologies de reconnaissance faciale et de biométrie sont des outils au potentiel énorme, mais leur utilisation doit être encadrée par des principes clairs qui assurent la protection des

[1234] Ibidem.
[1235] *Ibidem*.

droits fondamentaux. Il est impératif que la réglementation juridique suive le rythme des progrès technologiques et que la transparence dans l'utilisation de ces technologies devienne une priorité. En outre, le dialogue entre juristes, ingénieurs, politiciens et représentants de la société civile est essentiel pour construire un cadre équitable et durable dans lequel les avantages des technologies biométriques sont maximisés sans compromettre les libertés individuelles.

C.Dispositifs IoT (Internet of Things) et collecte de données personnelles

432. Dispositifs interconnectés. L'internet des objets (IdO) est défini comme un réseau mondial de dispositifs physiques interconnectés via l'internet[1236] qui peuvent collecter et transmettre des données en temps réel. Aujourd'hui, ces dispositifs sont de plusieurs types, allant des téléphones intelligents aux montres de fitness, en passant par les trackers de fitness, les appareils ménagers intelligents ou les systèmes de caméras de sécurité à domicile. Tous ces appareils sont devenus des éléments indispensables de la vie moderne. Le fait même que tous ces appareils soient connectés à l'internet et interconnectés génère un volume et un trafic considérables de données personnelles, dont la protection soulève des questions juridiques complexes en termes de respect de la vie privée et de sécurité des données[1237].

Des rapports technologiques récents estiment que d'ici 2025, le nombre de dispositifs IdO dépassera les 75 milliards dans le monde[1238]. Cette avancée technologique rapide nécessite une réévaluation du cadre réglementaire existant, en particulier en ce qui concerne la protection des données et de la vie privée. L'IdO ne se contente donc pas d'amplifier les risques de sécurité, mais crée également de nouveaux défis juridiques liés à la responsabilité des opérateurs et aux droits des utilisateurs. La croissance exponentielle du nombre d'appareils et d'utilisateurs entraîne la nécessité d'une réglementation équitable en faveur de la vie privée et des données sensibles des utilisateurs.

433. Collecte d'informations. Les appareils IoT sont conçus pour collecter un large éventail d'informations sur les utilisateurs, notamment :

- Données de localisation - tout appareil doté d'un GPS peut suivre la personne en temps

[1236]S.Greengard, *Internet of Things*, Article History, Britannica, 2024.https://www.britannica.com/science/Internet-of-Things

[1237]Voir Gartner, *Internet of Things: Unlocking True Digital Business Potential* https://www.gartner.com/en/information-technology/insights/internet-of-things**.**

[1238] T. Alam, *A Reliable Communication Framework and Its Use in Internet of Things (IoT*), International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2018*. Disponible à l'adresse : https://www.researchgate.net/publication/325645304.

réel.

- Données biométriques - les dispositifs de

surveillance de la santé physique, tels que les montres de fitness et autres dispositifs similaires, recueillent une multitude de données sur la santé, telles que la fréquence cardiaque, la qualité du sommeil, le niveau d'activité physique, les paramètres de santé mentale, etc.

- Données sur le comportement de consommation - les appareils domestiques intelligents enregistrent et transmettent sur l'internet des informations sur les préférences et les habitudes de l'utilisateur.

434. Cibles des cyberattaques. Les risques associés à la collecte de ces données sont importants. Les dispositifs IoT sont fréquemment la cible de cyberattaques, et nombre d'entre eux sont vulnérables en raison de l'absence de normes de sécurité solides. En octobre 2021, un tribunal britannique[1239] a statué dans l'affaire Fairhurst vs. Woodard[1240], dans laquelle l'utilisation d'une sonnette intelligente dotée d'une fonction vidéo a été jugée contraire aux droits à la vie privée et à la protection des données d'un voisin dont la maison se trouvait dans la ligne de mire de l'enregistrement. Jon Woodard, le défendeur dans cette affaire, avait installé plusieurs dispositifs de surveillance, dont une sonnette vidéo Ring et des caméras placées autour de sa propriété. Ces dispositifs capturaient des images vidéo et audio, dépassant les limites de sa propriété et enregistrant des activités et des conversations dans l'espace public ou sur la propriété de son voisin. La technologie audio de la sonnette pouvait enregistrer des conversations jusqu'à une distance de 12 mètres, ce qui a été jugé excessif par rapport à l'objectif déclaré de prévention de la criminalité. Le tribunal a jugé que ces actions enfreignaient la loi britannique sur la protection des données et le règlement général sur la protection des données (RGPD) de l'Union Européenne. Dans ce cas, le tribunal a également recommandé de désactiver la fonction d'enregistrement audio si elle n'est pas nécessaire et de mettre en place des zones de détection du mouvement à l'exclusion de la zone située à l'extérieur de la propriété de l'utilisateur.

L'affaire Fairhurst contre Woodard montre que la responsabilité des utilisateurs d'équipements de surveillance s'inscrit dans le cadre d'une utilisation légale et éthique visant à protéger la vie privée des individus. Cette affaire constitue un précédent important pour la réglementation de l'utilisation des dispositifs de surveillance intelligents dans l'espace public[1241].

[1239]Voir *Case Fairhurts v Woodard*, in The County Court at Oxford, 2021. https://www.judiciary.uk/judgments/fairhurst-v-woodard/.

[1240]C. Wong, *Use of a ring doorbell found to be in breach of data protection laws*, HJA, 2021. https://www.hja.net/expert-comments/opinion/dispute-resolution-for-individuals/use-of-a-ring- doorbell-found-to-be-in-breach-of-data-protection-laws/.

[1241]Voir Conosco, *IoT Security Breaches: 4 Real-World Examples*, 2021.https://conosco.com/industry-insights/blog/iot-security-breaches-4-real-world-examples.

Smart Thermostat Breach (2019)[1242] est une autre étude de cas qui a démontré la vulnérabilité des dispositifs intelligents de contrôle de la température ambiante connectés au réseau WiFi domestique. L'affaire s'est déroulée dans la résidence d'un couple à Milwakee, aux États-Unis, en 2019, lorsqu'un attaquant inconnu a pris le contrôle des appareils intelligents de la maison après que la famille a installé un système complexe Nest avec une caméra, un thermostat et une sonnette. Le cyber-attaquant a pris le contrôle du système vidéo de la maison et a joué de la musique au volume maximum, a parlé au couple à travers le système de sonorisation et a manipulé la température à travers le thermostat jusqu'à plus de 30 degrés Celsius à l'intérieur. Cette violation a mis en évidence les faiblesses de la sécurité de l'IdO et la nécessité de normes plus rigoureuses, que les fabricants d'appareils intelligents ont déjà commencé à mettre en œuvre avec l'authentification à deux facteurs.

435. Privacy by Design.[1243] La collecte et le traitement des données personnelles par les dispositifs IoT sont régis par plusieurs lois, notamment le Règlement Général sur la Protection des Données (RGPD) qui, comme indiqué ci-dessus, énonce des principes stricts pour le traitement des données personnelles, avec l'exigence d'un consentement explicite au traitement, un droit d'accès et le droit de demander l'effacement des données à tout moment. Conformément à l'Article 25 du GDPR, le concept de "Privacy by Design" est imposé pour la conception des technologies IoT par la Directive NIS relative à des mesures visant à assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union[1244].

En même temps, comme la technologie évolue, le cadre réglementaire doit être constamment mis à jour à la lumière des nouveaux défis, tout en respectant les concepts clés. L'une des mesures clés de la mise à jour de la réglementation est le concept de "Privacy by Design", qui fait référence à l'exigence d'intégrer des mesures de protection des données dans les appareils dès la phase de développement ; les exigences de cryptage doivent s'appliquer à toutes les données transmises via l'IdO, afin de fournir une protection maximale contre l'accès non autorisé ; et le public doit être continuellement formé et informé des risques associés à l'utilisation des appareils IdO et de ses droits en matière de protection des données.

Conclusions du chapitre 2

Le chapitre 2 met en évidence le passage d'une définition abstraite de la vie privée à une analyse concrète des modes d'ingérence générés par les évolutions numériques. Le fil

[1242]Voir Cisomag, *Hackers take over Smart Home*, 2019 https://cisomag.com/hackers-take-over-smart-home/
[1243] C. Zolynski, *Privacy by Design Et Big Data*, Academia.edu, 2016.
[1244]*Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union*

conducteur est l'idée que la surveillance continue – réalisée à l'aide de technologies, de plateformes et d'infrastructures invisibles – ne produit pas seulement des atteintes ponctuelles à la vie privée, mais aussi un processus d'autocontrôle et de discipline de l'individu, qui modifie ses comportements en sachant (ou en devinant) qu'il est constamment suivi, profilé, évalué.

L'analyse du rôle de l'intelligence artificielle, du passage du Web 2.0 au Web 3.0, de l'internet des personnes et de l'internet des objets met en évidence la fragmentation de la personne en un ensemble de données interconnectées. Le concept d'*Homo numericus* exprime cette mutation identitaire : l'individu devient un sujet juridique hybride, présent à la fois dans l'espace physique et dans l'espace numérique, et sa vie privée est exposée par la connectivité, les appareils, les capteurs et les interfaces quotidiennes. Le chapitre souligne ainsi que la protection de la vie privée ne peut plus ignorer cette double existence.

La section consacrée à la sécurité des données et à la sensibilisation à la protection de la vie privée montre que les technologies émergentes génèrent un double rapport de forces : d'une part, l'imaginaire « Big Brother » et les nouvelles formes de surveillance, y compris la collaboration entre les géants informatiques et les autorités ; d'autre part, la participation volontaire des utilisateurs motivée par le besoin de visibilité, d'interaction et de récompense sociale. Les références à la biométrie, à la *blockchain*, aux réseaux sociaux, aux techniques de *phishing*, de *scamming*, de *spoofing*, de fraude publicitaire et de cyberharcèlement brossent un tableau cohérent des risques qui touchent directement l'identité numérique, la confidentialité et l'intégrité des données.

La deuxième partie du chapitre approfondit la dimension juridique de ces ingérences, en analysant l'interception illégale des communications, la surveillance non autorisée et la géolocalisation, ainsi que la violation de la sécurité informatique et le piratage. La présentation des éléments constitutifs des infractions, des interventions jurisprudentielles pertinentes, des vulnérabilités des systèmes d'information et des instruments normatifs (y compris la Convention de Budapest) montre que la cybersécurité devient un critère central de la protection de la vie privée.

Dans l'ensemble, le chapitre 2 offre une vision structurée des ingérences contemporaines : de la surveillance diffuse aux attaques informatiques, de la manipulation de l'identité numérique à l'utilisation des données biométriques et des objets connectés. La conclusion implicite est que la protection de la vie privée dans un environnement numérique suppose une articulation rigoureuse des normes pénales et de sécurité avec la réalité technologique décrite dans ce chapitre, sans perdre de vue la centralité de la personne face aux nouvelles formes de pouvoir technologique.

Conclusions du titre 1

Le titre I établit un fondement cohérent pour la protection juridique de la vie privée, en articulant sa dimension conceptuelle et axiologique (Chapitre 1) avec l'analyse des formes contemporaines d'ingérence générées par les évolutions numériques (Chapitre 2). De cette double perspective découle une conclusion essentielle : la vie privée ne peut plus être comprise comme une notion strictement philosophique, ni comme une simple catégorie juridique fixe, mais comme un droit fondamental soumis à une reconfiguration permanente sous l'impact de la technologie. Concrètement, la protection de la vie privée nécessite une articulation constante entre conceptualisation, technologie et normativité juridique.

Le titre I ne se limite pas à une description des transformations technologiques, mais formule le fondement juridique de la protection de la vie privée à l'ère numérique : il identifie les valeurs protégées, précise les principes (sécurité, confidentialité, intégrité, contrôle, consentement valable), décrit les nouvelles formes d'exposition et de surveillance et prépare, de manière rigoureuse, le terrain pour l'analyse des instruments de sanction dont dispose le droit pénal.

Titre II
LES INFRACTIONS CLASSIQUES DESTINÉES À ASSURER LA PROTECTION DE LA VIE PRIVÉE EN ROUMANIE ET EN FRANCE

436. La doctrine de la vie privée entre droit civil et droit pénal : Carbonnier, Merle et Lindon. Si l'on pense à la déclaration de J. Carbonnier selon laquelle « la vie privée se traduit par l'obligation d'abstention : laissez-moi tranquille »[1245], il faut définir la notion de vie privée et sa délimitation de la vie publique. Des auteurs comme R. Badinter estiment que la vie d'un individu est divisée entre ces deux concepts : privé, intime, secret et celui public, qui est caractérisé par des activités collectives[1246]. Dans une tentative de définir les limites du droit à la vie privée, M. Lindon affirme que celui-ci comprend « les intérêts des membres de sa famille, l'intimité de sa vie familiale et de son amour, ainsi que ses biens personnels »[1247]. Jean Carbonnier considère que c'est « la sphère secrète de la vie dans laquelle l'individu aura le pouvoir d'exclure des tiers »[1248]. R. Merle et A. Vitu la définissent comme « tout ce qui concerne l'individu dans ses relations familiales ou amicales, sa vie conjugale ou sentimentale, sa vie physique, ses maladies »[1249].

Chapitre 1
LES RÉGLEMENTATIONS TRADITIONNELLES RELATIVES AU DOMICILE ET À LA CORRESPONDANCE

437. Droit à la vie privée: droit constitutionnel. Le droit au respect de la vie privée est garanti par le Conseil constitutionnel, dont les décisions le renforcent au fil du temps : en 1995, le droit au respect de la vie privée est attribué à l'article 66 de la Constitution de 1958[1250]. Par la suite, en 1999[1251] et 2014[1252], il est associé aux droits fondamentaux de l'homme énoncés à l'article 2 de la Déclaration des droits de l'homme de 1789.

[1245] J. Carbonnier, „*Droit civil, Les personnes*", PUF, 21e éd., col.Thémis, 2000.
[1246] R. Badinter, „*Le droit au respect de la vie privée*", JCP, I. ch. 2136, 1968.
[1247] R. Lindon, „*La presse et la vie privée*", JCP, I. ch. 1887, 1965.
[1248] J. Carbonnier, „*Droit civil, Les personnes*", PUF, 21e éd., col.Thémis, 2000.
[1249] R. Merle, A. Vitu, „*Droit pénal spécial*", Cujas, no.2033, 1981.
[1250] *Décision n° 94-352 DC du 18 janvier 1995 - Loi d'orientation et de programmation relative à la sécurité* https://www.vie-publique.fr/fiches/23879-en-quoi-consiste-le-droit-au-respect-de-la-vie-privee.
[1251] *Décision n° 99-416 DC du 23 juillet 1999 - Loi portant création d'une couverture maladie universelle* https://www.conseil-constitutionnel.fr/decision/1999/99416DC.htm
[1252] *Décision n° 2014-693 DC du 25 mars 2014 - Loi relative à la géolocalisation* https://www.conseil constitutionnel.fr/decision/2014/2014693DC.htm

438. La dimension du droit à la vie privée. Brièvement, le droit au respect de la vie privée implique :

- Le droit à la vie privée, à la confidentialité des données personnelles, au secret médical ou professionnel, à l'image[1253].

- Des réglementations claires (et leur respect méticuleux) concernant la surveillance et l'interception lors de l'enquête sur un délit[1254].

- Cadre législatif solide face au risque imposé par le développement de la technologie. Tout acte illégal impliquant la violation d'un principe ci-dessus peut constituer une atteinte à la vie privée.

Section 1. LES BASES JURIDIQUES PROPRES AU DROIT FRANÇAIS

439. Fondements civiles. En examinant le cadre législatif français destiné à protéger la vie privée, on peut citer l'article 9 de la loi no 70-643[1255] du 17 juillet 1970 du code civil, selon lequel « chacun a droit au respect de la vie privée ». En même temps, le législateur a introduit dans le Code pénal un certain nombre de délits visant à protéger la vie privée. L'infraction de l'atteinte à la vie privée est entrée en vigueur dans l'ancien Code pénal le 1er janvier 1978 (art.368), avant d'être reprise dans le Code actuel en 1994 (aux articles 226-1 à 226-7)[1256].

La Loi Informatique et Libertés (Loi Informatique et Libertés), adoptée en 1978 et modifiée par la suite pour se conformer au RGPD, prévoit des règles de protection des données à caractère personnel. Elle impose des obligations strictes aux entités qui collectent et traitent les données à caractère personnel, garantissant ainsi les droits des personnes dans la gestion de ces données personnelles.[1257]

Toujours en 1978, la Commission nationale de l'informatique et des libertés (CNIL) a été créée, chargée du respect de la législation relative à la protection de la vie privée et des

---

[1253] J. Seuvic, *André Vitu (6 juillet 1920 - 27 octobre 2013),* Revue de science criminelle et de droit pénal comparé, n°4(4), 2013. p.731-733. https://doi.org/10.3917/rsc.1304.0731.

[1254] *Action publique en matière d'atteinte à la vie privée et preuve par enregistrements de conversations privées*, Dalloz, 2012. https://actu.dalloz-etudiant.fr/a-la-une/article/action-publique-en-matiere-datteinte-a-la vie-privee-et-preuve-par-enregistrements-de-conversa/h/9e8df5427ed1eb04c79ee33e066113b3.html

[1255] *Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens*, https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000006529713 203

[1256] *Code Penal*. https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006149831/#LEGISCTA000006149831

[1257] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068624.

données personnelles. De plus, la CNIL a le pouvoir d'appliquer des sanctions si elle constate des manquements à la réglementation.[1258]

Le droit à la vie privée est également protégé par l'article 8 de la CEDH, qui garantit à « toute personne le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance, et la participation des pouvoirs publics n'est permise que dans certaines situations prévues par la loi ».[1259]

440. Réglementation des services d'information. La loi no 2015-912 du 24 juillet 2015[1260] réglemente la surveillance et l'interception en France. Les articles 323-1 à 323-8 du Code pénal français (modifiés par la loi précitée) protègent les données personnelles informatiques contre tout accès non autorisé, toute modification ou destruction ou toute action visant à compromettre leur fonctionnalité.[1261]

La loi sur la liberté de la presse du 29 juillet 1881 protège contre la diffamation et les injures. Elle protège la réputation personnelle, empêchant les déclarations fausses ou préjudiciables de nuire à l'image d'une personne.[1262]

§1. LES INFRACTIONS CONNEXES ET COMPLÉMENTAIRES À LA PROTECTION DE LA VIE PRIVÉE

A. Violation de domicile

441. Respect du domicile : cadre juridique français. La protection du domicile, à savoir son inviolabilité, est garantie en France depuis la révolution de 1789 et n'a pas été contestée jusqu'à ce jour[1263].

[1258] La Commission Nationale de l'Informatique et Libertés (CNIL), www.cnil.fr

[1259] U. Kilkelly, *Le droit au respect de la vie privée et familiale*, Direction Générale des Droits de l'Homme, Conseil de l'Europe, 2003. https://rm.coe.int/168007ff5a

[1260] *LOI n° 2015-912 du 24 juillet 2015 relative au renseignement*, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899/2015-07-27/

[1261] *Code Penal - Chapitre III : Des atteintes aux systèmes de traitement automatisé de données (Articles 323-1 à 323-8)*

[1262] *La loi du 29 juillet 1981, „Loi sur la liberté de la presse*", https://www.legifrance.gouv.fr/.

[1263] J.L. Rosenthal, *The Fruits of Revolution: Property Rights, Litigation, and French Agriculture, 1700 1860*, The Journal of Economic History, vol.50(2), 1990. p.438-440. doi:10.1017/S0022050700036585 https://www.cambridge.org/core/journals/journal-of-economic-history/article/abs/fruits-of-revolution-property rights-litigation-and-french-agriculture-17001860/E332FB953436269BA5F21476F9578DBE

Dans le Code pénal de 1810, l'article 184 incluait comme délit toute entrée des autorités, sans autorisation, dans la maison d'un citoyen, et punissait cette entrée avec emprisonnement et amende[1264].

L'actuel Code pénal français incrimine la violation de domicile par son article 226-4[1265], celle-ci étant définie comme l'entrée non autorisée dans un domicile ou un espace privé, utilisant la menace, l'agression ou la coercition[1266]. En ce qui concerne les pouvoirs publics, la loi est plus stricte. Selon l'article 432-8 du Code pénal, l'entrée non autorisée, même sans éléments de violence dans le domicile d'une personne[1267], constitue un délit. En outre, la Cour constitutionnelle rappelle au fil du temps l'importance de protéger ce droit fondamental. Par exemple, dans sa décision de la loi no 83-1179 relative aux finances pour 1984[1268], les dispositions de l'article 89 sont déclarées inconstitutionnelles, soulignant l'obligation de respecter l'article 66 de la Constitution[1269] dans toute intervention des autorités[1270]. Un autre exemple est la décision no 18-40.040 de 2019[1271], dans laquelle la Cour constitutionnelle déclare inconstitutionnel l'article L.651-6, paragraphe 6 du Code de la construction et du logement[1272], selon lequel le personnel municipal peut entrer sans accord dans des maisons privées, s'il est accompagné du maire ou d'un policier. Il a donc été modifié par l'ordonnance no 2019-964 du 18 septembre 2019 (art. 5)[1273].

442. La notion de domicile dans la sphère privée. Depuis 1997, la Cour de cassation de France clarifie la notion de « domicile » du point de vue pénal en établissant qu'elle comprend, outre le lieu où l'individu a sa résidence principale, tout autre lieu considéré par l'individu comme sa « maison », quelle que soit la destination donnée à cet espace[1274]. Ainsi, une chambre

---

[1264] *Code pénal de 1810*, Édition originale en version intégrale, publiée sous le titre : *Code des délits et des peines,* https://www.ledroitcriminel.fr/la_legislation_criminelle/anciens_textes/code_penal_1810/code_penal_1810_1.htm"

[1265] *Code pénal Art. 226-4,* https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CPEN003692

[1266] Violation de domicile - Septembre 2022

[1267] *Code pénal, Paragraphe 3: Des atteintes à l'inviolabilité du domicile, article 432-8*. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418510/2022-03-19

[1268] *Loi n° 83-1179 du 29 décembre 1983 de finances pour 1984*, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000319977

[1269] *Constitution du 4 octobre 1958*. https://www.legifrance.gouv.fr/loda/id/LEGISCTA000006095828"

[1270] *Décision 83-164 DC - 29 décembre 1983 - Loi de finances pour 1984 - Non conformité partielle* https://www.legifrance.gouv.fr/cons/id/CONSTEXT000017667530

[1271] Cour de cassation - Troisième chambre civile *17 janvier 2019 / n° 18-40.040*, https://www-dalloz fr.docelec.u-bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_2019-01-17_1840040

[1272] *Code de la construction et de l'habitation, Article L651-6* https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000039119648

[1273] *Ordonnance n° 2019-964 du 18 septembre 2019 prise en application de la loi n° 2019-222 du 23 mars 2019 de 2018-2022 et de réforme* https://www.legifrance.gouv.fr/loda/id/LEGIARTI000039110953/2020-01-01/

[1274] Cour de cassation - Chambre criminelle *22 janvier 1997 / n° justice, 95-81.186* https://www.dalloz.fr/documentation/Document?id=CASS_LIEUVIDE_1997-01 22_9581186&FromId=DZ_OASIS_001855#texte-integral

d'hôtel, une tente ou un parking sont considérés comme des domiciles[1275], l'occupation de l'espace pouvant être temporaire[1276]. La discussion sur l'octroi du titre de domicile à un véhicule automobile a suscité beaucoup de controverses dans le passé[1277]. À l'heure actuelle, les voitures ne sont pas considérées comme un domicile, ce qui a été confirmé par le Conseil constitutionnel dans diverses décisions[1278].

443. Configuration juridique de la violation de domicile. Comme tout délit, la violation du domicile comporte également deux composantes [1279]:

- Composante matérielle (comportement) : action physique, d'entrer dans un logement sans permission. De plus, le consentement du propriétaire doit être sans équivoque et ne pas être obtenu sous la menace.

- Composante morale : l'intention du délinquant, c'est-à-dire la connaissance de la cause du délit qu'il s'apprête à commettre.

La Cour européenne des droits de l'homme (CEDH) défend la vie privée encadrant dans le terme de domicile, près du logement, les lieux d'activité professionnelle ou personnelle[1280].

a). Violation de domicile lors du divorce

444. Le divorce : régime juridique. Le domicile conjugal est le foyer commun des époux et, dans le cadre d'une procédure de divorce, l'un des époux peut perdre son droit sur ce logement, même s'il en est le propriétaire légal[1281]. [1282]

Partant de l'article 226-4 du Code pénal français, l'un des époux peut commettre le délit d'atteinte au domicile s'il ne se conforme pas à la décision judiciaire sur l'usage du domicile conjugal[1283]. En approfondissant, il est considéré comme une violation du domicile si le partenaire qui a perdu ses droits entre sans permission dans l'ancien domicile, pour quelque

[1275] Cour de cassation - Chambre criminelle *7 mars 2007 / n° 06-88.651*, https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_2007-03-07_0688651
[1276] M. Véron, *Droit pénal spécial*, 14e éd., no.272, Sirey, 2012.
[1277] *Décision n° 76-75 DC du 12 janvier 1977 - Loi autorisant la visite des véhicules en vue de la recherche et de la prévention des infractions pénales*, https://www.conseil-constitutionnel.fr/decision/1977/7675DC.htm
[1278] *Décision n° 94-352 DC du 18 janvier 1995 - Loi d'orientation et de programmation relative à la sécurité*, https://www.conseil-constitutionnel.fr/decision/1995/94352DC.htm
[1279] S. Corioland, *Responsabilité pénale des personnes publiques: infractions intentionnelles*, Dalloz, 2022. https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=RPP_RUB000039
[1280] *Niemietz c. Allemagne – no 13710/88, 16.12.1992*. https://www.lexbase.fr/jurisprudence/1029413-cedh-16 12-1992-req.-72-1991-324-396-niemietz-c.-allemagne
[1281] Y. Mayaud, *Perte et violation du domicile conjugal*, Dalloz, 1997. https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=RSC/CHRON/1997/0110
[1282] T. Moussa, J.-J. Bourdillat, *L'expulsion d'un époux du domicile conjugal: des procédures civiles d'exécution au droit pénal*, Procédures, comm.9, 2002.
[1283] Y. Mayaud, *Perte et violation du domicile conjugal*, Dalloz, 1997. https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=RSC/CHRON/1997/0110

raison que ce soit (même pour la récupération des affaires personnelles[1284])[1285] ou s'il ne quitte pas le domicile à la date fixée par le tribunal[1286].

445. Peines complémentaires. En cas de réconciliation entre conjoints, l'infraction ne sera pas annulée, mais des circonstances atténuantes peuvent être accordées si l'auteur n'a pas commis d'autres délits (vandalisme, autres actes de violence)[1287].

Dans ce contexte, la violation de domicile est punie d'un an d'emprisonnement et d'une amende de 15 000 euros, selon l'article 226-31[1288] du Code pénal. La tentative est punie dans les mêmes conditions que l'infraction, selon l'article 226-5[1289] du Code pénal.

b). Violation de domicile par un agent public

446. Protection du domicile vis-à-vis des autorités publiques. Pour constituer un délit, l'entrée d'un agent public dans le domicile doit se faire contre la volonté du propriétaire et en dehors des cas prévus par la loi[1290]. L'agent doit également entrer dans la maison en abusant de sa qualité officielle, portant un uniforme, un badge ou des documents prouvant de son statut.

Le terme d'agent comprend la personne qui exerce une fonction publique ou est chargée d'une mission de service public, le plus souvent : police, gendarmerie, huissiers de justice, magistrats[1291].

447. Perquisition domiciliaire : légalité et proportionnalité. Du point de vue du code de procédure pénale, il est permis d'entrer dans la maison sans consentement dans les situations suivantes :

[1284] Paris, 15 déc. 1989, *Dr. pénal* 1990. Comm. 213

[1285] P.J. Claux, S. David et all., *Droit et pratique du divorce Livre 0 - Introduction générale*, Dalloz référence, 2024/2025. https://www dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=NOTE_DZ/REFERENCE/DIVORCE/2023/PARA/422.34_2

[1286] Cour de cassation - Chambre criminelle, *9 décembre 1998 / n° 97-80.578*. https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_1998-12-09_9780578

[1287] Cour de cassation - Chambre criminelle, *22 janvier 1997 / n° 95-81.186*. https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_1997-01-22_9581186

[1288] *Code pénal, Section 7: Peines complémentaires applicables aux personnes physiques (Articles 226-31 à 226 32)*.https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165316/2022-01 26/#LEGISCTA000006165316

[1289] *Code pénal: Section 1: De l'atteinte à la vie privée (Articles 226-1 à 226-7)* https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165309/2022-01 26/#LEGISCTA000006165309

[1290] Collège des procureurs généraux, *Privation de liberté et possibilités de pénétrer dans le domicile privé en vue d'arrêter un suspect, un inculpé ou une personne condamnée*, Ministère public, Bruxelles, 2011. https://www.om-mp.be/sites/default/files/u1/col11_2011_position_du_college.pdf

[1291] S. Corioland, *Responsabilité pénale des personnes publiques: infractions intentionnelles*, Dalloz, 2022. (actualisation: 2024) https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=RPP_RUB000039

- Délit flagrant : les autorités peuvent violer le principe d'inviolabilité du domicile si elles ont de bonnes raisons de soupçonner qu'une infraction y est/a été commise (violence, vol, trafic de drogue)[1292].

- Enquête préliminaire[1293]

-perquisitions : en cas de soupçon d'infraction, par le juge d'instruction ou par une commission désignée par lui, avec mandat de perquisition, entre les heures légales (06:00 et 22:00), conformément aux dispositions des articles 57 et 59[1294].

Par conséquent, les perquisitions doivent être effectuées dans le strict respect des règles de l'article 96 du code de procédure pénale, sinon elles peuvent constituer une violation du domicile[1295]. Par exemple, dans sa décision no. 003614 de 1991, la Cour de cassation précise clairement qu'il faut respecter les heures légales de perquisition (6:00 à 22 :00), déclarant l'entrée illégale dans le domicile en dehors de cette période horaire[1296]. Dans le code de procédure pénale, certaines exceptions à cette règle sont également stipulées, telles que : les perquisitions en cas de proxénétisme (art. 706-35)[1297], le terrorisme (art. 706-24-1)[1298], la consommation ou le stockage de substances illicites (art. 706-28)[1299].

Comme indiqué ci-dessus, l'article 432-8 du Code pénal français criminalise l'entrée au domicile personnel sans autorisation, mais ne prévoit rien sur le maintien dans le logement, c'est-à-dire sur le refus des autorités de quitter le lieu si le propriétaire le leur demande[1300].

c). Violation de domicile par un particulier (personne physique ou morale)

448. L'infraction de violation du domicile par un particulier[1301] est prévue à l'article 226-4, du Code pénal français. Elle vise à protéger et respecter la vie privée ainsi qu'à protéger

[1292] *Code de procédure pénale.* bordeaux.fr/documentation/Document?id=CPRP000914
[1293] Ibidem
[1294] *Code de procédure pénale, Art. 56 77 96*. https://www-dalloz-fr.docelec.u https://www-dalloz-fr.docelec.u https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CPRP001748&scrll=CPRP014745&FromId=PEN_RUB000326_DOC_1
[1295] C Guéry, *Instruction préparatoire* , Dalloz, 2018. (actualisation: 2024) https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ENCY/PEN/RUB000180
[1296] Cass. crim. *3 juin 1991, Juris-Data no 003614*
[1297] *Code de procédure pénale, Art. 706-35* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CPRP007194
[1298] *Code de procédure pénale, Art. 706-24-1* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CPRP080935
[1299] *Code de procédure pénale, Art. 706-28* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CPRP007167 partie inférieure du formulaire / partie supérieure du formulaire / partie inférieure du formulaire
[1300] *Code de procédure pénale, Art. 77* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CPRP065024
[1301] É. Garçon, *La Violation de domicile, éléments constitutifs*, extrait du « Code pénal annoté » Art. 184, 1ère éd., Paris 1901. par.5.

l'intégrité des propriétés. Dans l'arrêt no. 15-82.400 du 13 avril 2016, la Cour de cassation souligne que la violation du domicile par des menaces, de la force, de la tromperie est soumise au Code pénal[1302].

d). Droit de propriété versus droit au respect du domicile

449. Collision des droits : droit au logement vs droit à la propriété. En 2018, dans l'appel no. 16-15.792, la Cour de cassation de France analyse une atteinte au droit au respect du domicile dans l'affaire suivante : Un couple est appelé à démolir sa maison construite sur un terrain qui ne lui appartient pas et qu'il occupe illégalement depuis 30 ans[1303].

La difficulté de la décision est donnée par le fait que tant le droit à la propriété que le droit au respect du domicile sont des droits fondamentaux protégés par la Convention européenne des droits de l'homme[1304]. La protection du domicile est également garantie par la Constitution[1305]. En l'espèce, la Cour a jugé que la mesure de démolition constitue une atteinte au droit au respect du domicile, mais qu'elle est légitime, étant justifiée par la protection du droit à la propriété. Cette décision met en évidence la difficulté d'équilibrer deux droits fondamentaux et de donner la priorité à l'un d'entre eux[1306].

B. Violation du secret de la correspondance

450. Réglementation relative à la confidentialité de la correspondance. La confidentialité de la correspondance est réglementée par l'article 226–15 du Code pénal, qui interdit l'ouverture, l'interception, l'utilisation ou la divulgation de la correspondance sans le consentement du destinataire[1307]. Dans le cas des autorités publiques, l'infraction est stipulée à l'article 432-9 du Code pénal[1308], précisant que la violation peut être justifiée par autorisation

---

https://ledroitcriminel.fr/la_science_criminelle/penalistes/la_loi_penale/infraction/pcpales_incrim/garcon_violat_dom.htm

[1302] Cour de cassation - Chambre criminelle, *13 avril 2016 / n° 15-82.400.* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_2016-04-13_1582400

[1303] Cour de cassation, *Pourvoi n° 16-15.792.* https://www.courdecassation.fr/decision/5fca90b1d20f5d8407eff47f

[1304] Le droit au respect du domicile est garanti par l'article 8 de la Convention, tandis que le droit à la propriété par l'article 1er, du Protocole no. 1 de la même Convention https://www.echr.coe.int/documents/d/echr/Convention_FRA

[1305] *Décision n° 83-164 DC du 29 décembre 1983, Loi de finances pour 1984*. https://www.conseil constitutionnel.fr/decision/1983/83164DC.htm

[1306] *Droit de propriété vs Droit au respect du domicile*, Dalloz, 2018. https://actu.dalloz etudiant.fr/a-la-une/article/droit-de-propriete-vs-droit-au-respect-du domicile/h/da170da0f035294e1170f82ac842a3b3.html

[1307] *Code pénal français, Article 226-15*, "*Interdiction d'ouvrir ou d'intercepter la correspondance*" https://codexpenal.just.ro/laws/Cod-Penal-Franta-RO.html.

[1308] *Code pénal, Paragraphe 4: Des atteintes au secret des correspondances (Article 432-9*)

de la loi. Le même article criminalise également l'incitation ou la provocation. Le code distingue deux variantes : violation de la correspondance matérielle (lettres) et violation de la correspondance téléphonique (interceptions).

451. La clarté de la notion de correspondance. La définition de la correspondance soulève beaucoup de controverses. Juridiquement, la correspondance comprend tout échange de messages, personnels ou professionnels, entre deux personnes à distance[1309]. Selon l'arrêt no. 11-88.136 de la Cour de cassation sur la plainte pour violation de correspondance, pas tout billet (fourni par l'avocat à son client) n'est considéré comme une correspondance protégée[1310]. Toutefois, cette affaire a également été portée devant la CEDH, qui a déclaré que le billet était une correspondance privée protégée par l'article 8 de la Convention européenne des droits de l'homme[1311].

a). Violation du secret de la correspondance par une autorité publique

452. Infraction relative à la correspondance. La violation du secret de la correspondance par les pouvoirs publics constitue un abus de pouvoir, tel que prévu à l'article 432-9 du Code pénal français[1312]. Près des autorités publiques, les opérateurs ou fournisseurs de services de communications qui interceptent, accèdent ou divulguent la correspondance de ses utilisateurs sont également inclus (conformément à l'article 432-9, paragraphe 2).

Selon l'article ci-dessus, l'interception implique l'utilisation d'un appareil qui enregistre une correspondance téléphonique. Cependant, si les autorités publiques signalent une conversation qui a eu lieu en leur présence sans utiliser un tel dispositif, la Cour de cassation a jugé dans plusieurs arrêts que cela ne constitue pas une infraction[1313].

b). Violation du secret de correspondance lors d'un divorce

453. Confidentialité de la correspondance en cas de divorce. Si le délit est commis par l'ancien/ancienne-époux/épouse de la victime, il s'agit d'une circonstance aggravante et la

[1309] D. Truchet, *Correspondance et communication*, Dalloz, 2014. p.2353 https://www.dalloz.fr/lien?famille=revues&dochype=RECUEIL%2FCHRON%2F2014%2F0434

[1310] Cour de cassation - Chambre criminelle *16 octobre 2012 / n° 11-88.136* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_2012-10-16_1188136

[1311] Cour européenne des droits de l'homme *5e section 24 mai 2018, N° 28798/13*. https://www-dalloz fr.docelec.u-bordeaux.fr/documentation/Document?id=CEDH_LIEUVIDE_2018-05-24_2879813"

[1312] Ibidem ref.69

[1313] Cour de cassation - Chambre criminelle*, 2 avril 1997 / n° 97-80.269, n° 97-80.270.* https://www-dalloz fr.docelec.u-bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_1997-04-02_9780269

peine est portée à deux ans de prison et à une amende pouvant aller jusqu'à 60 000 euros, conformément à la loi no 2020-936 du 30 juillet 2020[1314].

La Cour de cassation cherche également à clarifier l'utilisation des preuves en cas de divorce, notamment celles qui sont susceptibles de violer le secret de la correspondance[1315]. Dans la décision no. 07-21.796, le tribunal a estimé que les SMS présentés comme preuve d'adultère, obtenus sans consentement, étaient protégés par la confidentialité de la correspondance et constituaient une violation grave de la vie privée. Par conséquent, ils ont été exclus[1316].

c). Violation du secret de la correspondance avocat - client

La confidentialité de la relation avocat-client, qui comprend tous les échanges d'informations entre les deux parties, est fondamentale pour assurer un procès juste et équitable[1317].

454. Confidentialité avocat-client : protection jurisprudentielle au niveau de la CJUE et de la CEDH. En 2018, un avocat saisit la Cour de justice sur l'inclusion au dossier d'une enquête de preuves obtenues par écoute de conversations téléphoniques portées avec son client, invoquant la violation des articles 226-15 et 432-9 du Code pénal, ainsi que les articles 6 et 8 de la CEDH[1318]. Suite à la décision no. 17-81.850, la Cour de cassation a demandé l'annulation des preuves fondées sur le contenu de ces conversations, soulignant la violation du droit à la confidentialité[1319].

La confidentialité de la correspondance avocat-client est également soutenue par la Cour de justice européenne (CJUE) à travers de nombreux arrêts[1320]. Par exemple, dans la décision 155/79 de 1982, la CJUE établit que le droit à la confidentialité des correspondances s'étend

---

[1314] *LOI n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales* https://www.legifrance.gouv.fr/loda/id/LEGIARTI000042181440/2020-08-01/

[1315] Cour de cassation - Deuxième chambre civile *29 janvier 1997 / n° 95-15.255* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_1997-01-29_9515255

[1316] Cour de cassation - Première chambre civile *17 juin 2009 / n° 07-21.796* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_2009-06-17_0721796

[1317] J. Dechepy-Tellier, *La confidentialité de la correspondance échangée entre un avocat et son client: une exigence du procès équitable*, Revue Internationale de Droit Comparé. vol.71, n°2, 2019. p.349-370. Fait partie d'un numéro thématique: Études de droit contemporain. Contributions françaises au 20e Congrès international de droit comparé (Fukuoka, 22-28 juillet 2018). DOI : https://doi.org/10.3406/ridc.2019.21088

[1318] Cour de cassation - chambre criminelle audience publique du *27 février 2018 N° de pourvoi: 17-81850* https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2018/03/17-81.850.pdf"

[1319] L. Priou-Alibert, *Précisions sur l'élément intentionnel du délit d'atteinte au secret des correspondances,* Dalloz, 2018. https://www.dalloz-actualite.fr/flash/precisions-sur-l-element-intentionnel-du-delit d-atteinte-au-secret-des-correspondances

[1320] C. Tahri, [*Jurisprudence] Les limites à la confidentialité des correspondances de l'avocat*, La lettre juridique, 2010. https://www.lexbase.fr/article-juridique/3212596 jurisprudenceleslimitesalaconfidentialitedescorrespondancesdelavocat

tant aux correspondances postérieures à l'ouverture de la procédure (conformément au règlement no 17/62 du Conseil de l'Europe[1321]) qu'aux précédentes[1322].

L'avocat est également tenu de préserver la confidentialité de la correspondance[1323]. D'autre part, le client peut rendre publique sa correspondance avec l'avocat, renonçant ainsi à son caractère confidentiel[1324].

d). Attaque contre le secret professionnel

455. Définition pénale du terme « secret professionnel ». Selon l'article 226-13 du Code pénal, la divulgation, sans autorisation, d'informations privées par des personnes ayant accès à ces informations dans leurs relations professionnelles est un délit[1325]. Outre ce règlement général, il existe des domaines professionnels qui requièrent un règlement spécifique, et nous mentionnons ici :

-les médecins (article R.4127-4 du code de la santé publique)

-les avocats (code déontologique). Le décret no. 2023-552 du 30 juin 2023[1326] souligne le caractère absolu, général et illimité dans le temps du secret professionnel de l'avocat et son obligation de ne pas divulguer des informations, sauf dans les cas imposés par la loi. Selon l'avocat Vincent Niore, la profession d'avocat est régie par 2 principes : l'indépendance, son âme et le secret professionnel qui représente son esprit. L'indépendance assure la confiance et le secret professionnel assure la puissance de cette profession libérale[1327].

-les agents de l'administration des douanes (article 59 bis du code des douanes)

-les agents pénitentiaires (article D.581 du Code de procédure pénale)

-les commissaires aux comptes (article L.820-5 et article L.822.15 du Code de commerce), etc.

[1321] *Règlement (CE) n° 17/62 DU CONSEIL, 06-02-1962*. Premier règlement d'application des articles 85 et 86 du traité, https://www.lexbase.fr/texte-de-loi/reglement-ce-n-1762-du-conseil-06021962-premier-reglement dapplication-des-articles-85-et-86-du-trai/L0186AWS.html

[1322] Judgment of the Court of *18 May 1982. - AM & S Europe Limited v Commission of the European Communities*, Legal privilege. content/EN/TXT/?uri=CELEX:61979CJ0155"

[1323] Cour de Cassation - Chambre civile 1, du *6 avril 2004, 00-19.245*, Inédit https://www.legifrance.gouv.fr/juri/id/JURITEXT000007470694/

[1324]Cour de cassation, *4 avril 2006, n° 04-20.735* https://www.courdecassation.fr/decision/60794d4a9ba5988459c48715

[1325] *Code pénal français, articles 226-13 et 226-14, relatifs à l'atteinte au secret professionnel*, https://codexpenal.just.ro/laws/Cod-Penal-Franta-RO.html.

[1326] *Décret n° 2023-552 du 30 juin 2023 portant code de déontologie des avocats* https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047774060

[1327] V. Nioré , L. Dusseau, *Le cœur de la défense*, Gaz. Pal., ed. prof. 2015. https://www.gazette du-palais.fr/article/GPL223k2/

456. Confidentialité avocat-client à la lumière des obligations AML. Des discussions sensibles concernant la protection du secret professionnel des avocats ont également eu lieu dans l'affaire Michaud c. France (no. 12323/11)[1328]. Le requérant (avocat, membre du barreau de Paris) conteste l'obligation des avocats en France de signaler d'éventuels soupçons de blanchiment d'argent commis par leurs clients, alléguant une atteinte au droit au respect de la vie privée. Cependant, en 2017, le Conseil national des barreaux a adopté une décision qui oblige les avocats à déclarer tout soupçon concernant des transitions financières ou immobilières illégales[1329]. Cette décision fait suite aux directives sur le même sujet adoptées par l'Union Européenne depuis 1991[1330]. Par conséquent, dans l'affaire précitée, la Cour européenne des droits de l'homme conclut en unanimité qu'il n'y a pas violation de l'article 8 de la CEDH, la situation étant une atteinte au droit à la confidentialité de la relation avocat-client[1331].

457. Le secret professionnel entre avocat et client dans les mécanismes anticorruption. Au début de l'année 2023, dans l'arrêt no. 2022-1030 QPC[1332], le Conseil constitutionnel confirme le caractère constitutionnel des dispositions de la loi no 2016-1691 du 9 décembre 2016 (également appelée loi Sapin II »)[1333]. Cette loi permet aux autorités publiques de superviser le travail des avocats et d'utiliser par la suite les informations obtenues dans l'exercice de leur profession, afin de prévenir la fraude et la corruption. Dans l'arrêt précité, la Cour considère que les mesures de Sapin II ne portent pas atteinte à la protection du secret professionnel des avocats, pour autant que la confidentialité et les droits fondamentaux de l'homme soient respectés.

458. Secret professionnel : principe absolu. Il existe de nombreuses jurisprudences qui réaffirment l'importance du secret professionnel, mais condamnent son utilisation à des fins

---

[1328] Cour européenne des droits de l'homme, *affaire Michaud c. France, no 12323/11,* 2012. https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-115055%22]}

[1329] *Décision du 26 janvier 2017 portant réforme du règlement intérieur national (RIN) de la profession d'avocat* (art. 21-1 de la loi du 31 décembre 1971 modifiée) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000034413885

[1330] *Directive 2005/60/CE relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme*

[1331] Cour européenne des droits de l'homme, *L'obligation de déclaration de soupçon incombant aux avocats dans le cadre de la lutte contre le blanchiment ne porte pas une atteinte disproportionnée au secret professionnel*, Communiqué de presse du Greffier de la Cour, 2012. https://actu.dalloz etudiant.fr/fileadmin/actualites/pdfs/DECEMBRE_2012/Arret_de_chambre_Michaud_c._France_06.12.2012.pdf

[1332] *Décision n° 2022-1030 QPC du 19 janvier 2023* https://www.conseil-constitutionnel.fr/decision/2023/20221030QPC.htm

[1333] *LOI n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique.* https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033558528

illégales ou pour entraver la justice[1334]. Toutefois, le secret professionnel demeure un principe absolu, dans le but de garantir la confidentialité avocat-client.

Cependant, de nombreuses voix craignent l'érosion du principe du secret professionnel, à la fois par les décisions des tribunaux pénaux et en raison des règlements législatifs[1335]. Dans ce contexte, le Conseil d'Etat français a ordonné l'annulation[1336] des dispositions du décret du 26 juin 2006[1337] qui obligeait les avocats à signaler les soupçons de fraude fiscale.

C. Diffamation et insultes

459. Diffamation, injure : définition, distinction. En France, la loi du 29 juillet 1881 sur la liberté de la presse[1338] réglemente la liberté d'expression et ses limitations, notamment en matière de diffamation, d'injuries et de calomnie. L'article 29 de la loi du 29 juillet 1881 définit la diffamation comme « une imputation à tout fait qui touche à l'honneur ou à la réputation d'une personne ». Dans le même article, on entend par injurie « toute expression offensante, tout terme de mépris ou d'invective qui ne comprend pas l'imputation d'un fait ». L'injurie, par opposition à la diffamation, fait référence aux mots ou expressions offensants, humiliants et insultants[1339].

La diffamation, également considérée comme « la reine des délits de presse »[1340], est un acte pénal, correspondant à la calomnie et impliquant une accusation fausse et malveillante, bien que la véracité des allégations n'influence pas l'application des sanctions (selon l'article 35 de la loi précitée)[1341].

460. Diffamation : atteinte à la liberté d'expression. La diffamation, définie en d'autres termes, est un abus de la liberté d'expression. La liberté d'expression est un droit fondamental, garantie par l'article 11 de la Déclaration des droits de l'homme et du citoyen, qui la définit comme l'un des droits de l'homme le plus précieux[1342]. L'article 10 de la Convention pour la

---

[1334] Cour de cassation, civile, Chambre civile 1, *12 octobre 2016, 15-14.896*, Publié au bulletin https://www.legifrance.gouv.fr/juri/id/JURITEXT000033267688/

[1335] B. Py, *Secret professionnel: le syndrome des assignats*?, Actualité juridique Pénal, vol.04, 2004. pp.133. ⟨halshs-02224859⟩

[1336] Conseil d'État, Section du Contentieux, *10/04/2008, 296845,* Publié au recueil Lebon https://www.legifrance.gouv.fr/ceta/id/CETATEXT000018624326/

[1337] *Décret n°2006-736 du 26 juin 2006 relatif à la lutte contre le blanchiment de capitaux et modifiant le code monétaire et financier* (partie réglementaire). https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000457902/2020-11-24/

[1338] *Loi du 29 juillet 1881 sur la liberté de la presse* https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722/2021-01-04/

[1339] *La différence entre Diffamation et Injurie*, La Monde du Droit. https://www.lemondedudroit.fr/

[1340] A. Lepage, H. Matsopoulou, *Droit pénal spécial*, PUF 1re éd., coll. Thémis Droit, 2015.

[1341] Ibidem note 123

[1342] *La déclaration des droits de l'homme et du citoyen,* Assemblée Nationale, 1789. https://www.elysee.fr/la-presidence/la-declaration-des-droits-de-l-homme-et-du-citoyen

protection des droits de l'homme et des libertés fondamentales stipule également le droit à la liberté d'expression, à la liberté d'opinion, à la liberté de recevoir et de transmettre des informations ou des idées[1343].

Au niveau européen, l'article 10 (« Liberté de pensée, de conscience et de religion »), paragraphe 2 de la Convention européenne des droits de l'homme[1344], stipule que ces droits seront réalisés conformément aux lois nationales, permettant ainsi aux autorités locales de restreindre et de contrôler la liberté d'expression. Pour illustrer cela, nous pouvons regarder l'affaire Reichman c. France, où un journaliste, condamné en France pour diffamation, affirme que son droit à la liberté d'expression a été violé[1345]. Dans ce cas, la CEDH souscrit à l'arrêt de la justice française, en faisant valoir que « la réputation », bénéficiant d'une protection au titre de la vie privée, est défendue par les lois nationales qui la qualifient « d'ingérence de l'État ».

461. Test de proportionnalité entre la liberté d'expression et la protection de la réputation. S'adaptant à l'évolution actuelle de la technologie, la France adopte en 2015 la loi no. 2015-1779[1346], suivie plus tard par la loi no. 2020-766 sur la lutte contre les discours haineux sur internet[1347]. Afin de protéger le droit à la liberté d'expression, le Conseil d'Etat analyse la constitutionnalité de cette première loi, et dans la décision n. 2015-512 QPC déclare que des limitations ou sanctions en matière de liberté d'expression sont permises, lorsque des abus sont commis, la réalisation de l'exercice de cette liberté devant être proportionnelle à l'objectif poursuivi[1348].

462. Cas classique: de J'accuse à l'exil. L'un des premiers cas de diffamation en France, et peut-être le plus connu, est celui d'Emile Zola[1349]. En 1898, le célèbre écrivain et journaliste est accusé de diffamation[1350] suite à la publication de l'article « J'accuse »[1351].

[1343] *Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentale*s telle qu'amendée par le Protocole n°15. à compter de son entrée en vigueur le 1er août 2021 https://rm.coe.int/1680a2353e

[1344] *Carta des droits fondamentaux de l'Union Européenne, Titre II : Libertés, Article 10 – Liberté de pensée, de conscience et de religion*.

[1345] *Affaire Reichman c. France, requête no 50147/11*

[1346] *LOI n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public* https://www.legifrance.gouv.fr/loda/id/LEGIARTI000031706238/2024-11-21/?isSuggest=true

[1347] *LOI n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet* https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970

[1348] Conseil constitutionnel *Décision n° 2015-512 QPC du 8 janvier 2016.* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CONSCONST_LIEUVIDE_2016-01-08_2015512

[1349] S. Tonnerre-Seychelles, *Après "J'accuse...!", les procès de Zola*, BnFG Gallica, 2018. https://gallica.bnf.fr/blog/05032018/apres-jaccuse-les-proces-de zola?mode=desktop

[1350] P.-V. Stock (éd), *L'affaire Dreyfus. Le procès Zola devant la cour d'assises de la Seine et la cour de cassation (7 février-23 février-31 mars-2 avril 1898): compte rendu sténographique "in extenso" et documents annexes*, aux bureaux du „Siècle", 1989.

[1351] Dans cette lettre ouverte, Emile Zola accuse l'armée française de corruption, antisémitisme et conspiration, suite à la condamnation injuste du capitaine Alfred Dreyfus.

463. Cas récent : incitation à la discrimination et à la haine religieuse. Un autre cas plus récent de diffamation est celui d'Eric Zemmour en 2021. Le politicien et journaliste français a été accusé par les tribunaux français de diffamation à la suite de déclarations racistes contre les musulmans et l'islamisme[1352]. L'affaire est portée devant la CEDH (no 63539/19)[1353], où Zemmour réclame une violation de son droit d'expression garanti par l'article 10 de la Convention. La CEDH estime que les droits fondamentaux n'ont pas été violés et que la décision des autorités françaises était légitime.

D. Article 226-19 du Code pénal français (conservation illicite de données)

464. La conservation et la mise en mémoire de données à caractère personnel. L'article 226-19 du Code pénal français s'inscrit dans le cadre législatif visant à protéger la vie privée et les droits de la personne dans le contexte du traitement des données à caractère personnel. D'un point de vue législatif, l'État français a été l'un des premiers pays d'Europe à imposer une réglementation stricte sur l'utilisation des données à caractère personnel, avec l'adoption en 1978 de la loi relative à l'informatique, aux fichiers et aux libertés[1354]. Cette loi a facilité le développement de la législation actuelle dans ce domaine, en créant la base pour l'intégration ultérieure des règles promues au sein de l'Union Européenne dans le droit national.

L'article 226-19 est pertinent car il protège les informations personnelles d'un individu. Dans une société moderne où toute information personnelle est un bien précieux qui peut être exploité, la réglementation de l'utilisation et de la protection de ces informations devient un processus impératif que chaque État doit suivre[1355]. Les données personnelles peuvent être utilisées de nombreuses façons, que ce soit à des fins économiques ou criminelles. La protection de ces données n'est pas seulement une exigence technique à laquelle doit se conformer tout opérateur de services essentiels, mais aussi une question qui peut avoir des implications éthiques pour les droits fondamentaux de tout individu. Pour ces raisons, l'État a l'obligation de créer et de réglementer les exigences nécessaires, et les opérateurs de services essentiels ont l'obligation d'appliquer strictement ces règles.

Toute tentative de traitement non autorisé de données à caractère personnel est sanctionnée en fonction de la gravité du délit. On entend par traitement non autorisé la collecte,

---

[1352] Le Monde, *Article sur Éric Zemmour*, 2021. https://www.lemonde.fr/police justice/article/2021/11/17/ouverture-du-proces-contre-eric-zemmour-pour-ses-propos-sur-les-mineurs isoles_6102349_1653578.html.

[1353] CEDH, *Zemmour c. France, 1er mars 2021, 63539/19*

[1354] *Loi n° 78-17 du 6 janvier 1978 relative à 'informatique, aux fichiers et aux libertés*, consulté le 27 novembre 2024, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/.

[1355] Ibidem, *article 226-19*.

l'enregistrement, la conservation ou la communication de données à caractère personnel sans le consentement de la personne concernée. En vertu de la législation européenne et de la législation française subséquente, les données à caractère personnel désignent tout type d'information susceptible de permettre l'identification d'une personne physique, que ce soit par des moyens directs ou indirects[1356]. Les moyens directs d'identification d'une personne font référence au nom, à l'adresse, au numéro de téléphone, au code numérique personnel ou à toute autre information susceptible de permettre l'identification d'une personne. Selon la loi, ces délits sont passibles d'une peine d'emprisonnement pouvant aller jusqu'à cinq ans et d'une amende pouvant aller jusqu'à 300.000 euros pour les personnes physiques. En même temps, les personnes morales peuvent également être sanctionnées, les amendes étant beaucoup plus sévères[1357].

465. Traitement illicite de données. L'article 226-16 du Code pénal a également été mis à jour en criminalisant le mauvais traitement des données personnelles[1358]. Caractéristique de ce règlement, on peut remarquer des changements en termes du côté subjectif du délit, à savoir la commission de l'acte, y compris la forme de culpabilité de négligence, qui nous prouve le sérieux pragmatisme avec lequel le législateur a proposé de prévenir et de combattre les traitements non conformes des données à caractère personnel. Par ailleurs, en analysant la complexité des situations illégales découlant de relations sociales à la lumière du non-respect des responsabilités des responsables du traitement des données à caractère personnel[1359], effectuées par des traitements non conformes, le législateur a jugé approprié, à titre préventif, inclure les dispositions des articles 226-16-1 - 226-22-1 du Code pénal.

466. Les articles 226-16 à 226-24 du Code pénal[1360] criminalisent le régime de collecte, de stockage, de traitement ou de divulgation des données personnelles dans des conditions de non-respect des normes légales et de non-consentement des personnes concernées.

[1356] *Data protection explained*, European Commission. consulté le 27 novembre 2024, https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

[1357] *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*.

[1358] En ancienne variante, *l`art. 226-16 du Code pénal français* incriminait le fait de traiter en manquant de la loi.

[1359] En guise de complément, la forme de la loi couvre également les devoirs des destinataires ou des personnes habilitées par les responsables du traitement.

[1360] L'article 226-16 a été modifié par la loi no 2024-449 du 21 mai 2024 - art. 5 ; l'article 226-16-1 a été introduit par la loi cadre no 2004-801 du 6 août 2004 - art. 2. 14 JORF 7 août 200 ; l'article 226-16 2 a été introduit par la loi cadre no 2021-646 du 25 mai 2021 - art. 6. 52 (V); l'article 226-17 a été modifié par l'Ordonnance no 2018-1125 du 12 décembre 2018 - art. 13 ; l'article 226-17-1 a été modifié par l'Ordonnance no 2018-1125 du 12 décembre 2018 - art. 13 ; l'article 226-18 a été modifié par la loi no 2004-801 du 6 août 2004 - art. 14 () JORF 7 août 2004 ; l'article 226-18-1 a été introduit par la Loi cadre no. 2004-801 du 6 août 2004 - art. 14 () JORF 7 août 2004 ; l'article 226-19 a été modifié par l'Ordonnance no 2018-1125 du 12 décembre 2018 - art. 6. 13 ; l'article 226-19-1 a été introduit par la loi cadre no 2004-801 du 6 août 2004 - art. 2. 14 () JORF 7 août 2004 ; l'article 226-20 a été modifié par la loi no 2004-801 du 6 août 2004 - art. 14 () JORF 7 août 2004 et par la loi no 2000-321 du 12 avril 2000 - art. 6 ; l'article 226-21 a été modifié par la loi no 2004-801 du 6 août 2004 - art. 14 () JORF 7 août 2004 ; l'article 226-22 a été modifié par la loi no 2004-801 du 6 août 2004 - art. 14 () JORF 7 août 2004 ; l'article 226-22-1 a été modifié par l'Ordonnance no 2018-1125 du 12 décembre 2018 - art. 6. 13 ;

Section 2. **LES BASES JURIDIQUES PROPRES AU DROIT ROUMAIN**

467. La vie privée en Roumanie. La vie privée est un droit fondamental de l'homme, qui doit être mieux protégé pour que les individus puissent en jouir. Le législateur roumain, afin de respecter son obligation positive de prendre des moyens pour protéger ce droit fondamental, a criminalisé divers délits pour garantir le respect et l'inviolabilité de la vie privée. De plus, dans le contexte de la mondialisation et particulièrement de l'accélération des progrès technologiques, le Code pénal a introduit dans son contenu des délits qui protègent la vie privée de l'individu par rapport à l'environnement informatique et en ligne.

468. Formes de violation de la vie privée en Roumanie. Ainsi, en vertu du Code pénal, dans le titre I, chapitre IX[1361] de la partie spéciale, les délits suivants sont constatés : la violation de domicile et celle du siège professionnel, la violation de la vie privée et la divulgation du secret professionnel. Il convient de noter d'avance que, malgré la structure unitaire apparente des infractions touchant la vie privée, le législateur n'a pas été suffisamment cohérent, car il existe d'autres délits qui sont réglementés ailleurs dans le Code pénal. Il s'agit notamment de l'infraction de violation du secret de la correspondance, réglementée au titre V, chapitre II, relatif aux infractions d'emploi. Le motif de l'incrimination distincte pourrait être la sanction plus grave de l'acte, si celui-ci est commis par un agent public. En outre, il y a aussi des délits informatiques qui « attaquent » la vie privée de la personne, réglée au titre VII, chapitre VI de la partie spéciale du Code pénal[1362]. Il est donc noté que la réglementation des délits visant à défendre la vie privée n'est pas unitaire.

Dans ce qui suit, nous présenterons en détail les délits mentionnés ci-dessus (et pas seulement celles-ci) par la structure suivante : l'objet juridique, l'objet matériel (le cas échéant), les sujets du délit; le côté objectif (l'élément matériel, le suivi immédiat et le lien causal), le côté subjectif (la forme de la culpabilité, le motif et le but), les formes du délit, les variantes du délit, le cas échéant (aggravants, atténués ou assimilés, selon le cas), sanctions, aspects procéduraux et autres (le cas échéant).

---

l'article 226-22-2 a été modifié par l'Ordonnance no 2018-1125 du 12 décembre 2018 - art. 1 ; l'article 226 23 a été modifié par l'Ordonnance no 2018-125 du 12018 - art. 13 ; l'article 226-24 a été modifié par la loi no 2009-526 du 12 mai 2009 - art. 12.

[1361] Le chapitre intitulé « *Délits touchant le domicile et la vie privée* ».

[1362] Les délits en question sont les suivants : l'accès illégal à un système informatique, l'interception illégale d'une transmission de données informatiques, l'altération de l'intégrité des données informatiques, le transfert non autorisé de données informatiques et les opérations illégales avec des dispositifs informatiques ou logiciels.

§1. LES INFRACTIONS CONNEXES ET COMPLÉMENTAIRES À LA PROTECTION DE LA VIE PRIVÉE

A. Violation de domicile

469. Engagement de l'action pénale. L'article 226-4 du Code pénal français[1363] vise à protéger le droit à l'inviolabilité du domicile, sanctionnant respectivement l'auteur d'entrer sans droit dans le domicile d'une autre personne. L'art. 224 comporte dans son contenu trois alinéas: le premier consacre la forme-type, la base de ce délit, suivant qu'au alinéa (2) précise la forme aggravée du délit et, enfin, au alinéa (3) indique la manière dont l'action pénale est engagée.

470. Objet juridique. L'objet juridique de ce délit est représenté par les relations sociales liées à l'inviolabilité du domicile, la criminalisation étant nécessaire pour la protection effective de la vie privée de l'individu, mais aussi de ses relations familiales, puisque, dans le cadre d'un domicile, la liberté d'expression vis-à-vis des membres de la famille est de principe maximum et il faut les cacher de l'espace public[1364]. De plus, la criminalisation de la violation du domicile n'a pas seulement été effectuée dans l'intérêt particulier des individus, mais elle concerne également un intérêt de la société en général, car nous ne pourrions avoir d'ordre social sans ordre privé. L'inviolabilité du domicile n'est pas exclusivement régie par l'art. 224 du Code pénal, mais est également garantie par les dispositions de l'article 27 de la Constitution[1365].

471. Définition pénale de la notion de domicile. Le domicile, au sens pénal, est défini par l'art. 224 du Code pénal comme la maison, la chambre, la dépendance ou l'endroit clôturé qui lui est rattaché, c'est-à-dire l'espace où vit la victime, l'espace où elle souhaitait mener librement sa vie privée. Le logement désigne tout un espace qui peut être habité - par exemple, une maison, un appartement, une caravane ou une voiture, et la pièce n'est qu'une partie d'un

---

[1363] L'article a été modifié par la *loi no. 2023-668 du 27 juillet 2023 – art. 3 et par la Loi no. 2023-668 du 27 juillet 2023 – l'art. 6*, en vigueur à partir du 29 juillet 2023.

[1364] Dans la doctrine (G. Antoniu, M. Popa, S. Danes, *Criminal Code understandable*, éd. Politică, Bucarest, 1970. p.178), on a constaté que « *les Roumains considéraient le logement comme un refuge, l'asile sacré de la personne* ». Une loi spéciale (« *lex Cornelia de injuriis* ») « *punissait non seulement la pénétration par la violence dans le domicile d'une personne, mais et le fait qu'un particulier a enlevé quelqu'un de sa maison pour le remettre à la justice. Le droit anglais appelle la demeure de l'homme sa forteresse, et la révolution française a proclamé dès les premiers instants* » : « *La maison de tout citoyen est un lieu inviolable*. »

[1365] Le paragraphe (1) de cet article est consacré à la règle d'inviolabilité du domicile : « *Le domicile et la résidence sont inviolables. Nul ne peut entrer ou demeurer dans le domicile ou la résidence d'une personne sans son consentement*. » Toutefois, le paragraphe (2) prévoit également certaines exceptions jugées essentielles par le législateur, lorsque l'inviolabilité du domicile peut être violée : a) « *exécution d'un mandat d'arrêt ou d'une ordonnance de justice* »; b) « *élimination d'un danger pour la vie, l'intégrité physique ou les biens d'une personne »; c) « la sécurité nationale ou la protection de l'ordre public* »; d) « *la prévention de la propagation d'une épidémie* ». Une telle exception est prévue aux deux derniers alinéas de l'article 27, qui indiquent les conditions à remplir : « *(3) La perquisition est ordonnée par le juge et s'effectue dans les conditions et selon les formes prévues par la loi. (4) Les perquisitions nocturnes sont interdites, sauf dans le cas de délits flagrants.* »

logement (comme une pièce dans un appartement). La dépendance est un espace accessoire au logement, qui améliore son utilisation, comme les caves du sous-sol d'un bâtiment, une terrasse, une cave, des séchoirs, etc., et le lieu clôturé qui dépend d'une maison ou d'une dépendance se réfère, par exemple, à un jardin, à une cour et ainsi de suite. Il n'est pas nécessaire, pour l'existence du délit, que le domicile soit permanent, pouvant retenir la violation de domicile même si nous parlons d'un hôtel ou d'une chambre d'étudiant. Cependant, dans la doctrine, dans le cas du logement, il est estimé que celui-ci doit être effectivement occupé afin de pouvoir exister le délit de violation de domicile[1366].

472. Objet matériel. En ce qui concerne l'objet matériel du délit, il existe deux opinions opposées : soit on considère qu'il n'existe pas, justifié par l'objet légal du délit[1367], soit on estime qu'il y a, celui-ci étant la maison, la chambre, la dépendance ou l'endroit clôturé qui lui est rattaché [1368]. Nous considérons qu'en ce qui concerne l'objet juridique et le lieu où est prévue la violation du domicile, étant une infraction à l'encontre de la personne et affectant le domicile et la vie privée, il ne peut être question de l'existence d'un fait matériel sur lequel s'exerce l'action, puisque ce que protège l'article 224 est, en fait, un droit non patrimonial, sans existence matérielle, à savoir l'inviolabilité du domicile.

473. Sujets du délit. Protection pénale du domicile dans les relations locatives. Le sujet actif est générique, l'infraction pouvant être commise par toute personne, y compris le propriétaire/copropriétaire de la propriété louée, dont l'usage a été cédé à une autre personne, et qui entre dans le bâtiment sans le consentement du locataire/sous-locataire[1369]. Des personnes

---

[1366] Un auteur (R. Slavoiu, *Protectia penala a vietii private*, Ed. Universul Juridic, Bucarest, 2016, p. 65-66) considère que la simple occupation d'un espace ne le transforme pas en habitation, ce qui montre qu'une pénétration possible sans droit n'affecterait pas la vie privée de quiconque. Par ailleurs, l'auteur apprécie qu'un espace se transforme en habitation lorsque celui qui utilise cet espace a appliqué à ce lieu quelque chose lié à son intimité, comme le placement de vêtements, d'objets personnels et autres. D'autres auteurs ont estimé que pour qu'un logement soit un foyer au sens du droit pénal, le sujet passif de l'infraction doit y passer sa vie privée pendant une période suffisamment longue et non seulement courte. Ainsi, il est estimé qu'une chambre d'hôtel louée pendant un séjour de vacances ne peut pas constituer un domicile au sens du droit pénal. Nous ne partageons pas ces points de vue, car les dispositions de l'art. 224 du Code pénal ne conditionnent aucunement la possibilité que le logement représente un domicile. Tout ce que l'article 224 exige, c'est que le domicile soit utilisé, sans préciser qu'il doit être utilisé effectivement ou pour une durée déterminée. Admettre une solution contraire signifierait que nous serions privés de protection pénale pour les personnes qui, par exemple, séjournent dans un hôtel pour une soirée et laissent leurs bagages et quittent la chambre immédiatement. Ce qui importe dans ce cas, c'est l'existence d'une intention minimale d'utiliser la chambre, même en laissant les bagages, sans importance sur la période de temps pour laquelle ils sont logés.

[1367] V. Cioclei, „*Drept penal. Partea specială I*", vol. I, 7e éd., Ed. C.H. Beck, București, 2022, p.231-232; M. Udroiu, „*Sinteze de drept penal. Partea specială*" (ci-après M. Udroiu, vol. I) vol. I, 3e éd., Ed. C.H. Beck, București, 2022, p. 375.

[1368] Al. Boroi, „*Drept penal. Partea specială*", 6e éd., Ed. C.H. Beck, București, 2022, p. 197.

[1369] En ce sens, la doctrine (S. Bogdan, D.A. Șerban, *Drept penal. Partea speciala. Infractiuni contra persoanei si contra infaptuirii justitiei,* editia III, Ed. Universul juridic, Bucuresti, 2022. p. 380) a réitéré l'idée de maintenir la violation de domicile dans la situation où le propriétaire du logement entre sans la volonté du locataire, car ce qui est défendu par l'art. 224 du Code pénal n'est pas le patrimoine, mais la liberté et l'inviolabilité du domicile, y compris du locataire. Bien que les contrats de location comportent des clauses qui donnent au propriétaire le droit d'entrer dans la propriété quand il veut, elles ne suppriment pas le droit à l'inviolabilité du domicile du locataire.

actives et morales peuvent être impliquées si, par exemple, les employés de la société qui effectuent des opérations de rénovation d'un appartement y entrent sans le consentement du propriétaire. Également, si l'acte est commis par un agent public au sens de l'art. 175 du Code pénal ou par un agent « privé » au sens de celles prévues à l'art. 308 du Code pénal, l'acte ne constituera qu'un abus de fonction – l'art. 297 du Code pénal - respectivement abus de fonction lié à l'art. 308 du Code pénal[1370]. Si l'agent a la permission de la loi d'entrer au domicile, mais il n'a pas la compétence pour effectuer une telle action, l'infraction d'usurpation de la fonction prévue par l'art. 300 du Code pénal retenue.

474. Formes possibles de participation pénale. En ce qui concerne les formes possibles de participation pénale dans le cas d'une violation du domicile, nous trouvons les trois formes : co-auteur, instigation et complicité.

En ce qui concerne le sujet passif, il peut s'agir de toute personne physique qui utilise la maison, la chambre, la dépendance ou l'endroit clôturé qui lui est rattaché. Par conséquent, il peut être victime d'une violation de domicile à la fois la personne qui utilise le domicile, ainsi qu'un propriétaire ou possesseur. En ce qui concerne le sujet passif de la violation du domicile, deux questions sont soulevées. La première se réfère à la nécessité de légitimité, à la légalité de l'usage de la possession pour qu'une personne puisse être le sujet passif d'incrimination de l'art. 224 du Code pénal. En d'autres termes, pour qu'une personne soit protégée par la disposition précitée, l'utilisation du bien doit-elle être détenue sur le fondement d'un titre légal ? D'une part, il est considéré que, pour être un sujet passif de la violation du domicile, il faut un acte prouvant la possession légitime de l'usage du bien et seule cette personne peut s'opposer à l'auteur de l'infraction à l'entrée ou à la présence illégale dans le domicile[1371].

475. Protection de l'utilisateur effectif du logement, quel que soit son titre. D'autre part, l'opinion contraire avec laquelle nous sommes d'accord est que le sujet passif de la violation du domicile peut inclure une personne qui vit dans un espace sans avoir un titre, donc il vit illicitement. Les dispositions de l'art. 224 du Code pénal exige que la victime du délit utilise la maison, la chambre, la dépendance ou l'endroit clôturé qui lui est rattaché, donc l'utilisation est considérée comme un état de fait et non pas de droit. Aussi, l'art. 224 du Code pénal protège la

---

Le droit apparent du propriétaire d'entrer dans le domicile du locataire est fondé sur un consentement exprès du locataire donné à la conclusion de l'acte juridique, mais ce « consentement » ne supprime pas la protection pénale de l'inviolabilité du domicile. Même si l'opposition ultérieure du locataire concernant l'entrée du propriétaire dans le bien viole une disposition contractuelle expresse, qui pourrait conduire à la résiliation de l'acte, le propriétaire est responsable pénalement pour violation de domicile, qui pourrait avoir un caractère dissuasif, tant en ce qui concerne la violation de l'inviolabilité du domicile, mais aussi sur la résiliation du contrat s'il y avait un accord entre le bailleur et le locataire de ne pas résilier le contrat et de ne pas déposer une plainte préalable en retour.

[1370] Dans une autre opinion (M. Udroiu, *Fișe de drept penal. Partea specială*, București, Universul Juridic, 2014, p.376), on considère que la violation de domicile sera retenue en concours idéal avec le fait d'abus de fonction.

[1371] V. Dobrinoiu, I. Pascu, A.M. Hotca, I. Chiș, M. Gorunescu, C. Păun, M. Dobrinoiu, N. Neagu, M.C. Sinescu, *Le nouveau Code pénal commenté. Partie spéciale*, ediția a III-a, Ed. Universul Juridic, București, 2016. p.201.

vie privée, qui ne dépend pas de l'existence ou de l'absence d'un acte justifiant l'occupation du domicile. Or, si nous devions admettre la première opinion, qui prétend que seuls ceux qui peuvent prouver l'utilisation du logement seraient protégés par la loi pénale, il y aurait une immense injustice pour ceux qui ne peuvent pas prouver l'utilisation du bien, les niant pratiquement le droit à la vie privée et à l'inviolabilité du domicile, violant ainsi les dispositions de la Constitution. Quelle serait la différence, par exemple, entre la situation d'un vagabond qui vit dans une propriété abandonnée et celle d'un locataire qui a conclu un bail? Ou, peut-être encore plus illustratif, on peut aussi considérer la situation des locataires qui utilisent un bien immobilier ou une chambre de celui-ci, pour lequel ils paient un loyer, même si un contrat de location n'a pas été conclu[1372] pour diverses raisons (par exemple, éviter le paiement d'impôts par le bailleur). Dans une telle situation, l'interprétation du droit pénal en ce sens qu'il protège ceux qui peuvent justifier l'utilisation et la non-protection de ceux qui ne peuvent pas, montre d'une manière flagrante l'injustice qui se produirait si nous devions considérer comme valide la première opinion mentionnée ci-dessus.

476. Protection des utilisateurs multiples du logement. La deuxième question que nous soulevons concerne la situation où, si nous avons plus de personnes dans la même maison, nous devrions retenir un délit pour chaque personne blessée ou un seul délit. Par principe, nous considérons que s'agissant d'un délit contre la personne qui défend l'inviolabilité du domicile et de la vie privée, il doit retenir la pluralité des délits s'il y a plusieurs victimes[1373]. Bien que nous ne pouvons pas nier qu'il pourrait y avoir des situations qui sont profondément défavorables pour l'auteur, lorsque, par exemple, dans le même appartement où il entre, vivent, par exemple, 6 personnes, auquel cas 6 délits concurrents de violation du domicile seraient retenus (et si l'acte devait se produire pendant la nuit, nous parlerions d'une responsabilité notablement plus grave), nous pensons que compte tenu de la valeur sociale protégée par l'art. 224 du Code pénal et dont le titulaire est la personne lésée, la pluralité des infractions liées à la pluralité des victimes est conservée (sans pouvoir retenir le délit continué, étant un délit contre la personne). Cependant, nous considérons qu'il existe une solution dans des situations telles que celle mentionnée ci-dessus, à savoir le maintien d'une unité naturelle collective[1374], si la

[1372] Une telle situation a été constatée par la *décision no. 682/2017 du 21.06.2017* prononcée par la Cour d'appel de Constanta (www.rejust.ro) où il était essentiellement conclu que la victime, avec son partenaire, avait vécu dans l'appartement du défendeur, en payant 750 lei/mois de loyer, sans avoir conclu un contrat de bail en ce sens. À un moment donné, la personne blessée voulait déménager et, au milieu d'un malentendu sur le paiement du loyer, le défendeur est entré dans l'immeuble et a frappé la victime, le défendeur étant reconnu coupable de violation de domicile.

[1373] Dans une autre opinion (S. Bogdan, D.A. Șerban, *op. cit.,* p.421) une loi Ferenda est proposée afin de changer la violation du domicile du Code pénal, pour ne pas être un délit contre la personne, mais un délit contre l'ordre public.

[1374] M. Udroiu, *Fișe de drept penal. Partea specială*, București, Universul Juridic, 2014., p.377.

violation du domicile de plusieurs personnes est commise dans la même circonstance, par rapport au temps, au lieu et à la manière de commettre l'acte d'exécution.

Il est à noter que pour retenir un délit, il n'est pas nécessaire que le sujet passif soit à son domicile, la loi n'imposant pas une telle condition.

477. Entrée/refus de quitter le domicile. En ce qui concerne l'élément matériel, nous constatons qu'il prend la forme à la fois d'une action-pénétration dans le foyer et d'une inaction-refus de quitter le foyer, constituant un délit au contenu alternatif. Si l'auteur du délit commet les deux façons de commettre le délit sur la même personne, nous retiendrons une seule infraction de violation de domicile. Par « pénétration », nous entendons l'action de l'entrée physique, effective dans la maison, la chambre, la dépendance ou l'endroit clôturé qui lui est rattaché, avec tout le corps. Si la manière dont il est pénétré correspond au contenu constitutif d'un autre délit (par exemple, pour entrer dans un appartement, l'auteur frappe à poing le locataire), alors nous retiendrons un concours d'infractions entre la violation de domicile et l'acte concret commis.

Il y a deux autres conditions dans le cas de sa pénétration, outre son effectivité : avoir lieu sans droit et sans consentement. Quant à la première, nous comprenons que la pénétration se produit sans autorisation. On peut parler de pénétration sans droit même lorsque la personne qui effectue l'acte d'exécution aurait le droit d'entrer (par exemple, le propriétaire de l'appartement loué), mais abuse du droit qu'il a. Il y a des situations où l'entrée dans le domicile se fait avec droit, comme dans le cas d'un mandat de perquisition, d'un mandat pour la fouille domiciliaire, etc., lorsque l'existence du consentement de la personne lésée n'est plus requise et que l'acte de violation du domicile ne constituera pas un délit, en manquant la typicalité objective de l'acte concret. En ce qui concerne la deuxième condition - l'absence de consentement de la personne lésée, nous faisons référence au fait que la personne lésée n'a pas donné son consentement, exprès ou tacite, concernant la pénétration. Si, toutefois, le consentement de la victime existe, il est nécessaire qu'il soit valablement exprimé, même si le consentement d'une des personnes vivant dans cet espace est suffisant (s'il y a plusieurs locataires). Il peut également y avoir des situations où le consentement de la personne lésée existe, mais la pénétration est toujours un délit (par exemple, lorsque l'auteur, voisin de la personne blessée, a son consentement pour entrer dans une pièce et que l'auteur néglige la permission donnée et entre dans toutes les pièces de l'appartement).

a). Nouvelles méthodes de violation de domicile dans le contexte du développement technologique.

478. En cas de violation du domicile par l'action de la pénétration, on peut également mettre en évidence les méthodes d'entrée dans un espace de vie à l'aide des nouvelles technologies. Dans ce contexte, pour la prévention des violations de domicile, il existe certains dispositifs IoT (Internet of Things)[1375], conçus précisément pour protéger le droit à l'inviolabilité du domicile. Par exemple, de tels dispositifs IoT sont des caméras de surveillance, des serrures intelligentes, des systèmes d'alarme, etc., ceux-ci étant souvent capables de communiquer entre eux, mais aussi avec l'usager[1376]. De plus, en ce qui concerne les serrures intelligentes, la sécurité qu'elles apportent est obtenue grâce à plusieurs technologies : balayage du dessin papillaire au moyen d'un capteur d'empreintes digitales, balayage de l'iris ou même via une connexion Bluetooth, dans ce dernier cas, la serrure communique avec le téléphone portable pour ouvrir automatiquement la porte lorsque l'appareil mobile est suffisamment proche, ce qui rend plus pratique d'entrer dans la maison.

Compte tenu de l'évolution des nouvelles technologies qui se trouvent souvent dans les foyers, les agresseurs ont évolué à cet égard, trouvant de nouveaux moyens d'entrer dans un foyer, sans le droit et sans le consentement de la personne qui utilise le domicile. Ainsi, la destruction effective des dispositifs susmentionnés n'est plus utilisée, mais, par exemple, le compromis du logiciel sur lequel ils sont basés, de sorte qu'ils ne sont plus fonctionnels. Il est également possible d'intercepter les communications que les appareils intelligents font par le réseau Wi-Fi ou Bluetooth, en capturant et déchiffrant ces communications, ce qui permet la manipulation des caméras de surveillance, des systèmes d'alarme, des serrures intelligentes, etc. Enfin et surtout, comme une dernière méthode de violation du domicile en utilisant les nouvelles technologies, nous pourrions également remettre en question la possibilité d'exploiter les vulnérabilités logicielles que de nombreux appareils intelligents ont, en corrompant le système d'exploitation sur lequel l'appareil intelligent est basé, afin de prendre le contrôle de l'objet intelligent pour sa manipulation, nécessaire pour l'entrée non autorisée dans la maison.

[1375] Les appareils IoT sont généralement des objets physiques qui contiennent divers composants technologiques et logiciels et sont connectés à Internet via le routeur Wi-Fi situé dans la maison, dont beaucoup sont capables de collecter et de communiquer des données. Les appareils IoT peuvent être des réfrigérateurs intelligents, des thermostats intelligents

[1376] Par exemple, nous pouvons imaginer la situation où une maison bénéficie à la fois de caméras de surveillance et de portes équipées de serrures intelligentes. Si les caméras de surveillance détectent une présence humaine inhabituelle à l'intérieur de la cour - par exemple, une personne dont le portrait facial n'a pas été enregistré, elles communiquent un message sur le téléphone de l'utilisateur avec les enregistrements vidéo de la présence de la personne inconnue dans la maison, afin que l'utilisateur puisse agir directement sur les serrures intelligentes, bloquant ainsi les portes et l'accès à la maison. Il est possible que les caméras communiquent directement avec les serrures immédiatement après avoir averti le suspect, l'utilisateur n'étant plus directement impliqué.

479. Refus de quitter le domicile, forme continue de l'infraction. La deuxième façon de commettre une violation du domicile consiste à refuser de quitter le domicile. Pour avoir cette façon de commettre, la présence préalable de l'auteur dans le domicile de la victime[1377] est nécessaire, suivie d'une demande expresse de la part de la victime (soit le propriétaire du logement ou une autre personne utilisant le domicile) de quitter le domicile, une demande que l'auteur refuse (expressément - verbalement ou implicitement en ne quittant pas le domicile). Tout comme dans le cas d'entrée, outre l'absence de consentement, le refus de quitter le domicile doit être fait sans droit et s'il y a un tel droit reconnu par la loi, l'acte ne constituera pas un délit en l'absence de la typicalité objective de l'acte.

La conséquence immédiate de l'acte est la réalisation de l'inviolabilité du domicile, qui se produit presque en même temps que l'acte d'exécution, le présent délit étant un danger abstrait.

En ce qui concerne le lien de causalité, puisque la violation du domicile est un acte de danger abstrait, le dommage est présumé et le lien de causalité découle de la commission même de l'élément matériel de l'acte (*ex re*).

480. Culpabilité directe ou indirecte. Sur le côté subjectif, la forme de culpabilité avec laquelle l'acte peut être commis est intentionnelle, directe ou indirecte. Par conséquent, la violation du domicile n'est pas criminalisée, et le motif et le but ne sont pas pertinents pour l'existence du délit, pouvant les prendre en compte comme une éventuelle individualisation de la peine. L'acte est commis avec une intention directe lorsque le sujet actif vise précisément à porter atteinte à l'inviolabilité du domicile et est commis avec une intention indirecte lorsque seul le préjudice à la valeur sociale susmentionnée[1378] est accepté. Si l'auteur pénètre par inadvertance dans le logement, l'erreur peut être retenue comme une cause qui élimine la culpabilité de l'acte commis.

481. Non-incrimination de la tentative et de la préparation de l'acte. Les actes de préparation et de tentative, bien que possibles dans l'hypothèse de la pénétration, ne sont pas incriminés et donc non punissables. En cas de refus de quitter le domicile, les actes de préparation et de tentative sont impossibles, puisqu'il s'agit d'une omission propre, qui est commise par sa nature à travers une inaction. Étant donné que le délit de violation du domicile

[1377] Nous pensons que cette présence de l'auteur dans la zone où vit la victime doit être légale pour conserver exclusivement le refus de quitter le domicile, puisque, s'il est illicite, la première variante alternative de ce délit serait conservée : la pénétration. Dans une telle situation, il n'y aura qu'un seul délit de violation du domicile, commis par les deux voies normatives.

[1378] En règle générale, cela se produit lorsque l'auteur poursuit un autre résultat, lorsque la violation de domicile est un délit- moyen, comme dans le cas où le propriétaire entre dans l'appartement loué pour demander au locataire un loyer impayé.

est un danger abstrait, la consommation a lieu au moment de la réalisation de l'élément matériel, c'est-à-dire que l'acte est consommé au moment de l'entrée/refus de quitter la maison, la chambre, la dépendance ou l'endroit clôturé qui lui est rattaché.

En même temps, dans la manière de refuser de quitter le domicile, la doctrine[1379] a apprécié que la violation du domicile prenne une forme continue de l'infraction, l'acte étant consommé à partir du moment du refus de quitter et est épuisé en quittant le logement.

482. Commettre un délit avec une arme. En plus de la forme de base de la violation du domicile prévue à l'alinéa (1er) de l'art. 224 du Code pénal, il existe également une variante aggravée de ce délit, prévue au paragraphe (2), qui a le contenu suivant : « *Si l'acte est commis par une personne armée, pendant la nuit ou en utilisant de fausses qualités, la peine est l'emprisonnement de 6 mois à 3 ans ou une amende* ».

Dans le cas d'une personne armée commettant l'acte, nous comprenons que le sujet actif doit avoir violé la résidence de la victime en ayant une arme à feu sur lui. Par la notion « d'arme à feu », il faut comprendre les armes elles-mêmes et les armes assimilées, telles qu'elles sont définies par l'art. 179 du Code pénal[1380]. En ce qui concerne les armes elles-mêmes, il n'est pas nécessaire qu'elles aient été effectivement utilisées ou que le sujet passif ait observé l'arme, mais il suffit que l'auteur de l'infraction la porte sur lui. Toutefois, dans le cas d'armes assimilées, il est nécessaire que l'arme ait été effectivement utilisée pour commettre l'acte (soit sur la victime ou sur d'autres obstacles à la commission de l'acte), afin de respecter l'exigence imposée par l'article 179 alinéa (2) du Code pénal - avoir été utilisées pour une attaque. Nous mentionnons aussi qu'il s'agit d'une circonstance réelle, donc elle s'applique également aux participants dans la mesure où ils la connaissaient ou l'avaient prévue.

483. Commettre un délit pendant la nuit. En cas de violation du domicile commis la nuit, il est nécessaire de consommer l'acte lorsque la nuit remplace le jour, l'organe judiciaire utilisant le critère astronomique pour la vérification. Si l'acte se déroule dans le temps, l'aggravation sera retenue lorsque même une partie de l'acte est commise la nuit. Par exemple, si l'auteur entre sans droit et sans le consentement de la victime dans son appartement à 14h00

[1379] M. Udroiu, vol. I *op. cit*., p.386.

[1380] Selon l'art. 179, alinéa (1er) du Code pénal, les armes elles-mêmes sont « *les instruments, les dispositifs ou les parties déclarés comme telles par des dispositions légales* ». A cet égard, la loi no 295/2004 sur le régime des armes et munitions - parue dans le M. Of no 425 du 10 juin 2014 - définit le terme « arme » à l'art. 2 point I.1 de la loi susmentionnée comme étant « *tout objet ou dispositif dont le fonctionnement provoque un ou plusieurs projectiles, des substances explosives, enflammées ou brillantes, des mélanges incendiaires ou la dispersion de gaz nocifs, irritants ou neutralisants, dans la mesure où il se trouve dans l'une des catégories définies à l'annexe* ». De plus, la loi distingue plusieurs types d'armes proprement-dites : les armes à feu, les armes prohibées, létales, non létales, mortelles, etc. Par arme assimilée nous entendons, selon l'art. 179 par. (2) Code pénal, « *tout autre objet pouvant servir d'arme et qui a été utilisé pour une attaque* », comme par exemple un couteau de cuisine, un morceau de bois, une brique, etc.

et refuse de quitter le bâtiment, et qu'il reste jusqu'à 2h00, après quoi il quitte le bâtiment, l'acte est commis pendant la nuit.

484. Commettre un délit en utilisant de fausses qualités. En ce qui concerne la dernière variante aggravée, à savoir commettre l'acte en utilisant de fausses qualités, se réfère à l'utilisation d'une certaine qualité fausse, que l'auteur ne possède pas réellement (par exemple, une personne se fait passer pour un procureur afin de procéder à une perquisition domiciliaire, auquel cas nous retiendrons un concours entre la violation du domicile et l'usurpation des qualités officielles). Toutefois, si le sujet actif a cette qualité invoquée et l'utilise illégalement pour entrer ou rester dans le logement de la victime, l'acte commis constituera un abus de fonction (par exemple, la personne utilise sa capacité de procureur pour effectuer une perquisition domiciliaire sans avoir obtenu un mandat de perquisition délivré par le juge des droits et libertés). Il n'est pas nécessaire que la fausse qualité utilisée soit officielle, mais elle peut aussi être informelle, comme celle du membre de famille, du voisin, du représentant de l'entreprise de téléphonie mobile et d'internet, etc.

485. Sanction pénale pour le délit de violation de domicile. En ce qui concerne le régime de sanction, sous la forme de base prévue à l'alinéa (1er) de l'art. 224 du Code pénal, la violation du domicile est punissable d'une peine de prison de 3 mois à 2 ans ou d'une amende, alors que pour forme aggravée de l'alinéa (2) du même article, la peine est l'emprisonnement de 6 mois à 3 ans ou une amende. Sur le plan procédural, l'action pénale en cas de violation du domicile est engagée sur plainte préalable de la personne lésée.

B. Violation du siège professionnel

486. Infraction similaire à la violation de domicile. Le délit de violation du siège professionnel, un fait incriminé à l'art. 225 du Code pénal, comporte, également à la violation du domicile, trois paragraphes, où la méthode réglementaire est identique : l'alinéa (1er) est la forme - type, l'alinéa (2) est la forme aggravée, et à l'alinéa (3), il est précisé la question du déclenchement de l'action pénale.

La violation du siège professionnel est un délit qui peut être vu dans « le miroir », par rapport à la violation de domicile, car il y a des incriminations très proches comme contenu. Cependant, il existe des différences importantes entre les deux. C'est pourquoi, dans cette section, nous ne ferons pas une analyse approfondie du délit, car la plupart des aspects analysés lors de la violation du domicile sont également applicables à la violation du siège professionnel. Ce que nous réaliserons, cependant, sera une analyse ponctuelle sur les questions avec lesquelles la criminalisation est distancée de l'art. 225 du Code pénal par rapport à l'art. 224.

487. Objet juridique. La raison de la criminalisation de ce fait repose sur une lacune législative de l'ancien Code pénal de 1968, qui prévoyait comme délit uniquement la violation du domicile, où la notion de « domicile » n'incluait pas le siège des personnes morales/physiques.

488. De domicile à domicile professionnel : extension de la protection pénale. L'objet juridique de ce délit est donné par les relations sociales sur l'inviolabilité des locaux de la personne morale/physique où elle exerce son activité professionnelle ou, en d'autres termes, l'objet juridique prend en compte la protection de la vie privée de la société. Nous considérons également que cette infraction protège aussi les locaux des entités sans personnalité juridique, c'est-à-dire les locaux de ces personnes morales sans but lucratif[1381]. Ainsi, bien que la violation du siège professionnel ne protège directement que le droit de l'entité à l'inviolabilité du siège professionnel (ce qui est facile à remarquer même de la norme de criminalisation), nous croyons que le droit de la personne physique à la vie privée au lieu de travail est également défendu indirectement, c'est-à-dire, l'intimité au lieu travail (sans constituer un objet juridique secondaire), étant donné que la protection de l'inviolabilité du siège dans l'art. 225 est un concept plus large qui englobe également la protection de l'activité effectuée par les personnes travaillant dans cet établissement.

Il est également rappelé dans la doctrine[1382] que, dans la jurisprudence de la Cour européenne des droits de l'homme, la notion de « domicile », en tant qu'élément de la vie privée protégé par les dispositions de l'article 8 de la Convention, est interprétée de façon extensive par la Cour, englobant également les sièges des personnes morales, physiques ou d'autres entités.

489. Définition de la notion de secret professionnel. Par la notion de « siège professionnel », nous entendons le lieu où une personne morale, une personne physique ou une entité sans personnalité juridique exerce son activité, pouvant distinguer les établissements principaux et secondaires. Ils sont donc protégés par l'art. 225 du Code pénal seulement les établissements où la vie privée de l'entreprise est effectivement réalisée - par exemple, une succursale bancaire, un siège social, un immeuble de bureaux, etc. Si l'activité de l'entreprise n'est pas exploitée dans cet espace, ce lieu n'est pas protégé par le droit pénal (par exemple, si l'espace de bureau d'une entreprise est utilisé comme entrepôt).

Il convient également de noter que dans l'art. 225 du Code pénal, il n'est pas fait référence aux espaces clôturés qui sont liés ou non au siège professionnel - par exemple, la cour

[1381] Dans le même sens, A.-R. Trandafir, „*Violarea sediului profesional. Obiectul protecției. Comparație cu violarea de domiciliu*", dans les Annales Scientifiques de l'Université „Alexandru Ioan Cuza" de Iasi, Tome LXVII/2, Sciences juridiques, 2021. p.165.
[1382] A.R. Trandafir, *op. cit*., p. 163.

d'une entreprise, parce que, comme le met en évidence la doctrine[1383], l'entité juridique n'exerce pas son activité dans l'espace clôturé du siège. La réglementation de l'art. 225 du Code pénal vise à protéger la vie privée de la personne morale dans l'endroit où elle pourrait être lésée, c'est-à-dire son siège.

490. Sujet passif. Divulgation du secret professionnel : qui est la victime ? L'objet passif de la violation du siège professionnel est la personne morale, la personne physique ou l'entité sans personnalité juridique elle-même (association, fondation, etc.) exerçant son activité dans cet établissement. Pour être un sujet passif, l'entité en question doit avoir en usage l'espace où elle exerce ses activités et avoir le pouvoir d'y autoriser ou de refuser l'entrée ou la présence. Ainsi, il s'ensuit que l'entité n'est pas tenue d'être propriétaire de cet espace, étant suffisant pour l'avoir en usage afin de bénéficier de la protection du droit pénal, ni qu'il soit nécessaire que l'usage existe sur la base d'un titre.

Comme je l'ai mentionné précédemment, bien que la loi ne le stipule pas expressément, nous devons considérer comme un sujet passif de ce délit aussi les entités juridiques, les personnes morales à but non lucratif. Aussi, en ce qui concerne la personne physique qui mène son activité dans un établissement, nous ne faisons pas référence, par exemple, aux employés d'une société, mais à certaines formes d'organisation d'une activité ou profession, telles que les bureaux de notaires, avocats, offices d'huissiers de justice, médiateurs, mais aussi les personnes physiques autorisées (PFA) et bien d'autres. En outre, il n'est pas important de retenir l'infraction si elle est commise contre une entité publique ou privée.

§2. CONTREFAÇON INFORMATIQUE DANS LE CONTEXTE DU DÉLIT D'ATTEINTE À LA VIE PRIVÉE

491. Manipulation illicite de données numériques, falsification informatique. Bien qu'à première vue il semble que les deux délits soient complètement différents, nous comprenons de faire une brève analyse comparative entre les deux, à la lumière de la décision no. 4/2021 de la Haute Cour de cassation et de justice, par laquelle la question de la classification juridique d'un fait qui est apparemment lié à l'atteinte à la vie privée a été réglée et qui a énoncé essentiellement que « l'acte d'ouvrir et d'utiliser un compte sur un réseau social ouvert au public, en utilisant comme nom d'utilisateur du nom d'une autre personne et en saisissant de données personnelles réelles permettant son identification, répond à deux des exigences essentielles du délit de fausse informatique stipulées à l'article 325 du Code pénal, à savoir que

[1383] S. Bogdan, D.A. Șerban*, Drept penal. Partea specială,* Universul Juridic, 2022*,* p.429.

l'action d'introduction de données informatiques doit être effectuée sans droit et que l'action d'introduction de données informatiques aboutit à des données erronées de la vérité »[1384].

Fondamentalement, ce qui est poursuivi dans cette analyse fait référence à la façon dont l'action liée à l'élément matériel du côté objectif de la cybercriminalité peut être trouvée dans le côté objectif du délit d'atteinte à la vie privée

Pour commencer, nous notons que l'infraction de cybercriminalité se trouve dans le Code pénal au titre VI – Infractions de contrefaçon, à l'article 325 et comporte le contenu suivant : « l'acte d'entrer, modifier ou supprimer, sans droit, des données informatiques ou restreindre, sans droit, l'accès à de telles données, entraînant des données qui sont inadéquates à la vérité, afin d'être utilisées pour produire une conséquence juridique constitue un délit et est punissable d'un emprisonnement de un à cinq ans ».

492. Atteintes à la vie privée. D'autre part, l'infraction d'atteinte à la vie privée se trouve dans le Code pénal au titre I, chapitre IX – Infractions touchant le domicile et la vie privée, à l'article 226 et qui, essentiellement, concerne « l'atteinte à la vie privée, sans droit, par la photographie, captage ou enregistrement des images, ou écouter par des moyens techniques, ou enregistrer le son d'une personne dans un logement ou une pièce ou dépendance ou encore d'une conversation privée ». En outre, un autre paragraphe de l'article 226 qui est pertinent dans notre analyse se réfère à « la divulgation, la diffusion, la présentation ou la transmission, par quelque moyen que ce soit, d'une image intime d'une personne identifiée ou identifiable par les informations fournies, sans le consentement de la personne montrée, susceptible de lui causer une détresse mentale ou un préjudice à son image » et la définition de l'image intime, qui est « toute reproduction, quel que soit le support, de l'image d'une personne nue, qui expose totalement ou partiellement ses organes génitaux, son anus ou sa zone pubienne, ou dans le cas d'une femme, ses seins, ou qui est impliquée dans une relation sexuelle ou un acte sexuel ».

493. Délit de falsification informatique ou délit d'atteinte à la vie privée. Considérant que la situation présentée à titre d'exemple, à savoir « l'acte d'ouverture et d'utilisation d'un compte sur un réseau social ouvert au public, en utilisant comme nom d'utilisateur le nom d'une autre personne et en saisissant des données personnelles réelles permettant son identification », a donné lieu à des débats et à des controverses dans la jurisprudence, les tribunaux interprétant différemment la classification juridique de ce fait, nous devons préciser que la décision no 639/Ap du 26.09.2019 prononcée par la Cour d'appel de Brasov a été le fondement de la saisine de la Haute Cour de cassation et de justice. En bref, pour cette situation de fait, le tribunal a

[1384] *Arrêté no. 4 du 25 janvier 2021*, Haute Cour de Cassation et Justice.

ordonné le changement du classement juridique des infractions d'atteinte à la vie privée et de falsification d'information dans le délit d'atteinte à la vie privée

Dans ce qui suit, nous voulons présenter une brève analyse des deux délits, afin de voir comment les éléments matériels du côté objectif s'entremêlent. Tout d'abord, si nous faisons référence au délit de contrefaçon informatique, il convient de mentionner qu'il n'avait pas de correspondant dans l'ancien Code pénal, le contenu de l'infraction étant pris de la loi 161/2003 dans son intégralité de la loi 161/2003.

L'objet juridique de ce délit consiste dans les relations sociales dont la formation et le comportement sont basés sur la confiance du public dans la véracité des systèmes d'information, dans tout le processus moderne de stockage et de traitement automatique dans l'intérêt public ou privé. Selon la doctrine, la défense de l'intégrité et de l'authenticité des données informatiques est actuellement nécessaire, car elles ont acquis un rôle important dans la société[1385].

L'essence de l'analyse de ce chapitre se réfère au côté objectif du délit de contrefaçon informatique, de sorte que nous montrons que son élément matériel peut être atteint en saisissant des données informatiques, en modifiant les données informatiques en altérant ou en modifiant son contenu, « supprimant des données informatiques et restreignant l'accès aux données informatiques », à condition qu'elles soient effectuées sans droit. Comme on peut le voir, il s'ensuit que le législateur a prévu pour l'appréhension de la commission de cette infraction l'accomplissement de deux conditions essentielles[1386]: la première étant que toute action exercée soit effectuée « sans droit », expression expliquée à l'article 35 (2) de la loi no 161/2003. La deuxième exigence expressément stipulée est que le résultat du délit soit des données informatiques qui ne correspondent pas à la vérité.

494. Dans le même esprit que les aspects mentionnés ci-dessus, l'infraction d'atteinte à la vie privée est également une nouvelle criminalisation, sans avoir une disposition similaire dans l'ancien Code pénal ou dans toute loi spéciale. Le but de ce règlement était de combler un vide législatif, la disposition juridique « complétant le cadre de la protection pénale des valeurs garanties par l'article 8 de la Convention européenne des droits de l'homme »[1387].

L'objet juridique le représente les relations sociales qui sous-tendent le droit de la personne à voir sa vie privée respectée, ayant comme référence la notion de vie privée, analysée à la lumière de l'article 8 de la Convention européenne des droits de l'homme. Selon la doctrine spécialisée, par la criminalisation prévue à l'art. 226 du Code pénal, « deux objectifs

[1385] G. Antoniu, T. Toader, *Explicațiile Noului Cod Penal*, vol. IV, Universul Juridic, 2016. p.547.
[1386] Ibidem., p.549.
[1387] Exposition des raisons du nouveau Code pénal, p. 43

ponctuels étaient poursuivis : le droit de la personne à sa propre image et la confidentialité des conversations privées »[1388].

Afin de délimiter l'aspect objectif du délit d'atteinte à la vie privée, le législateur a prévu diverses actions alternatives, en fonction de la variante type ou des variantes dérivées des paragraphes 2 et 3 de l'art. 226 du Code pénal, le point essentiel étant que l'atteinte à la vie privée s'effectue sans droit, c'est-à-dire sans autorisation valable ou consentement exprimé par la personne dont la vie privée est restreinte.

Rappelant la demande adressée par la Cour d'appel de Brasov à la Haute Cour, nous signalons qu'elle met en cause un élément très pertinent de la pratique judiciaire non unitaire : d'une part, il a été noté que « l'acte d'ouverture et d'utilisation d'un compte sur un réseau social ouvert au public (réseau qui n'exige pas de preuve pour montrer l'utilisation du vrai nom par le titulaire du compte), en fournissant comme nom d'utilisateur le nom d'une autre personne et en saisissant des données réelles ciblant cette personne (informations, photos, images vidéo, etc.) ne réalise pas les conditions typiques de contrefaçon informatique prévu par l'art. 325 du Code pénal » (décision no 234/03.06.2020 prononcée par la Cour d'appel de Brasov). D'autre part, à l'opposé de cet avis, dans la vue majoritaire, le même acte réalise le contenu du délit de contrefaçon informatique, un acte stipulé et sanctionné par l'art. 325 du Code pénal (décision no. 8/A/2010 du 26/01/2010, prononcée par la Cour d'appel de Cluj).

495. Analyse des conditions de typicité. La Haute Cour note[1389] que « l'analyse en l'espèce est circonstancielle à la situation lorsque l'auteur introduit, en créant un compte dans un réseau social ouvert au public, le nom et les données personnelles réelles d'une autre personne (données permettant l'identification - informations, photos, images vidéo) sans son consentement. La question de droit vise à répondre ou non à deux des exigences essentielles attachées à l'élément matériel du côté objectif du délit de contrefaçon informatique, celles que l'acte soit commis sans droit et qu'il en résulte des données inappropriées à la vérité. »

Ensuite, dans les considérants de la décision, la Haute Cour fait référence aux instruments juridiques internationaux qui ont constitué le fondement de la criminalisation du délit de contrefaçon informatique, à savoir l'article 7 de la Convention du Conseil de l'Europe sur la cybercriminalité[1390].

496. La falsification informatique : parallèle avec les falsifications classiques dans les écrits. Selon la Haute Cour, « en criminalisant le délit de contrefaçon informatique, il a été essayé à créer un délit parallèle avec les délits traditionnels de falsification dans des

[1388] V. Cioclei, *Drept penal. Partea Specială I. Infracțiuni contra persoanei și infracțiuni contra patrimoniului*, 2e éd., C.H.Beck, București, 2017, p.227.
[1389] *Décision no. 4 du 25.01.2021* de l'Haute cour de cassation et justice
[1390] Convention adoptée à Budapest en date d 23 novembre 2001, ratifiée par la *loi no. 64/2004*.

documents », une idée soutenue par l'approche doctrinale selon laquelle la façon dont les données d'information sont saisies correspond, en principe, à la falsification d'un document et la modification, l'effacement, la restriction de l'accès aux données informatiques correspondent au concept d'altération d'un document numérique »[1391]. Ainsi, une première conclusion, en termes des éléments typiques qui sont analysés dans ce cas, est que la réglementation nationale du délit de contrefaçon informatique a correspondant dans les dispositions de l'article 7 de la Convention du Conseil de l'Europe sur la cybercriminalité, en ce qui concerne « l'acte à commettre sans droit et avoir comme résultat des données inadéquates vérité ».

A. Saisie non autorisée de données pour créer un compte sur les réseaux sociaux

497. ICCJ : usurpation d'identité sur les réseaux sociaux. Dans les considérants de la décision, la Haute Cour examine tout d'abord la condition selon laquelle la saisie des données doit être effectuée sans droit, en se référant à la personne qui a le droit de fournir ces données et à l'existence ou non de la manifestation de sa volonté ; « Dans le cas présent, l'auteur qui crée un compte/profil sur un réseau social ouvert au public en saisissant le nom réel et les données personnelles d'une autre personne et en permettant son identification (informations, photographies, images vidéo, etc.) comme des données relatives à soi-même, agit en violation de la manifestation de volonté de la personne dont l'identité l'a usurpée. Les informations saisies lors de la création du compte et celles contenues dans divers publications sont circonscrites à la définition donnée par l'article 181(2) du Code pénal, étant des représentations qui peuvent être traitées par le système informatique. Ces données informatiques sont saisies sans droit, au sens des dispositions de l'article 35 (2) lettre a) de la loi no 161/2003, selon lesquelles la personne qui n'est pas autorisée, en vertu de la loi ou d'un contrat, agit sans droit »[1392].

B. Falsification de la manifestation de la volonté du véritable détenteur

498. Création d'un compte sans droit avec l'identité d'une autre personne. Deuxièmement, on s'est demandé si l'introduction de données informatiques dont les résultats ne sont pas appropriés à la vérité peut être considérée comme accomplie, si l'identité de la personne est réelle, ce qui signifie qu'aucun changement n'a été apporté aux aspects réels de

[1391] S. Bogdan, D. A. Şerban, G. Zlati, *Noul Cod penal, Partea specială, Analize, explicaţii, comentarii*, *Perspectiva clujeană*, Ed. Universul Juridic, Bucureşti, 2014. p.559.
[1392] *Décision no. 4 du 25.01.2021* de l'Haute cour de cassation et justice

son identité. La Cour a ainsi noté que « la création d'un compte sans droit, usurpant l'identité d'une personne, en saisissant des données réelles et en permettant l'identification de cette personne, suppose une falsification de la manifestation de sa volonté et crée une perception contraire à la réalité concernant le titulaire de ce compte (…), par exemple, en saisissant dans un réseau social ouvert au public le nom et d'autres données personnelles réelles d'une autre personne et en permettant son identification, comme s'il s'agissait des données sur sa propre identité, il résulte des données impropres à la vérité au sens de l'article 325 du Code pénal, étant satisfait à cette exigence liée à l'élément matériel du côté objectif du délit de contrefaçon informatique[1393] ».

Même si, à première vue, nous apprécierions que « l'acte d'ouverture et d'utilisation d'un compte sur un réseau social ouvert au public en fournissant comme nom d'utilisateur le nom d'une autre personne et en saisissant des données réelles concernant cette personne (informations, photos, images vidéo, etc.), ne réunit pas les conditions typiques du délit de contrefaçon informatique, prévu à l'art. 325 du Code pénal », constitue une atteinte réelle à la vie privée, tel que retenu à l'art. 226 du Code pénal, suite à l'analyse de la décision no. 4/2021, nous rejoignons les considérations et arguments de la Haute Cour, considérant que dans la manière présentée précédemment « l'acte d'ouverture et d'utilisation d'un compte sur un réseau social ouvert au public, en utilisant comme nom d'utilisateur le nom d'une autre personne et en saisissant des données personnelles réelles qui permettent son identification, répond à deux des exigences essentielles du délit de contrefaçon informatique stipulé à l'article 325 du Code pénal, à savoir que l'action de saisie de données informatiques doit être effectuée sans droit et que l'action de saisie de données informatiques aboutit à des données erronées de la vérité »[1394].

Conclusion du chapitre 1

Les infractions classiques qui protègent le domicile et la correspondance sont restées opérationnelles en tant que mécanismes de garantie de la sphère privée, structurées dès l'époque des codifications napoléoniennes, puis adaptées aux exigences contemporaines de légalité, de nécessité et de proportionnalité. Les infractions exposées dans ce chapitre constituent le pilier « analogique » de la vie privée, mais elles acquièrent leur actualité grâce aux extensions numériques : les données et l'identité en ligne sont traitées comme des espaces protégés, et les intrusions, qu'elles soient physiques ou informationnelles, doivent être évaluées de manière unitaire. Les éléments traditionnels tels que l'espace (domicile/lieu de travail), le canal de

[1393] Idem
[1394] *Décision no. 4 du 25.01.2021* de l'Haute cour de cassation et justice

communication (lettres, messages), les relations protégées (avocat-client), le statut social (honneur/réputation) sont, du point de vue du droit pénal, étroitement liés à l'environnement numérique. Les infractions commises à l'encontre des données et de l'identité présentent les caractéristiques suivantes : elles protègent l'information en tant que telle (collecte, stockage, traitement, divulgation), les moyens informatiques (accès, interception, altération) et le profil/l'identité en ligne (utilisation de données pour de faux comptes, falsification du consentement). Concrètement, les éléments traditionnels mentionnés ci-dessus sont protégés par des normes qui protègent le lieu où vous vivez ou travaillez - « où » - ou par celles qui concernent « comment » vous communiquez. Les éléments numériques concernent « ce que vous êtes en tant qu'information » et « comment circulent les données privées ».

La protection de la réputation suit toutefois une trajectoire normative distincte, consacrée principalement par le régime des délits de presse et des atteintes à l'honneur. Contrairement au droit français, dans le droit pénal roumain, la protection de la personnalité humaine s'effectue principalement par des voies extrapénales, la diffamation n'étant pas incriminée en tant que telle, l'accent étant mis sur la réparation du préjudice et l'équilibre avec la liberté d'expression. La calomnie et l'insulte ont été réglementées pour la première fois dans le droit roumain dans le Code pénal de 1864, dans la section consacrée aux crimes et délits contre la personne, puis reprises dans le Chapitre « Délits contre l'honneur » du Code pénal entré en vigueur en 1936. Même le Code pénal entré en vigueur sous le régime communiste (1969) a maintenu le caractère pénal de l'insulte et de la diffamation, mais la réforme pénale concrétisée par le nouveau Code pénal entré en vigueur le 1er février 2014 a rompu cette continuité, le législateur ayant choisi de ne plus les inclure comme infractions autonomes.

Chapitre 2
L'ANALYSE DE L'INFRACTION D'ATTEINTE À LA VIE PRIVÉE

Introduction

499. La vie privée dans la variable de la politique pénale. Un sujet de recherche aussi généreux nécessite une approche harmonieuse et élaborée, conditionnée par le besoin d'un rapport cohérent à l'ensemble phénoménologique actuel, afin que ses connaissances ne soient pas fragmentées. À ce titre, nous souhaitons dans ce chapitre attirer l'attention, par un regard comparatif, sur les moyens de protection du droit à la vie privée, dans le contexte de la criminalisation de l'acte d'atteinte à la vie privée dans la législation française et roumaine.

Un premier aspect jugé essentiel à mentionner est que, dans la perspective universelle du respect des libertés et droits fondamentaux de l'homme, la protection de la vie privée est identifiée dans la culture de l'État qui la coordonne[1395]. Ainsi, nous apprécions que, bien que la reconnaissance de l'existence du droit à la protection de la vie privée d'une personne soit indéniable, cependant, la manière dont elle est abordée varie selon les politiques pénales individuelles de l'État[1396].

Un deuxième aspect important à fixer est que, bien que le droit à la vie privée soit réglementé aussi bien en France qu'en Roumanie, tant selon les principes et normes imposés par la législation de l'Union Européenne, cependant, l'évolution législative des deux États a connu des moments, durées et contenus distincts[1397].

500. Similitudes et différences entre la France et la Roumanie. Ensuite, au cours de ce chapitre, nous aborderons les caractéristiques essentielles de la réglementation du délit d'atteinte à la vie privée, en référence aux dispositions en vigueur, à savoir les éléments prioritaires nécessaires pour une meilleure protection de la vie privée, en mettant en évidence les similitudes et les différences entre la législation pénale française et roumaine. Le présent

---

[1395] B. Garfield. *Privacy as a Cultural Phenomenon*, Journal of Media Critiques, vol.3, 2017. https://www.researchgate.net/publication/318678201_Privacy_as_a_Cultural_Phenomenon/citation/download

[1396] Nous sommes conscients qu'il faut faire deux commentaires au sujet des droits à la vie privée » : (1) le droit à la vie privée ne constitue pas un droit absolu ; et (2) les concepts de « vie privée » et de « respect de la vie privée » doivent être précisés pour devenir concrètement applicables. Ainsi, la législation sur les droits fondamentaux reconnaît que la vie privée ne peut être considérée comme une liberté absolue et est soumise à des limites lorsque les droits collectifs ou les besoins de la communauté l'exigent. Concernant l'essence « de la vie privée » – en tandem avec la nouvelle législation pénale analysée par cette recherche, nous pouvons comprendre que le droit à la vie privée implique la reconnaissance d'un espace protégé, où l'individu peut vivre sans pression extérieure, avoir garanti le respect et la dignité.

[1397] Nous mentionnons également qu'en France, le droit à la vie privée a été initialement consacré en 1970 par l'article 9 du code civil, sans prévoir de sanctions pénales, et que la protection explicite de la vie privée était réglementée par les articles 226-1 et suivants du Code pénal en 1994. En Roumanie, le droit à la vie privée a été introduit en 1991 par l'article 26 de la Constitution, protégeant la vie intime, familiale et privée en général, et la protection explicite de la vie privée était réglementée par les articles 226-227 du Code pénal de 2009, qui est entré en vigueur le 1er février 2014.

chapitre vise tout d'abord à déterminer comment chacun des deux systèmes juridiques a conceptualisé et criminalisé l'acte d'atteinte à la vie privée; et, deuxièmement, de mettre en lumière les stratégies législatives que chacun des deux États a utilisées pour s'adapter aux défis nés dans le domaine du numérique. Dans le même temps, l'analyse mettra en évidence le point de vue de la doctrine et de la jurisprudence pertinente, en mettant l'accent sur les solutions et les points de convergence.

Section 1. CADRE JURIDIQUE D'INCRIMINATION DE L'ATTEINTE À LA VIE PRIVÉE EN DROIT PÉNAL FRANÇAIS

501. Le droit au respect de la vie privée, garanti à chaque personne. Le but essentiel de la réglementation du délit d'atteinte à la vie privée[1398] est de garantir à chaque personne un environnement sûr pour l'exercice sans restriction des droits et libertés, de protéger les relations sociales privées, prévenir et combattre toute ingérence qui affecte ou est susceptible d'affecter les intérêts de la personne[1399].

Reconnaissant ses origines dans la jurisprudence civile[1400], le droit à la protection de la vie privée était défini par « le droit d'une personne de mener son existence selon ses propres désirs, avec un minimum d'ingérence extérieure »[1401]. Ainsi, en hommage au pouvoir créateur

[1398] Le terme « atteinte à la vie privée » a été utilisé vers 1890 et est défini par la loi comme une intrusion dans le droit d'être laissé tranquille, ce qui comprend l'intrusion dans la vie privée, l'utilisation du nom ou de l'image sans consentement, la divulgation publique de données privées, la publication de fausses informations sur une personne. https://legaldictionary.net/invasion-of-privacy/

[1399] En 2019, à la *Conférence internationale des commissaires pour la protection des données et de la vie privée* (CIDPPC), « *la résolution internationale sur la protection de la vie privée en tant que droit humain fondamental et condition préalable à l'exercice d'autres droits* » a été adoptée. Elle souligne l'importance de réglementer le délit d'atteinte à la vie privée. À ce jour, l'ICDPPC a changé son nom en *Global Privacy Assembly* (GPA) et s'occupe, en s'alignant à l'évolution de la technologie, des problèmes liés de la confidentialité et la protection des données. https://globalprivacyassembly.org/

[1400] J.C. Saint-Pau**,** *Art. 9, Fasc. 20 : Jouissance des droits civils. – Droit au respect de la vie privée. – Régime. Actions*, JurisClasseur Civil Code, Lexis 360 Intelligence, 2019. https://www-lexis360intelligence-fr.docelec.u-bordeaux.fr/encyclopedies/JurisClasseur_Civil_Code/CI0 TOCID/document/EN_KEJC-193171_0KRE

[1401] Bien qu'il ne connaisse pas encore une définition exacte, étant plutôt considéré comme un droit adaptable, le droit à la vie privée a été expliqué dans les décisions de la Cour d'appel de Paris comme « *le droit d'une personne de mener son existence selon ses propres désirs, avec un minimum d'interférence externe* ». Pour une meilleure caractérisation du droit, voir les arrêts de la Cour d'appel de Paris du 15 mai 1970, D. 1970, paragraphe 466, et RTD civ. de 1971, paragraphes 109 et 360 ; et la décision de la Cour d'appel de Paris du 5 décembre 1997 publiée dans Gazeta Pal. de 1998-1, paragraphe 234, affirmant que le droit à la vie privée concerne *« l'intimité de l'être humain dans ses divers aspects, notamment ceux liés à la vie familiale, à la vie sentimentale, à son image ou à son état de santé, qui doivent être respectés, car ils se rapportent à l'aspect le plus secret de la personne ».* Le contenu de la vie privée a été progressivement représenté dans la jurisprudence de l'époque comme reflétant le droit humain d'être protégé contre toute interférence liée de son nom, adresse, image, honneur, opinions, relations, y compris celles relatives à son décès. La jurisprudence ancienne était bien ancrée dans les réalités quotidiennes, puisqu'elle a reconnu que la divulgation publique de renseignements sur la situation financière, le mode de vie et la personnalité d'un artiste constitue une atteinte au droit à la vie privée. À cet égard, voir décision no 98-14.610 du 30 mai 2000, Bull. civ. I, no 167a de la Première Chambre civile de la Cour de cassation en France; et décision de la Première Chambre civile de la Cour de cassation en France no 13-21.929 du 5 février 2014. Cependant, la

de la jurisprudence civile[1402], la France a ouvert le cycle d'une protection pénale efficace en 1970[1403], lorsqu'elle a imposé pour la première fois un traitement punitif contre les comportements agressifs qui nuisent aux orientations, intérêts, préférences, activités professionnelles, relations sociales, choix de vie, résidence, correspondance, intimité de la personne[1404]. Ensuite, selon l'article 9 du Code civil[1405], l'action civile peut se poursuivre, avec certaines limitations, même après avoir obtenu un acquittement pénal[1406].

502. L'évolution de la protection du droit à la vie privée dans le droit pénal français. Depuis 2014, le Code pénal français a connu pas moins de 27 modifications substantielles de la forme fondamentale du délit[1407], en correspondance avec les articles 226-1 à 226-32. La préoccupation intense du législateur français pour la protection de la vie privée est notée dans la période 2023-2024, matérialisée par les rappels fréquents sur la loi. À cet égard, les spécialistes qualifient les changements législatifs de véritable réforme de la protection de la vie privée ; une réforme qui vise à répondre, en particulier, à l'émotion provoquée par la violence[1408]. Ils considèrent que, si le type d'actes violents est suffisamment clairement déterminé dans le plan législatif - juridictionnel, la réforme se concentre toutefois, à titre d'exemple, sur la nécessité d'assurer une protection plus efficace des mineurs, sur la relance d'un mouvement législatif visant à renforcer la protection des victimes de violence domestique[1409] contre les vulnérabilités et les lacunes des systèmes juridiques actuels[1410].

---

jurisprudence ancienne nous montre que les personnes morales ne bénéficiaient du même traitement privilégié de la personne physique.

[1402] Voir, à cet effet, l'avis de l'auteur R. Badinter, « *La protection de la vie privée contre l'écoute électronique clandestine »,* JCP 1971. p.2435, pt.1, dans lequel il présente comme justifié à l'époque el besoin de reconnaître la nécessité d'un droit effectif au respect de la vie privée, dans le contexte où la protection de la vie privée n'était initialement assurée que par le droit civil, à savoir par la jurisprudence civile.

[1403] Il s'agit de la *loi no 70-643 du 17 juillet 1970*, publiée au Journal officiel le 19 juillet 1970. Elle a introduit dans le droit français la protection de la vie privée, notamment par des modifications au Code civil (art. 9). Le 17 juillet 1970, le législateur français a introduit dans le Code pénal français les articles 368 et 369 qui punissent l'atteinte à la vie privée d'une personne, à savoir la conservation, la divulgation ou l'utilisation non autorisée de mots ou d'images obtenus illégalement. L'introduction de dispositions légales intervenait pour compléter la protection esquissée par d'autres règles existantes : violation de domicile, atteinte au secret professionnel, atteinte à la correspondance.

[1404] Voir l'opinion du spécialiste I. Lolies, *La protection pénale de la vie privée*, PUAM, 2ème partie, 1999. no. 202 et les suivants

[1405] J.-C. Saint-Pau, *L'article 9 du code civil : matrice des droits de la personnalité*. Dalloz, vol. 37, 1999. p.541. https://shs.hal.science/halshs-02205513v1

[1406] J. Pradel, *Procédure pénale*, Cujas, 18e éd., n° 1044, 2015.

[1407] Pour une image d'ensemble sur les effets produits, en général, par l'introduction d'une modification législative essentielle dans la vie privée de la personne, consulter l'œuvre de l'auteur J. Malherbe, „*La vie privée et le droit moderne*", Librairie du journal des notaires et des avocats ; Paris, 1968, pag.4.

[1408] Voir en ce sens les opinions des spécialistes J.-B. Perrier, F. Rousseau, „*Revue de droit science criminelle et de droit pénale comparé*", Lefebvre Dalloz, Doctrine 243, 2024. p.421 - 432.

[1409] À cet égard, il est fait référence à la modification bien accueillie des dispositions juridiques établissant que l'auteur ayant la capacité d'époux ou de partenaire de la victime domestique est plus sévèrement sanctionné, à savoir à partir d'un an d'emprisonnement, comme il était dans sa forme initiale, à deux ans d'emprisonnement.

[1410] Pour une analyse détaillée, nous recommandons à consulter l'opinion de l'auteur A. Denizot, „*Petites rectifications et grandes avancées en droit des victimes"*, RTDCiv. Revue trimestrielle de droit civil, no.04, 2020, page957.

503. Le droit à la vie privée, droit constitutionnel depuis 1977. En tant que droit constitutionnel, le respect de la vie privée n'est pas explicitement mentionné dans la Constitution de 1958. Le premier pas vers la reconnaissance de ce droit a été fait en 1977, à la suite d'une décision du Conseil constitutionnel de France[1411] qui limitait la fouille des véhicules[1412]. Dans une décision de 1983, la protection de la vie privée est remise en question, cette fois-ci dans le contexte des perquisitions fiscales[1413]. La reconnaissance du droit à la protection de la vie privée comme un droit fondamental a été réalisée en 1995, dans l'article 66 de la Constitution française[1414].

504. La vision du professeur R. Savatier sur le droit à la vie privée. Le droit à la vie privée, ce véritable droit subjectif, a été reconnu comme une suprématie dans le contexte de la technologie depuis 1959, grâce à la vision du professeur R. Savatier qui appréciait que « Ce n'est pas la personne humaine d'être l'esclave de la technique, c'est elle de servir l'homme »[1415]. De plus, et en particulier, la réforme législative à laquelle nous assistons vise à mettre à jour le cadre législatif pénal en augmentant l'efficacité du régime de protection concernant les actes pénaux commis dans le domaine privé de la technologie numérique[1416]. En tant que tel, étant donné que l'ingérence dans la vie privée de la personne est réalisée par des moyens diversifiés qui ne bénéficient pas de la stabilité d'un cadre législatif spécifique[1417], la réforme législative qui esquisse un modèle infractionnel propre aux délits commis dans le contexte du numérique est existentielle pour la réalisation d'un correspondant juridique approprié.

505. Amélioration du cadre juridique numérique. Ayant un effet direct sur les droits privés de la personne, la circulaire du 24 février 2024[1418] souligne la nécessité d'engager des

---

[1411] Le 12 janvier 1977, le Conseil constitutionnel français décide (selon la décision « Cons. Const., *12 janv. 1977, no. 76-75 DC* » que la loi autorisant la fouille de tout véhicule sur les routes publiques dans le but de prévenir les infractions touche aux principes fondamentaux qui protègent la vie privée et n'est pas conforme à la Constitution.

[1412] P. Kayser, *La protection de la vie privée par le droit : protection du secret de la vie privée*, 3e éd., Economica, 1995. https://gallica.bnf.fr/ark:/12148/bpt6k33323068/f10.item.texteImage

[1413] Décision *n° 83-164 DC du 29 Décembre 1983,* Source Lexis 360 Intelligence.

[1414] Décision *n° 94-352 DC du 18 janvier 1995.* https://www.conseil constitutionnel.fr/decision/1995/94352DC.htm

[1415] R. Savatier, *Les métamorphoses économiques et sociales du droit privé d'aujourd'hui, 2ème série, tome 1 L'universalisme renouvelé des disciplines juridiques*, Paris, Dalloz, 1959. disponible sur www.gallica.bnf.fr. En traduction : « *La personne humaine ne doit pas être l'escale de la technologie, mais la technologie doit être au service de l'homme ».*

[1416] *Le droit au respect de la vie privée: les défis digitaux, une perspective de droit comparé*, Service de recherche du Parlament européen, 2018. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/628292/EPRS_STU(2018)628292_FR.pdf

[1417] Par exemple, la divulgation de données privées en ligne, la distribution d'images de contenu sexuellement intime sans consentement via des sources numériques, le vol d'identité en ligne, les attaques cyber-patrimoniales, le harcèlement en ligne et autres.

[1418] Voir *Circ. JUSD2403689C du 14 février 2024,* d. mis à jour le 1e mars 2024 - Le Directeur des affaires pénales et grâces a demandé au Ministère public de prendre part activement dans le régime progressif de sanction des téléchargements illicites. Conséquences possibles pour les infractions de grade 5 pour négligence caractérisée (Code de la propriété intellectuelle, art. R. 335-5) ou pour les infractions de contrefaçon (art. L. 335-2, L. 335-2-

poursuites pénales contre les personnes qui mettent à disposition, notamment à des fins commerciales, des contenus en ligne via des téléchargements illicites. Ainsi, a été créée la possibilité d'enquêter sous forme pénale sur les faits initialement sanctionnés par des contraventions, dans le cas de leur répétition de manière régulière ou massive. L'intérêt du législateur français pour améliorer le cadre juridique numérique ne se limite pas uniquement à la mise à jour des infractions du Code pénal. Par le décret no. 2023-1083 du 23 novembre 2023, l'Office de lutte contre la cybercriminalité (OFAC)[1419] est créé, un bureau central dédié à la lutte contre la cybercriminalité, en réponse à l'augmentation de la cybercriminalité et au besoin de surveiller les enquêtes cybernétiques.

Ces réglementations sont d'autant plus nécessaires que l'on ne peut plus s'opposer à la participation de l'homme dans une société technologique, qui se matérialise dans le plan privé de chacun, à partir des échanges banals de messages mobiles, à la gestion de transactions financières complexes[1420]. Nous ne pouvons pas le contester, la technologie a radicalement changé la façon dont nous communiquons avec nous-mêmes ainsi qu'avec les autres, devenant une extension indispensable de notre vie privée, mais non exemptée de vulnérabilités, de menaces, de défis essentiels en matière de sécurité, de vie privée et de justice pénale[1421]. En 2005, un rapport sur la lutte contre la cybercriminalité concluait que, bien que la communication par des moyens électroniques soit un espace de liberté d'expression[1422], la liberté ne peut être absolue puisque le contenu de cette expression peut porter atteinte à la sécurité, à la dignité ou à l'intégrité de la personne[1423].

1, L. 335-3 et L. 335-4 du CCI). La procédure de l'ordonnance pénale est proposée pour la violation de l'article R. 335-5 de la CPI. Les personnes qui rendent des contenus disponibles en ligne, notamment à des fins commerciales, doivent être poursuivies devant les tribunaux. La circulaire souligne le besoin d'une information correcte des victimes.

[1419] Le décret crée l'Office de lutte contre la cybercriminalité (OFAC), qui remplace la sous-direction pour la lutte contre la cybercriminalité et l'Office central pour la lutte contre la criminalité liés aux technologies de l'information et des communications. Le bureau central est dédié à la lutte contre la cybercriminalité, en réorganisation pour renforcer son rôle de coordination opérationnelle des services de cybercriminalité. Le décret peut être consulté sur le site Légifrance à www.legifrance.gouv.fr

[1420] P. Yves, *La vie privée à l'heure de la société du numérique Chapitre 1 - La révolution technologique –État des lieux*, Larcier, 2019. https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=DZ/LARCIER/VIE PRIVEE-A-HEURE-SOCIETE-NUMERIQUE/2018/NIVO/T01-C001

[1421] *A/HRC/51/17: Le droit à la vie privée à l'ère numérique, Nations Unies Droits de l'homme, 2022* https://www.ohchr.org/fr/documents/thematic-reports/ahrc5117-right-privacy-digital-age

[1422] *Loi no. 2004-575 du 21 juin 2004 sur la confiance dans l'économique numérique, Art.1*. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000801164/

[1423] Voir *Rapport de lutte contre la cybercriminalité,* Notes bleues de Bercy, 2005, nr. 289 *: „Cette liberté ne saurait être absolue, dès lors que les contenus peuvent porter atteinte à la sécurité et, notamment, à la dignité ou à l'intégrité physique des personnes".*

§1. MODALITÉ DE COMMISSION DU DÉLIT D'ATTEINTE À LA VIE PRIVÉE DANS LE DOMAINE DU DROIT FRANÇAIS

Avant de procéder à une comparaison entre le droit pénal français et le droit pénal roumain, nous estimons opportun de mentionner, en principe et en résumé, les éléments modificateurs et nouveaux qui ont été introduits dans le Code pénal français, notamment au cours des dernières années. Nous examinerons, y compris, mais surtout, comment le législateur entendait protéger la vie privée menée dans le domaine du numérique[1424], un monde nouveau[1425] et d'une façon insuffisante sous-exploité[1426], tel que certains auteurs considèrent [1427].

506. Analyse du Code pénal français. L'atteinte à la vie privée commise dans le domaine du numérique est directement prévue et dérivée des dispositions des articles 226-1, 226-2, 226-2-1, 226-3, 226-4, 226-16 - 226-24, 432-9, 131-39 du Code pénal français et des dispositions législatives y afférentes, respectivement la loi du 11 mai 1868[1428], la loi no. 78-17 du

[1424] Pour une perspective détaillée, voir l'opinion de l'auteur historique israélien Y. N. Harari, « *21 Lessons for the 21st Century* », Penguin Books, 2018. p.30-31. Nous offrons, en bref, un petit fragment : Les révolutions dans la technologie de l'information et la biotechnologie sont encore à leurs débuts (.). „*La plupart des habitants de Birmingham, d'Istanbul, de Saint-Pétersbourg et de Mumbai ne sont que vaguement conscients - ou pas du tout - du développement de l'intelligence artificielle et de son impact potentiel sur leur vie. Mais il ne fait aucun doute que les révolutions technologiques vont décoller dans les prochaines décennies et soumettre l'humanité aux épreuves les plus difficiles qu'on ait jamais connues. Toute histoire qui essaiera d'attirer la loyauté de l'humanité sera testée tout d'abord sa capacité à faire face aux deux révolutions (..) devront non seulement comprendre l'intelligence artificielle, les algorithmes de Big Data et la bioingénierie, mais aussi les intégrer dans une nouvelle histoire qui a du sens."*

[1425] Le terme de « nouveau monde » est utilisé au sens figuré, une opinion sur la découverte du Nouveau Monde par Christophe Colomb le 12 octobre 1492, l'un des événements les plus importants de l'histoire de l'humanité.

[1426] Pour une perspective détaillée, voir l'opinion de l'auteur historique israélien Y. N. Harari, « *21 Lessons for the 21st Century* », Penguin Books, 2018. p.20 - 21 : « *Les révolutions de la biotechnologie et des technologies de l'information nous donneront le contrôle de notre monde intérieur et nous permettront de concevoir et de créer la vie. Nous apprendrons à concevoir des cerveaux, prolonger la vie et tuer la pensée à volonté. Personne ne sait quelles en seront les conséquences. Les gens ont toujours été beaucoup mieux à inventer des outils qu'à les utiliser avec sagesse. Il est plus facile de manipuler une rivière en construisant un barrage sur son cours que de prévoir toutes les conséquences complexes de celle-ci sur le système écologique au sens large. De même, il sera plus facile de réorienter le flux de l'esprit que de prédire ce que cela signifiera pour notre psyché ou nos systèmes sociaux* ».

[1427] Pour une discussion détaillée, voir l'opinion de l'auteur T. Marshal, „*The Age of Walls: How Barriers Between Nations Are Changing Our World*", Scribner Book Company, 2019. p.12-13.
Nous donnons, en bref, un petit fragment : « *L'ère nouvelle dans laquelle nous sommes est reflétée et exacerbée par les progrès du monde numérique. Mark Zucherberg, le cofondateur de Facebook, croyait que les réseaux sociaux nous unifiaient. Il a par la suite admis qu'il avait tort. Si à certains égards ils nous ont rapprochés, les réseaux sociaux ont donné l'occasion de s'exprimer et de prouver leur capacité d'organisation aux nouvelles tribus cybernétiques ; (...) La question à laquelle il faut répondre est : quelle forme prennent les tribus modernes ? Nous définissons-nous par la classe sociale, la race, la religion, la nationalité à laquelle nous appartenons ? Et est-il possible que ces tribus coexistent ?*».

[1428] La loi, également appelée « *Loi sur la presse* », marque la réforme de la presse en France, remplaçant le système préventif de contrôle de la presse par un système répressif, contrôlé par la justice. F. Brayer, *La loi annotée du 11 mai 1868 sur la presse*, Paris, Librairie A. Durand, 1868. L'article 11 de cette loi stipule : « *Toute publication dans un écrit périodique relatif à un acte de vie privée constitue une contravention passible d'une amende de 500 F* », représentant les premières références législatives au terme de la vie privée

6 janvier 1978[1429], le code civil[1430], le code de procédure pénale[1431], la loi sur la lutte contre la cybercriminalité[1432].

507. L'ancien et l'actuel Code pénal. Dans l'ancien Code pénal, l'atteinte à la vie privée incriminait l'invasion du domicile et la violation du secret de la correspondance. Actuellement, le Code pénal français criminalise au moyen de la première section « De l'atteinte à la vie privée », le fait type d'atteinte à la vie privée, commise selon des voies spécifiques mises en évidence par le législateur dans le contenu des articles 226-1 - 226-7, avec un résultat volontaire direct ou indirect sur l'ingérence dans les droits privés de la personne[1433].

L'article 226-1 du Code pénal français réglemente le principal délit d'atteinte à la vie privée et a été constaté devant la Première chambre civile de la Cour de cassation en France depuis 2014, lorsqu'il a fait l'objet d'une question préliminaire d'inconstitutionnalité aux côtés de l'article 226-2 du Code pénal français, qui rêve de l'infraction dite consécutive en relation avec le droit à la liberté d'expression garanti par l'article 11 de la Déclaration universelle des droits de l'homme. La critique visait à interdire « de manière générale et absolue » toute diffusion qui aurait inclus des discussions privées ou confidentielles enregistrées sans le consentement du titulaire. Étonnamment (si l'on se réfère à la jurisprudence actuelle), la Cour a conclu que cette question n'était pas sérieuse et qu'il ne restait qu'au juge d'évaluer si les discussions enregistrées violeraient ou non un droit privé[1434]. On peut rappeler ici la déclaration du ministre René Pleven[1435] au Journal officiel de l'Assemblée nationale (JOAN), en 1970 :

[1429] La loi est également connue sous le nom de « *Loi sur la protection des données* » (Loi informatique et libertés) et réglemente le processus de collecte, de traitement et de stockage des données personnelles, faisant du respect du droit à la vie privée l'objet d'un cadre de protection supplémentaire. La loi a intégré les dispositions du règlement général sur la protection des données (RGPD).

[1430] L'article 9 du Code civil français dispose que toute personne a droit au respect de sa vie privée et de son image. Bien qu'il s'agisse d'une règle purement civile, la jurisprudence française lui accorde le statut de norme complémentaire de protection pénale.

[1431] Aux fins des dispositions régissant les conditions d'utilisation de preuves obtenues illégalement, qui prévoient que les preuves obtenues par atteinte à la vie privée ne peuvent pas être utilisées en justice.

[1432] La loi est également connue sous le nom de *Loi GODFROY* et fait référence à la protection des données personnelles et des communications contre le délit numérique.

[1433] Le Code pénal français prévoit la forme type de l'infraction d'atteinte à la vie privée, comme suit : „ *Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui*" ; 1°„*En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel*"; 2°„*En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé".*

[1434] Pour une analyse plus complexe, voir l'avis de A. Lepage, « *Refus de renvoyer une QPC portant sur les articles 226-1 et 226-2 du Code pénal* », CCE, 2014. comm.39.
Aussi, pour mieux comprendre l'évolution impressionnante de l'article 226-1 du Code pénal français de 2014 à nos jours, consultez également Civ. Décision no 13-21.929 du 5 février 2014, qui renforce notre conclusion sur l'applicabilité stricte de l'article 226-1 du Code pénal français dans la jurisprudence ancienne.

[1435] René Pleven (1901-1993) est un politicien français important, qui a été premier ministre et ministre de la justice dans la république, également connu pour d'importantes réformes juridiques dans la gestion des débats liés à l'équilibre entre les droits fondamentaux.

« Les dispositions sur la protection de la vie privée ne doivent en aucun cas porter atteinte à la liberté d'expression de la presse »[1436].

508. Distinction entre infraction principale et infraction secondaire. Bien que le nom de la section soit général et puisse paraître abstrait, il ne faut pas sous-estimer d'une part la capacité du législateur à inclure dans son contenu des moyens suffisants pour mener l'attaque contre la vie privée, et d'autre part, nous ne devons pas limiter l'attaque exclusivement aux dispositions de cette catégorie de faits, car cette partie contient des règlements uniquement en ce qui concerne les infractions principales; ou la législation pénale dans le domaine comprend également d'autres infractions, secondaires ou dérivées, correspondant à l'incrimination type[1437]. À cet égard, il apprécie la doctrine française[1438], qui distingue entre l'infraction principale (type) et l'infraction secondaire (dérivée, connexe, périphérique), cette dernière étant incriminée en termes de son lien avec la pluralité des actes matériels compris dans le contenu de la première (appelée, comme nous l'avons vu, « l'atteinte à la vie privée »).

L'article 226-1 et suivants du Code pénal regroupe la conduite en plusieurs sous-catégories, le législateur s'autorisant à sanctionner non seulement les actes qui entrent expressément dans ce type d'atteinte à la vie privée, mais aussi ceux qui en découlent ou y sont liés. À ce titre, par exemple, le comportement illicite postérieur à l'acte est criminalisé au moyen de l'article 226-2, respectivement par l'utilisation du produit obtenu par atteinte à la vie privée. L'attitude illégale avant la commission de l'acte type, consistant dans la fabrication ou la promotion d'un dispositif susceptible d'être apte à porter atteinte à la vie privée[1439], est sanctionnée au moyen de l'article 226-3.

A. Espionnage auditif

a). Caractère privé ou confidentiel

509. Définition de l'espionnage auditif. L'article 226-1, paragraphe 1, alinéa 1 du Code pénal français prévoit que le fait de capturer, d'enregistrer ou de transmettre des propos

---

1436 *Journal Officiel Assemblée Nationale – No 41*, 28 mai 1970. https://archives.assemblee nationale.fr/4/cri/1969-1970-ordinaire2/033.pdf

1437 Pour un regard en détail, voir l'opinion de J. Pradel, M. Danti-Juan, *« Droit Pénal social : Droit commun – Droit des affaires,* 7e éd., Cujas, Paris, 2017. p.204

1438 Pour références supplémentaires, consulter y compris les œuvres de M.-L. Rassat, M. Véron, J. Pradel, M. Danti-Juan, V. Malabat et autres.

1439 Voir V. Malabat, „*Droit Pénal spécial*", Dalloz, Paris, p.335, duquel nous citons: "*Parmi les comportements incriminés figurent l'atteinte à la vie privé elle-même mai aussi des infractions périphériques, c'es-a-dire qui sanctionnent en réalité les conséquences ou la préparation de l'infraction d'atteinte a la vie privée: il s'agit de l'utilisation du produit de l'atteinte a l'intimité de la vie privée et de la fabrication ou de la publicité d'un appareil permettant l'atteinte a la vie privée*".

prononcés en privé ou confidentiel sans le consentement de la personne concernée constitue une infraction[1440]. Ainsi, plusieurs voies alternatives de commettre le délit entrent dans le corps infractionnel, mais pour retenir un délit il est essentiel qu'à travers ces voies, les éléments liés à la nature privée de la vie soient affectés. Dans la pratique, il n'est pas facile de déterminer le caractère privé d'une conversation. Par exemple, lorsqu'un employé installe secrètement un magnétophone dans le bureau de son employé, la Cour de cassation qualifie l'acte d'atteinte à la vie privée, peu importe la nature des conversations qui auraient pu avoir lieu dans cet espace[1441]. Si, dans l'ancienne législation, seules les actions prises dans un espace privé étaient criminalisées, cette notion disparaît actuellement, de sorte que toutes les conversations confidentielles, quel qu'il soit l'endroit, entrent sous l'incidence de la loi[1442]. Dans une autre affaire, la Cour de cassation annule la décision de la Cour d'appel en faisant valoir que les discussions clandestines enregistrées ne concernaient que l'activité professionnelle des salariés, par conséquent une atteinte à la vie privée n'est pas démontrée (il n'y a pas d'élément matériel du délit)[1443]. Le paragraphe 1 de l'article 226-1 se réfère strictement à la capture des paroles, qui est traduite dans la pratique, soit comme une discussion en face à face ou au téléphone. Elle ne comprend pas les messages écrits privés, qui sont en fait des mots transformés en texte à la suite du processus de numérisation, et qui sont plutôt sujets au délit d'atteinte au secret de la correspondance.

b). Capture, enregistrement et transmission

510. Capture, enregistrement et transmission audio illégaux. L'article comprend trois façons d'atteinte à la vie privée par l'écoute clandestine, c'est-à-dire par « un processus quelconque », qui permet de capturer, d'enregistrer et de transmettre des paroles privées ou confidentielles[1444]. Il convient de souligner que le simple enregistrement est considéré une infraction, quel que soit le résultat[1445]. Dans ce contexte, la doctrine considère que l'on peut imaginer l'hypothèse d'utiliser des stéthoscopes très sensibles à appliquer sur un mur afin de capturer des conversations tenues dans une pièce proche, ou d'utiliser un mini-microphone

[1440] Édité par la *loi no. 2024-120 du 19 février 2024 – article2.*
[1441] Cour de cassation - Chambre criminelle *24 janvier 1995 / n° 94-81.207*
[1442] M.-L. Rassat, *Droit pénal spécial – Infractions du Code pénal*, 9e édition, Dalloz, 2024. p.584 https://bibliotheque-lefebvre-dalloz-fr.docelec.u-bordeaux.fr/acces-liseuse/9782247233489?page=596
[1443] Crim. *16 janv. 1990, Bull. crim. n° 25*. https://www.legifrance.gouv.fr/juri/id/JURITEXT000007062529/
[1444] J.C. Saint-Pau, *L'enregistrement clandestin d'une conversation téléphonique amicale relative à l'activité professionnelle*, Recueil Dalloz, 2007, pp.1184. ⟨halshs-02210053⟩
[1445] Voir la décision Cass. Crim., *19 mai. 1981, pourvoi n°80-94634, Bull. crim. N. 161*. Dans ce cas, la Cour de cassation met en évidence que le simple acte d'enregistrement clandestine d'une conversation privée, sans le consentement des personnes impliquées, constitue une atteinte à l'intimité de la vie privée.

caché dans cette pièce, ou même d'intercepter des communications téléphoniques sous toutes les formes possibles[1446]. Bien que le formulaire en vigueur ait modifié l'ancienne disposition, qui prévoyait la violation par l'utilisation d'un « dispositif aléatoire », cependant, l'acte d'écoute du texte actuel ne peut être retenu comme illégal en l'absence d'un tel dispositif. Par exemple, l'acte d'écouter à la porte ou à travers le mur ne remplit pas une fonction infractionnelle[1447]. Si une conversation impliquant des échanges de nature privée ou confidentielle est écoutée, au moyen d'un drone équipé de capteurs audio[1448], dans la mesure où les sons sont enregistrés sur un support qui stocke les données à l'intérieur du drone[1449], ou qu'ils sont transmis à un serveur distant, le législateur considère que nous sommes en présence d'un délit d'atteinte au droit à la vie même si cette conversation a eu lieu dans un espace public.

511. Méthodes d'écoute clandestine, incriminées pénalement. L'acte d'enregistrement sans le consentement de la personne concernée est le moyen le plus couramment utilisé pour porter atteinte à la vie privée. L'enregistrement des mots prononcés à l'aide de n'importe quel type de technique (téléphone, caméra, magnétophone) est un moyen d'atteindre la vie intime de cette personne[1450]. Comme on peut le voir, dans le droit pénal français la plupart des voies de l'écoute clandestine sont susceptibles d'atteindre la vie privée[1451], au fil du temps les

---

[1446] Voir R. Badinter, „*Le droit au respect de la vie privée*", JCP, I. 2136, 1968. et „*La protection de la vie privée contre l'écoute électronique clandestine*", JCP, I. 2435, 1971.

[1447] Voir la décision Cour de Cassation, Chambre criminelle, du *12 avril 2005, 04-85.637*, qui clarifie le fait que l'écoute à la porte ou aux murs, sans moyens techniques dédiés ne constitue pas un délit selon l'art. 226-1. https://www.legifrance.gouv.fr/juri/id/JURITEXT000007071241/

[1448] H. Pelletier, D. Beauvais, *JurisClasseur Pénal Code, art. 226-1 à 226-3-1*, *Fasc. 20* : *Atteinte à la vie privée – Enregistrement de la parole ou de l'image – Fabrication, détention, location ou vente d'appareils d'enregistrement*, Lexis 360 Intelligence, 2022. pf.17

[1449] Tel qu'une carte de mémoire ou un disque dur.

[1450] Voir, à titre d'exemple, la jurisprudence :

- l'écoute par le mari dans l'appartement et les bureaux de sa femme, après la délivrance d'un ordre de réconciliation, constitue une atteinte à la vie privée, celui-ci reconnaissant d'ailleurs qu'il s'est toujours intéressé à la vie privée de son épouse - en Crim. 11 févr. 1987, D. 1987, somm. 142 ;
- l'enregistrement des conversations que les employés ont eues pendant le déjeuner, à l'aide d'un interphone situé dans la salle qui leur a servi de cantine, constitue, de la part de l'employeur, une atteinte à la vie privée, étant donné que ces conversations ne concernaient pas seulement la vie professionnelle, mais aussi la vie privée des diverses personnes - dans T. corr. Saint-Etienne, 19 avr. 1977, D. 1978. 123, note de Lindon,
- Nous notons également que l'exclusion des questions patrimoniales de la sphère de la vie privée cesse lorsque les discussions enregistrées se croisent avec des relations sentimentales. Cet aspect a été illustré dans un cas qui ne concernait pas les relations amoureuses, mais familiales. Dans cette situation, il s'agissait de l'enregistrement par le propriétaire d'une pharmacie d'une conversation menée par une employée avec son père. Le Tribunal a estimé que la discussion « avait pour sujet principal la famille et qu'elle était donc liée à la vie privée », même si des questions matérielles ont également été abordées – plus particulièrement, la vente d'un bien immobilier - dans l'affaire T. corr. Paris, 7 nov. 1975, D. 1976. 270, note de Lindon; RSC 1976. 729, observations de Levasseur,
- l'employeur qui a caché un magnétophone à commande vocale dans le faux plafond du bureau occupé par deux de ses employés a également été reconnu coupable d'atteinte à la vie privée - en crim. 24 janvier 1995, no. 94-81.207.

[1451] Cour de cassation - Chambre criminelle *31 octobre 2017 / n° 16-87.411* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_2017-10-31_1687411

tribunaux nationaux incluant aussi par ses décisions, dans la notion de vie privée, l'information sur la santé, la famille ou la vie sentimentale[1452].

512. Conversation privée vs discussion publique. Cependant, l'enregistrement exclusif des paroles prononcées par une personne ne connaît pas un caractère illicite. Par conséquent, si l'enregistrement est effectué par un tiers qui ne participe pas activement à la conversation, l'article 226-1[1453] n'est plus applicable. Toutefois, l'acte peut constituer le délit d'atteinte au secret de la correspondance et est soumis à l'article 226-15 paragraphe 2[1454]. L'enregistrement secret d'une conversation professionnelle avec un collègue ne constitue pas une atteinte à la vie privée[1455]. Pour entrer dans le champ d'application de l'article 226-1, le caractère privé ou confidentiel de la conversation est requis.

Une discussion délicate demeure sur la situation où un journaliste enregistre[1456], sans en informer l'interlocuteur, une interview qui sera rendue publique sous forme d'article. Bien que l'action constitue une invasion civile, étant dépourvue de normes éthiques et professionnelles[1457], de nombreux experts estiment que les éléments qualitatifs du délit d'atteinte à la vie privée ne sont pas satisfaits, donc il ne devrait pas tomber sous l'incidence pénale[1458].

c). Cause justificative

513. Clarification des causes justificatives. La Cour de cassation rappelle dans de nombreuses décisions que le respect de la vie privée est un droit fondamental et ne peut être violé, quel que soit l'objet de l'enregistrement (même s'il est effectué pour mettre en évidence

---

[1452] Cour d'appel de Paris *5 décembre 1997 – D. 1998. 32*. dans cette décision, la Cour d'appel de Paris établit que l'information sur l'hospitalisation dans un établissement psychiatrique d'un maire est une atteinte à la vie privée, le droit à la vie privée n'étant pas annulé par le statut public de l'individu. https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=RECUEIL/IR/1998/0168.
-Cour de cassation, Chambre *criminelle 15 février 2011 / n° 10-82.808* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_2011-02-15_1082808. Dans cette affaire, la Cour de cassation annule la décision initiale de la Cour d'appel, en mettant en évidence que l'utilisation d'un dispositif d'enregistrement dans un cabinet médical, où des discussions confidentielles ont lieu et qui sont protégées par le secret médical, constitue un délit

[1453] Voir en ce sens la jurispru Crim. *16 ian. 1974, Bull. Crim. nr. 25; JCP 1974. II. 17731*, note de Lindon.

[1454] M.L. Rassat, *Droit pénal spécial*, 5e éd., Dalloz, no.421, 2006.

[1455] J.-C. Saint-Pau, « *L'enregistrement clandestin d'une conversation téléphonique amicale relative à l'activité professionnelle* », Recueil Dalloz, n°17, 2007. p.1184

[1456] Les journalistes ont généralement recours à l'enregistrement des interviews pour ne pas attenter à la vie privée de l'interlocuteur, mais pour assurer une transcription fidèle des réponses, pour éviter d'éventuelles distorsions des déclarations et pour disposer d'un moyen de preuve si les déclarations sont contestées ultérieurement.

[1457] E. Dreyer, *Droit de la presse et droits de la personnalité,* Dalloz, 2012. p.765. https://www-dalloz fr.docelec.u-bordeaux.fr/documentation/Document?id=RECUEIL/CHRON/2012/0076

[1458] C. Bigot, *Hors collection Pratique du droit de la presse - Chapitre 441 - Protection pénale des droits de la personnalité*, Dalloz, 2023/2024 https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=DZ/HORS-COLLECTION/PRESSE/2023/NIVO/L04-T44-C441

une pratique illégale) que dans des situations légalement justifiées[1459]. Cependant, l'enregistrement de communications téléphoniques anonymes et répétées afin d'identifier l'auteur d'un acte de violence conjugale, bien que cela perturbe la vie familiale d'une personne, ne présente pas la nature d'une atteinte à la vie privée[1460]. Ce comportement peut être justifié, si la loi autorise l'utilisation de telles procédures[1461], le législateur considérant légitime l'atteinte apportée à la vie privée, donc cet acte n'aura pas d'effets pénaux[1462].

B. Espionnage visuel

a). Caractère privé et confidentiel

514. Distinction entre l'infraction d'espionnage visuel et l'infraction d'espionnage. Une autre façon de porter atteinte à la vie privée est de recueillir, enregistrer et diffuser l'image d'une personne sans consentement dans un lieu privé, tel que visé à l'article 226-1 alinéa 1er, paragraphe 2. Contrairement à l'espionnage auditif, l'espionnage visuel n'est criminalisé que dans des lieux privés.

515. Protection des personnes décédées. Ce droit s'applique également au-delà du décès aux personnes décédées ou sur leur lit de mort[1463]. Cela crée une différence entre la protection civile, qui cesse avec la mort[1464] et la protection pénale, que le législateur a décidé d'étendre et de soutenir à travers l'article 226-6 du Code pénal, qui permet aux ayant-droits de porter plainte. La justification reste fragile, et soulève de nombreuses questions[1465].

L'image d'une personne est considérée dans ce domaine comme « la taille visible de la personne humaine »[1466], c'est-à-dire que la vie privée d'une personne est contenue dans son image, et c'est pourquoi cet article ne protège que l'image de la personne, pas de ses biens, tels

---

[1459] Cour de cassation, Chambre criminelle, *4 Mars 1997 - n° 96-84.773*, où un groupe de journaliste étaient accusés et condamnés pour le délit d'atteinte à la vie privée après avoir enregistré en secret les employés d'une entreprise, afin de mettre en évidence des pratiques illégales présumées.

[1460] Voir en ce sens la jurisprudence pénale en *Crim. 17 iul. 1984, Bull. Crim. nr. 259 ; RSC 1985. 304*, observations de Levasseur.

[1461] Par exemple, dans le cadre d'une enquête judiciare afin de découvrir la réalité.

[1462] Selon les articles 100, 706-95, 706-96 du Code de procédure pénal, l'autorité judiciaire peut disposer l'interception, l'enregistrement ou la transcription des télécommunications. https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154/
La Convention européenne des droits de l'homme (articles 6, 8 et 13) reconnaît également le besoin d'interception des communications téléphoniques.

[1463] Cour de cassation, Chambre criminelle, *20 Octobre 1998 - n° 97-84.621,* Source Lexis 360 Intelligence,

[1464] B. Beignier, *La vie privée : un droit des vivants*, Recueil Dalloz, 2000. p.372 https://www-dalloz fr.docelec.u-bordeaux.fr/documentation/Document?id=RECUEIL/NOTE/2000/0535

[1465] G. Beaussonie, « *Les bornes de la personnalité juridique en droit pénal* », Dr. fam., Doss. 5, 2012.

[1466] F. Zenati-Castaing, Th. Revet, *Manuel de droit des personnes*, no 321, PUF, 2006.

que le logement. Le propriétaire peut toutefois contester l'utilisation de l'image si cela lui cause un préjudice[1467].

516. Lieu du délit : public ou privé. Bien que la distinction entre lieu public et lieu privé soit parfois évidente, la distinction entre eux est parfois sensible et discutable. La principale caractéristique de l'espace privé est son accessibilité limitée. Considéré évidemment comme un espace privé, toute manière de photographier une personne à la maison, même à travers une fenêtre fermée, peut être un délit[1468]. L'intérieur d'une voiture est également considéré comme un espace privé, même lorsqu'elle se déplace sur les routes publiques, et il est interdit de photographier des personnes à l'intérieur[1469].[1470]

Une photographie prise dans la rue, également évidemment un lieu public, si elle ne porte pas atteinte à la vie privée de la personne concernée, ne constitue pas une violation de l'article susmentionné. En outre, la surveillance à l'œil nu ou par jumelles sans prise ni transmission de photographie ne relève pas des dispositions de l'article 226-1, alinéa 2[1471].

b). Capture, enregistrement et transmission

517. De la surveillance à la vidéo/photo et jusqu'à la diffusion. Comme le délit d'écoute clandestine, cela implique l'utilisation de toute méthode de capture, d'enregistrement et de transmission de l'image d'une personne, obtenue au préalable par l'une des techniques prévues à l'article 226-3 du Code pénal[1472], si la personne se trouve dans un lieu privé.

Le fait d'intercepter une photographie à l'aide d'un drone équipé de capteurs d'images, en survolant des personnes se trouvant dans un lieu privé[1473] est un délit en enregistrant les photos sur un support mémoire à bord du drone[1474].

[1467] Cour de cassation, Assemblée plénière, *7 Mai 2004 - n° 02-10.450,* Source Lexis 360 Intelligence
[1468] Cour de cassation, Chambre criminelle, *25 Avril 1989 - n° 86-93.632*, Source Lexis 360 Intelligence
[1469] Cour de cassation, Chambre criminelle, *20 Novembre 2007 - n° 06-82.753,* Source Lexis 360 Intelligence
[1470] Cour de Cassation, Chambre criminelle, *28 novembre 2006, 06-81.200*, *Inédit.* https://www.legifrance.gouv.fr/juri/id/JURITEXT000007639039
[1471] Cour d'appel, CAEN, Chambre correctionnelle*, 15 Novembre 2004* Source Lexis 360 Intelligence. En l'espèce, le défendeur est accusé de surveillance clandestine dans les toilettes des femmes à l'aide d'un miroir. Tant qu'il n'a pas enregistré ou transmis des images, mais seulement regardé, les tribunaux ont considéré que tous les éléments nécessaires à la création du délit d'atteinte à la vie privée ne sont pas touchés, et le défendeur a été retiré de la poursuite pénale.
[1472] *Arrêté du 4 juillet 2012 fixant la liste d'appareils et de dispositifs techniques prévue par l'article 226-3 du code pénal.* La liste des dispositifs techniques est réitérée par l'ordre de ministre. La dernière édition de l'ordre était en août 2016. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000026241910
[1473] Voir la *Circulaire du 14 septembre 2011 sur le cadre légal applicable à l'installation des caméras de vidéo-*protection sur les routes publiques et dans les lieux ou les unités ouverts au public, d'une part, et dans les lieux non ouverts au public.
[1474] M. Bourgeois, B. Touzanne, *Aéronefs télépilotés équipés de capteurs : « drones légaux »,* CCE, nº 12, étude 22, 2015.

c). Situations dans lesquelles le droit à la vie privée n'est pas violé

518. Cause justificative. En ce qui concerne certaines situations où le droit à la vie privée n'est pas atteint, la jurisprudence française est assez riche. Par exemple, il s'agissait de savoir si elle représentait une interférence dans la vie privée en cas d'enregistrement de l'image, à l'aide d'un radar équipé d'une caméra vidéo, d'un conducteur qui roule à grande vitesse afin de permettre son identification[1475]. La Cour de cassation affirme qu'en l'espèce, le droit à la vie privée n'est pas atteint[1476]. En outre, la surveillance à l'œil nu ou au moyen de jumelles sans prise ni transmission d'une photo ne relève pas des dispositions de l'article 226-1, alinéa 2[1477].

Également, dans le cas d'une personne non identifiable, l'acte de capter, enregistrer ou transmettre des sons ou des images sur un mineur non identifiable, en l'absence du consentement des titulaires de l'autorité parentale ne peut être considérée comme une atteinte à la vie privée au sens de l'art. 226-1 du Code pénal français. En particulier, la Cour de cassation française a jugé que l'acte du médecin consistant à distribuer l'image d'un nouveau-né par e-mail n'est pas un acte illicite si son acte ne permettait pas l'identification du mineur. En conclusion, l'acte du médecin ne saurait être associé à une atteinte à la vie privée au sens de l'art. 226-1 du Code pénal français[1478].

Dans une autre décision, la Cour de cassation annule partiellement la décision de la Cour d'appel[1479] en arguant que la liberté de presse et le droit à l'information permettent la diffusion d'images de personnes impliquées dans des événements actuels, sous réserve du respect de la dignité humaine. Et les commentaires relatifs à la publication, bien que critiques, ne violaient pas la dignité de la personne concernée[1480], un concept largement abordé plus loin.

519. Loi antiterroriste. Une mesure exceptionnelle qui permet la violation des dispositions de l'article 226-1 alinéas 1 à 3, par les autorités réglementées et sous le contrôle d'un juge, est

---

[1475] F. Taquet, *Trib. police Paris, 25 mai 1984 ; Ministère public c. Nanos*, Lexis 360 Intelligence, La Semaine Juridique - Édition générale, n° 6, du 5 février 1986.
[1476] Cour de cassation, Chambre criminelle, *12 Décembre 2000 - n° 00-83.323*
[1477] Cour d'appel, CAEN, Chambre correctionnelle, *15 Novembre 2004* Source Lexis 360 Intelligence. En l'espèce, le défendeur est accusé de surveillance clandestine dans les toilettes des femmes à l'aide d'un miroir. Tant qu'il n'a pas enregistré ou transmis des images, mais seulement regardé, les tribunaux ont considéré que tous les éléments nécessaires à la création du délit d'atteinte à la vie privée ne sont pas touchés, et le défendeur a été retiré de la poursuite pénale.
[1478] Voir les mentions et les observations faites par G. Loiseau dans la revue Légipresse, parue en janvier 2015 à la page 64, émise sur la décision de la Cour de cassation *no. 12-29.588, point no. 67 du 9 avril 2014*.
[1479] Dans cette affaire, la Cour d'appel de Metz a jugé que la diffusion d'une vidéo prise sans le consentement d'un médecin, bien que son visage soit flou et sa voix pâlie, constituait une violation de son droit à l'image.
[1480] Cour de cassation, *Pourvoi n° 15-28.813, 29 mars 2017*
https://www.courdecassation.fr/decision/5fd90811eaeb97a050042a87

exposée dans la loi no. 2016-731 du 3 juin 2016, informellement intitulée la loi anti-terrorisme[1481].

520. Protection de la vie privée des victimes de violence conjugale. Article 226-1 alinéa 4 du Code pénal sanctionne plus sévèrement les actes commis par le conjoint ou partenaire de la victime, la mise à jour des dispositions légales ayant pour objectif direct de protéger les éléments privés liés à la vie des victimes de violences conjugales[1482].

Par l'article 226-2 du Code pénal, le législateur français considère qu'il est de bon augure de sanctionner distinctement l'acte commis au moyen de la presse écrite ou de l'audiovisuel, ayant pour moyens de commettre l'acte de détention, de porter ou de laisser à la connaissance du public ou d'un tiers, ou l'utilisation de tout document obtenu au moyen d'un des actes visés à l'article 226-1[1483].

521. Ambiguïté législative concernant les images intimes. L'article 226-2-1 du Code pénal français[1484] fait référence à l'utilisation d'images ou de mots à connotation sexuelle. L'article prévoit que : « sont passibles des mêmes sanctions en mettant à la connaissance du public ou d'un tiers, sans le consentement de la personne, tout enregistrement ou document contenant des mots ou des images de nature sexuelle, obtenu avec le consentement exprès ou présumé de la personne, ou même par elle, par l'un des actes prévus à l'article 226-1 ». Ainsi, la simple publication en ligne d'une vidéo pornographique montrant une personne filmée sans son consentement, même dans un lieu privé, est désormais punie d'une peine de deux ans d'emprisonnement[1485]. La Cour de cassation sanctionne l'ambiguïté de cet article de la loi, puisqu'il ne définit pas clairement le terme « nature sexuelle »[1486]. Cependant, le Conseil constitutionnel considère ce terme comme suffisamment clair et précis, laissant aux instances compétentes les analyses ultérieures[1487].

Cet article représente, avec l'article 226-1 du même code, le pilier de la protection du droit à la vie privée. Comme nous l'avons vu, cette disposition réglemente le droit à la vie privée des individus, avec une attention particulière portée à sanctionner le résultat produit par l'utilisation de technologies.

[1481] *LOI n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et l'efficacité et les garanties* https://www.legifrance.gouv.fr/jorf/id/JORFSCTA000032627246

[1482] Pour une analyse détaillée, consulter l'opinion de l'auteur A. Denizot, „*Petites rectifications et grandes avancées en droit des victimes*", RTDCiv. „Revue trimestrielle de droit civil", no 04, 2020. pag.957.

[1483] Cour de cassation, Chambre criminelle, *10 Mai 2005 - n° 04-84.705* https://www-lexis360intelligence fr.

[1484] L'article a été introduit par *la loi cadre no. 2016-1321 du 7 octobre 2016 – art. 67*, en vigueur en date de 9 octobre 2016.

[1485] Par exemple, le Tribunal correctionnel de Montpellier a condamné le 16 novembre 2016, un homme qui s'était vengé de son ex-compagne en publiant sur des sites pornographiques une vidéo tournée sans son accord pendant certains rapports sexuels.

[1486] Cour de cassation, Chambre criminelle, *23 Juin 2021 – n° 21-80.682* https://www-lexis360intelligence fr.

[1487] Conseil constitutionnel, *30 Septembre 2021 – n° 2021-933* QPC https://www-lexis360intelligence fr.docelec.u-bordeaux.fr

d). Droit à l'image

522. Droit à l'image, délimitation par rapport à la vie privée. En l'absence d'un texte de loi spécifique, il découle de l'article 226-1 du Code pénal et de diverses jurisprudences qui le différencient du droit au respect de la vie privée[1488]. Le droit à l'image d'une personne comprend la capture, « la conservation, la reproduction et l'utilisation de son image », et sa violation donne à la victime le droit à réparation, sans qu'il soit nécessaire d'objectiver un autre dommage[1489]. Un autre exemple d'ingérence dans la vie privée est l'utilisation de l'Internet pour diffuser un film d'amour réalisé avec une autre personne, à qui il n'a pas porté à son attention l'acte de filmer et implicitement n'a pas eu son consentement[1490]. Le tribunal pénal a décidé que la divulgation au public/tiers d'une image représentant une personne qui a été trouvée dans un lieu privé ne peut être sanctionnée que si l'enregistrement a été fait sans le consentement de la personne concernée[1491]. Dans le même registre, le tribunal de Paris a retenu pour violation du droit au respect de la vie privée et du droit à l'image de la personne, l'utilisation de l'identité d'une personne à son insu pour créer un faux profil sur Facebook[1492].

e). Limites de la loi. Forme aggravée

523. Cet article peut présenter des limitations concernant les pratiques utilisées dans l'environnement en ligne, les exigences typiques concernant les conditions de prise d'image dans un lieu privé, à savoir le consentement de la personne à la capture d'image n'étant pas accomplies, lorsque nous nous référons à la publication de selfies, dans ce cas, celles faites en particulier et dans le groupe. Ainsi, nous apprécions que l'acte d'une personne de capturer l'image d'une autre personne par surprise, par hasard, au motif qu'elle était près de la personne qui faisait du selfie, ne répond pas aux conditions typiques de cet article, y compris dans le cas où la capture pourrait affecter (par l'acte ultérieur de distribution des photos dans l'environnement numérique) l'image, la réputation ou la dignité de la personne captée.

[1488] Cour de Cassation, Chambre civile 1, *Pourvoi 98-21.161, 12 décembre 2000.* https://www.legifrance.gouv.fr/juri/id/JURITEXT000007041721/

[1489] Cass. soc., *n° 20-12.420 et 20-12.421 19 janvier 2022*.- Dans ce cas, la Cour de cassation annule la décision de la Cour d'appel et estime qu'il est justifié d'accorder une indemnisation en cas de violation du droit à l'image, même si l'image en question a été retirée et qu'aucun dommage personnel n'a été démontré visant la victime

[1490] *Baptiste C c Min. public*, Paris, 24 avril 2007. www.juritel.com - La Cour d'appel de Paris a retenu le délit d'atteinte à la vie privée par fixation ou transmission d'une image et le délit d'utilisation d'un document ou enregistrement obtenu par une atteinte à la vie privée d'autrui.

[1491] Crim., *nr. 15-82.676, 16 mar 2016* AJ penal, 2016. p268

[1492] Décision du Tribunal de grande instance de Paris (TGI), Paris, le 24 novembre 2010 à www.legalis.net

524. Diffusion non consensuelle d'images intimes. Une autre hypothèse pour limiter à retenir le délit d'atteinte à la vie privée est la pratique immorale de « la vengeance pornographique (revenge porn) », valorisée par la publication de photos ou vidéos compromettantes dans le but de se venger entre anciens partenaires. Ici, la discussion devient extrêmement sensible parce que la plupart des photos sont prises avec le consentement de la victime[1493]. Ainsi, même si la pratique est immorale, contraire à l'éthique, la Cour de cassation française établit que la publication d'une image sur Internet, même en l'absence d'un consentement actuel, ne peut être considéré comme un délit si, au moment de la prise de la photo, il y avait consentement pour la réalisation et la distribution, et il n'est pas plausible à l'heure actuelle de retirer le consentement en fonction du contexte, et la nature privée du lieu où la photo[1494] a été prise n'est pas importante. Cependant, si de telles décisions sont contestées, il y a un risque de créer une lacune juridique, étant nécessaire en ce cas la clarté dans les dispositions du droit pénal[1495]. En outre, il existe aussi des jugements qui soulignent le fait que le consentement à la photographie ou au tournage ne comprend pas nécessairement le consentement à la diffusion[1496].

Toutefois, le tribunal peut sanctionner l'acte de « la vengeance pornographique » au moyen d'une autre infraction, à savoir l'acte d'usurpation de l'identité numérique[1497].

En résumé, nous constatons que la personnalité pénale de l'acte est déterminée par l'accomplissement de trois circonstances importantes : avoir un caractère volontaire[1498], manifesté par la forme de culpabilité d'intention directe ou indirecte[1499]; le résultat produit doit se manifester sous la forme d'un dommage causé à un élément privé de la vie de la personne;

[1493] Cour d'appel Montpellier, Chambre correctionnelle 3, *2 Février 2006, no 2006-301727.* https://www-lexis360intelligence-fr.docelec.u-bordeaux.fr

[1494] Cour de cassation, Chambre criminelle, *16 Mars 2016 – n° 15-82.676,* lexis 360 intelligence fr.

[1495] P. Conte, *Atteinte à la vie privée - Diffusion d'une photographie sans le consentement de l'intéressé*, Droit pénal, 2016. "*La diffusion d'une photographie n'est punissable que si l'enregistrement ou le document qui les contient a été réalisé sans le consentement de l'intéressé*" (voir Cass. crim., 16 mars 2016, n° 15-82.676, FS-P+B+I : JurisData n° 2016- 004598).

[1496] Cour d'appel, Amiens, Chambre correctionnelle, *15 Avril 2009 – n° 08/01374* https://www lexis360intelligence-fr.docelec.u-bordeaux.fr/. En 2008, l'accusé est condamné à une peine de prison pour avoir utilisé des photographies intimes afin de faire du chantage et de dénigrer l'image de son ex-partenaire. En 2009, la Cour d'appel a rejeté l'exception de nullité du jugement, ajoutant de nouvelles sanctions à la sentence.
- Cour d'appel, Rouen, Chambre correctionnelle, *25 Juin 2009 - n° 08/00962.* https://www-lexis360intelligence fr

[1497] Voir, par exemple, la Décision rendue par la 17ème Chambre correctionnelle du Tribunal de grande instance en date de 24 mars 2015, dans l'affaire des parties anonymisées *V.P. et F.Z. contre A.S. et K.G*. Aspecte traité par E.-A. Caprioli**,** *obs. sous V.P. et F.Z. c/ A.S. et K.G.*, Contrats Concurrence Consommation, comm.86.

[1498] Cour de cassation, Chambre criminelle, *7 Octobre 1997 - n° 96-81.485,* https://juricaf.org/arret/FRANCE COURDECASSATION-19971007-9681485

[1499] Il est un délit d'enregistrer et de transmettre des mots ou des images d'une personne, obtenus dans le cadre d'une conversation confidentielle ou dans un lieu privé.

être remplie la condition de l'absence de consentement préalable du titulaire des paroles prononcées[1500].

525. Capture, enregistrement, diffusion d'images intimes, forme aggravée de l'infraction. L'Article 226-3-1 du Code pénal français[1501] interdit, comme nouveauté, l'utilisation de tout moyen pour observer les parties intimes d'une personne, sur fond de vêtements considérés comme sommaires, indécents ou nus, tant que la personne concernée se trouve dans un lieu fermé (toilettes, vestiaire, véhicule automobile), caché « aux yeux de tiers », si l'acte est commis à l'insu ou sans le consentement de la personne concernée[1502]. L'infraction comporte également une forme aggravée avec un contenu alternatif, par exemple l`implication d'un mineur en tant que titulaire du droit lésé, lorsque l`auteur de l`acte est représenté par le conducteur d`un véhicule de transport public de passagers, ou lorsqu'il se trouve dans une relation de travail contractuelle dans un lieu destiné à l'accès d'un moyen public de passagers. Par exemple, il n'est pas un délit les images prises sur une plage de nudistes[1503].

f). Nécessité du consentement

Comme dans toute situation où le consentement est en cause, il doit être libre, éclairé et donné avant, ou au plus simultanément, l'action de capture auditive ou d'image[1504].

526. Consentement à l'enregistrement audio ou vidéo. Dans le cas de l'espionnage auditif et visuel, l'absence de consentement représente un élément constitutif commun. Dans l'hypothèse où les actes qui entrent dans le corps du délit sont accomplis avec la connaissance de la personne titulaire, et que celle-ci aurait pu bénéficier du droit de pouvoir s'y opposer, le législateur accorde à l'acte la présomption relative d'un consentement librement exprimé. Plus précisément, la loi considère qu'il n'est pas nécessaire d'imposer à l'auteur un caractère illégal lorsque l'acte d'espionnage auditif[1505] ou l'acte d'espionnage visuel[1506] a été effectué par un accord tacite de la part de la personne concernée. En d'autres termes, si la personne concernée

---

[1500] J. Larguier, S. Fournier, P. Conte, *Droit spécial*, Dalloz, 2024. p.94-96. https://bibliotheque-lefebvre-dalloz-fr.docelec.u-bordeaux.fr/acces-liseuse/9782247236251?page=114

[1501] L'article a été introduit par la loi cadre no. 2018-703 du 3 août 2018 – l'art. 16, en vigueur le 6 août 2018, concernant la lutte contre la violence sexuelle et le sexisme.

[1502] V. C. Pautrel, B. Partouche, *Le voyeur et le droit pénal: quelle qualification se cache sous les jupes des filles?*, Gaz. Pal. Rec. 2012. p.639

[1503] V. L. Saenko, S. Detraz, *La loi nº2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes : les femmes et les enfants d'abord,* Dalloz. 2018. cron. 2031

[1504]H. Pelletier, D. Beauvais, , *Art. 226-1 à 226-3-1, Fasc.20 : Atteinte à la vie privée, Enregistrement de la parola ou de l'image, fabrication, détention, location ou vente d'appareils d'enregistrement*, JurisClasseur Pénal Code, Lexis 360 Intelligence, 2022.

[1505] Cette expression est utilisée par l'auteur M.-L. Rassat dans son œuvre intitulée „*Droit Pénal spécial – Infractions du Cod pénal*", Paris, ed. Dalloz, 7-edition, 2014, p.537.

[1506] *Idem*, p. 538

s'est rendu compte que l'une des actions décrites ci-dessus mettait sa vie privée en danger, l'absence d'opposition constitue une acceptation, conformément à l'article 226-1, alinéa 2 du Code pénal. Un caractère essentiel du délit d'atteinte à la vie privée est la clandestinité, et se réfère à la situation où la victime est informée de son enregistrement sans consentement et la poursuite peut avoir lieu à la plainte de la victime[1507].

527. Délimitation de l'espace privé. En ce qui concerne l'établissement d'un espace privé, où il est présumé être observable en l'absence de l'utilisation de technologies sophistiquées, il appartient aux autorités compétentes de vérifier que les conditions d'existence ou de l'absence du consentement pour la production d'images faisant l'objet d'un litige relatif à des droits privés sont remplies[1508].

528. Consentement à l'enregistrement vidéo ou audio de mineurs. Pour les mineurs, le consentement des parents est requis (conformément à l'article 226-1, alinéa 3)[1509]. Toutefois, dans le cas d'une personne non identifiable, l'acte consistant à capturer, enregistrer ou transmettre des sons ou des images d'un mineur non identifiable, sans le consentement des titulaires de l'autorité parentale ne peut être considéré comme une atteinte à la vie privée au sens de l'art. 226-1 du Code pénal français. En particulier, la Cour de cassation française a jugé que l'acte du médecin consistant à distribuer l'image d'un nouveau-né par courrier électronique n'est pas illicite si son acte ne permettait pas l'identification du mineur. En conclusion, l'acte du médecin ne saurait être associé à une atteinte à la vie privée au sens de l'art. 226-1 du Code pénal français[1510].

C. Géolocalisation

529. Évolution technologique en matière de localisation. L'article 226-1, alinéa 1er, point 3 du Code pénal français criminalise la capture, l'enregistrement ou la transmission, par quelque moyen que ce soit, de la localisation en temps réel ou en retard d'une personne, sans son consentement. Dans le contexte du développement de la technologie de localisation, le

[1507] Cour de Cassation, Chambre criminelle, du 4 mars 1997, 96-84.773, Publié au bulletin https://www.legifrance.gouv.fr/juri/id/JURITEXT000007067082/

[1508] A cet égard, par exemple, un tribunal de Paris a condamné, par une décision du 25 janvier 1999 (non publiée), deux journalistes qui à la fin d'un spectacle ont suivi Michel Sardou sur sa moto et l'ont photographié dans son propre véhicule, bien qu'il s'y oppose clairement et manifestement. À cet égard, le Tribunal a souligné *« qu'une voiture représente un lieu privé, tant qu'elle n'est pas ouverte à toute personne sans l'autorisation de l'occupant, même si elle se déplace sur une voie publique* ». Ainsi, le Tribunal a déterminé que les conditions pour commettre le délit d'atteinte à la vie privée sont remplies, parce que Michel Sardou a exprimé suffisamment clairement son désaccord pour la réalisation des images.

[1509] Cass. crim., *24 mai 2023, n° 21-87.509*

[1510] Consulter les mentions et les observations faites par G. Loiseau dans la revue Légipresse, parue en janvier 2015 à la page 64, émises sur la décision de la Cour de cassation *no. 12-29.588*, paragraphe 67 du 9 avril 2014

législateur a cherché à compléter le contenu constitutif du délit d'atteinte à la vie privée en criminalisant une nouvelle hypothèse de commission[1511], à savoir l'interdiction de l'acte de capture, de transmission ou d'enregistrement de la localisation en temps réel ou hors ligne d'une personne sans son consentement[1512].

530. Débats juridiques. Cette situation a suscité d'intenses débats juridiques dans la société française[1513], certains considérant qu'il serait opportun de restreindre l'immunité entre les membres de la famille[1514] ; et, d'autres, que ce règlement manque du caractère de proportionnalité et d'utilité, parce qu'il s'étendrait à un champ trop large, touchant des géants de l'informatique ou des employeurs, la pratique de la géolocalisation étant courante et même tacitement acceptée dans les relations de travail[1515].

Notons par ailleurs que le tribunal français a étendu sa jurisprudence sur les données de connexion aux géolocalisations en temps réel. Ainsi, la géolocalisation d'une ligne téléphonique en temps réel, sans le consentement préalable de l'autorité compétente[1516], est

---

[1511] La criminalisation se réfère à l'hypothèse de commettre l'acte de collecter des données de géolocalisation d'une personne sans respecter les dispositions légales et les normes européennes, la conséquence dans le plan jurisprudentiel étant y compris leur exclusion sur le principe d'obtention de preuves illicites.

[1512] *Loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales* https://www.legifrance.gouv.fr/jorf/id/JORFARTI000042176677

[1513] En particulier, la géolocalisation est largement développée dans les *articles 230-32 et 230-33 du code de procédure pénale*, leur interprétation récente en relation avec le respect du droit à la vie privée, conduisant à des controverses concernant leur incompatibilité avec le droit de l'UE, pour lequel l'accord préalable de surveillance émis par une autorité compétente est prévu.

[1514] Pour une perspective plus claire, voir l'analyse de l'auteur L. Mary, „*Présentation de la loi n° 2020 936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales*", AJ fam., 2020. p.384.

[1515] Pour l'analyse, voir le commentaire formulé par Marthe Bouchet, Université Paris 2 Panthéon-Assas, en « Revue de droit privé Lexbase », nº 837 du 24.09.2020, qui peut être consulté à www.lexbase.fr/revue juridique/60504393-edition-n-837-du-24-09-2020#article-474505.

[1516] Le code de procédure pénale subordonne la prise d'une mesure de géolocalisation au respect de certaines conditions, dont l'utilisation de la géolocalisation en cas de nécessité, soit « *d'une enquête ou d'une recherche portant sur une infraction ou un délit passible d'au moins trois ans d'emprisonnement* », soit d'une procédure « *d'enquête ou d'instruction pour rechercher les causes de décès ou de disparition* » (voir à cet effet C. p. en. , art. 74, 74-1, 80-4) ou une procédure « *de recherche d'une personne en fuite* » (voir, à cet effet, C.P.P., art. 74-2). Dans le cadre d'une procédure de recherche ou d'enquête préalable ou flagrante prévue ci-dessus, la géolocalisation est autorisée par le ministère public « *pour une durée maximale de quinze jours consécutifs dans les cas visés aux articles 74-74-2 ou lorsque l'enquête porte sur une infraction ou un délit visé aux articles 706-73 ou 706-73-1 du Code de procédure pénale ou pendant huit jours dans les autres cas. A l'expiration de ces délais, cette opération sera autorisée par le juge de la liberté et de la détention à la demande du ministère public pour une durée maximale d'un mois renouvela*ble » selon les mêmes délais (voir C. pr. peni. , art. 230-33 10).
Dans le cadre d'une enquête ou d'un renseignement visant à enquêter sur les causes de décès ou de disparition, la géolocalisation est autorisée par « *le juge d'instruction pour une durée maximale de quatre mois renouvelables dans les mêmes conditions de forme et de durée* » (C.pen., art. 230). -33 20). Dans tous les cas, la durée de la géolocalisation ne peut excéder un an ou, s'il s'agit d'une criminalité organisée, deux ans.
Lorsque le tribunal rend la décision sur la géolocalisation, celle-ci doit être écrite et motivée par référence aux éléments factuels et juridiques qui justifient la nécessité de cette opération. « *Ne relève pas de la compétence et n'est pas susceptible de recours* » (voir C. p. en., art. 230-33). Ce système peut, dans des cas spécifiques définis à l'article 230-34 du code de procédure pénale, être mis en place ou démantelé dans des lieux privés définis par le même article. Lorsque dans une telle situation, il est nécessaire l'autorisation écrite du procureur, cette autorisation ne peut pas être accordée après l'installation du dispositif de géolocalisation dans un lieu privé (voir, Crim. *9 mai 2018, no. 17-86.558*, Dalloz news 29 mai 2018), 2018, obs.

considérée comme contraire aux principes du droit européen[1517]. On peut aussi citer la décision de la Cour de cassation de 2013, qui annule la décision de la Cour d'appel, soulignant que la géolocalisation apporte des atteintes importantes à la vie privée et nécessite donc le contrôle d'un juge[1518]. Afin de mieux légiférer cette affaire et de se conformer aux exigences de la CEDH[1519], la loi no 2014-372 du 28 mars 2014[1520] réglant la géolocalisation par les articles 232-32 à 232-44 du code de procédure pénale est adoptée.

531. La manière légale d'utiliser la géolocalisation. Par conséquent, la géolocalisation peut être justifiée dans le cadre d'une enquête judiciaire. Le Conseil constitutionnel a également déclaré que les dispositions relatives à la géolocalisation sont conformes aux dispositions de la Constitution, en ce sens que « la géolocalisation, une mesure de la police judiciaire, n'implique pas un acte de contrainte sur l'intéressé, ni une atteinte à son intégrité corporelle, saisie, interception de correspondance ou enregistrement d'images ou de sons »[1521]. Toutefois, la Cour fixe deux limites importantes, à savoir que les géolocalisations effectuées par balise GPS restent légales au motif qu'elles ne peuvent être couvertes par le droit de l'Union Européenne, respectivement les géolocalisations téléphoniques considérées comme irrégulières ne peuvent être annulées que si l'existence d'un dommage peut être prouvé. Selon certains spécialistes, la géolocalisation est un outil utile pour localiser le téléphone portable d'une personne suivie en temps réel sur le territoire national[1522].

[1517] E. Verges, « *Géolocalisation en temps réel d'un téléphone : sauvetage d'une preuve illicite* », Revue AJ Annual, no.23-81, 2024. p.208. Professeur Verges analyse la décision de la Cour de cassation française de déclarer incompatibles au droit de l'Union Européenne les dispositions des articles 230-32 et 230-33 du code de procédure pénale français. Il convient de noter, cependant, que si nous parlons de délits graves tels que le crime organisé ou le trafic de drogue, dans la pratique judiciaire les géolocalisations ne sont pas sanctionnées, même si elles durent plusieurs mois.

[1518] Cour de cassation, Chambre criminelle, *22 Octobre 2013 – n° 13-81.945*. https://www-lexis360intelligence fr.

[1519] Cour Européenne des Droits de l'Homme, 5e section, *2 Septembre 2010 – n° 35623/05* https://www lexis360intelligence-fr. Dans ce cas, bien que la CEDH ait décidé que l'article 8 de la Convention n'était pas violé, elle a formulé certaines recommandations :

- la décision doit être proportionnelle à l'infraction
- la surveillance GPS ne doit être effectuée qu'après l'échec d'autres méthodes.
- la durée de la surveillance doit être limitée (environ 3 mois)
- l'existence obligatoire de garanties légales contre les abus

N.B dans ce cas il s'agit de surveiller le véhicule du contrevenant avec un dispositif GPS, à son insu et sans son consentement.

[1520] *Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation* https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000028790796

[1521] Const. *21 mars 2019, no. 2019-778 DC*., représente l'une des décisions la plus longue du Conseil constitutionnel en France, avec environ 400 paragraphes, où la conformité des dispositions de la « *loi de programmation 2018-2022 et la reforme de la justice* » avec les principes constitutionnelles est évaluée. https://www.conseil constitutionnel.fr/décision/2019/2019778DC.htm

[1522] Crim. *9 février 2016, no. 15-85.070* sur la géolocalisation à l'étranger nécessitant l'acceptation préalable ou concomitante de l'État étranger.

D. Droit à la vie privée versus droit à la liberté d'expression

532. Atteintes à la vie privée, justifiées par le droit à la liberté d'expression. Cependant, il existe des situations où l'on tente de justifier l'atteinte à la vie privée en invoquant un autre droit fondamental, à savoir la liberté d'expression, notamment dans les médias, en cas de surveillance numérique ou de publication de renseignements personnels[1523]. Un exemple célèbre dans ce cas est l'affaire Von Hannover contre Allemagne (CEDH, no. 59320/00), où la Cour européenne des droits de l'homme examine la publication sans consentement de certaines photographies de la princesse Caroline de Monaco. La Cour relève que, bien que la liberté d'expression comprenne la publication de photographies (loi garantie par l'article 10 de la CEDH)[1524], en l'espèce, la vie privée est primordiale et il y a violation de l'article 8 de la CEDH[1525].

533. Restriction de la liberté d'expression par la protection de la vie privée. Le respect du droit à la vie privée peut constituer une restriction au droit à l'expression[1526]. Toutefois, ce droit doit être exercé avec certaines restrictions afin d'assurer la protection de la réputation et des droits des autres. Lorsque des images du corps du défunt et le visage visible du préfet de Corse apparaissent dans la presse, les tribunaux français décident que l'action a violé le droit à la vie privée de la famille du défunt. Et la CEDH décide que la publication de la photo peu après, sans le consentement de la famille a accentué sa souffrance, constituant une atteinte à la vie privée. La Cour ne considère pas que l'article 10 de la CEDH ait été violé en l'espèce[1527].

Actuellement, la plus large portée du concept de vie privée est traitée par la Cour Européenne des Droits de l'Homme, y compris toutes les informations personnelles, ainsi que les tendances religieuses, politiques, morales, philosophiques, mais aussi les relations émotionnelles, familiales, conjugales et même les relations professionnelles (appartenant normalement à la sphère publique)[1528].

[1523] M. Harris, K. Hughes, *Privacy and Free Expression: Competing or Complementary Rights?*, en J. Lewis, P. Crick (ed.), *Media Law and Ethics in the 21st Century: Protecting Free Expression and Curbing Abuses*, Hart Publishing, 2014. p.151-166. https://doi.org/10.1057/9781137312648_8

[1524] *Convention européenne des droits de l'homme* https://www.cncdh.fr/sites/default/files/2022-02/cedh_0_1.pdf

[1525] Affaire *von Hannover c. Allemagne, requête no 59320/00*. https://juricaf.org/arret/CONSEILDELEUROPE-COUREUROPEENNEDESDROITSDELHOMME-20040624 5932000

[1526] La liberté d'expression est garantie par l'article 10 de la Convention européenne des droits de l'homme. Ce droit implique la liberté d'opinion, la possibilité de communiquer des informations, considérées comme indispensables dans une société démocratique https://legislatie.just.ro/Public/DetaliiDocumentAfis/175187

[1527] Cour Européenne des Droits de l'Homme, 1re section, *14 Juin 2007 – n° 71111/01*. https://juricaf.org/arret/CONSEILDELEUROPE-COUREUROPEENNEDESDROITSDELHOMME-20070614 7111101

[1528] N. Cazé-Gaillarde, *Atteintes à la vie privée – Frontières incertaines de la vie privée*, Jurisprudence de la Cour Européenne des droits de l'homme, 2019 (mise à jour: Mai 2023)

§2. AUTRES RÉGLEMENTATIONS JURIDIQUES ÉTROITEMENT LIÉES À LA VIE PRIVÉE

A. Fabrication, installation et promotion de dispositifs d'espionnage

534. Réglementation des dispositifs d'interception. L'article 226-3 alinéa 1er du Code pénal français[1529] concerne le contenu de l'acte d'interception illégale des communications, ainsi que l'installation de dispositifs destinés à capter ou enregistrer des conversations privées.

Le premier alinéa de cet article a subi des modifications importantes[1530], sa forme en vigueur criminalisant l'acte d'importer, fabriquer, détenir, exposer, offrir, louer ou vendre sans autorisation ministérielle, des dispositifs ou appareils techniques destinés à effectuer des opérations qui pourraient constituer l'infraction de violation du secret de la correspondance[1531], ou qui permettent l'infraction visée à l'article 226-1 ou la collecte de données informatiques[1532], lorsqu'ils sont conçus pour la détection à distance des conversations.

535. Fabrication de dispositifs sans autorisation. Ainsi, afin de prévenir la commission de ces infractions, la fabrication de ces dispositifs sans autorisation[1533] est sanctionnée. La spécificité de ce fait peut être constatée par la résolution infractionnelle de l'auteur, pouvant éventuellement être exécutée « même par négligence », cet aspect transformant l'acte en une simple infraction commise par imprudence[1534].

Il convient de noter que l'article 226-3 ne couvre que les dispositifs utilisés pour la détection à distance des conversations destinées à capturer des mots et/ou des données informatiques, étant exclus du champ d'application de la criminalisation des dispositifs utilisés pour capturer, enregistrer ou transmettre illégalement les images d'une personne.

536. Autorisation des dispositifs de surveillance. Afin de satisfaire à la typicité de l'acte, le dispositif en question doit être inscrit sur la liste établie par décret du Conseil d'Etat, le

---

[1529] L'article a été modifié nombreuses fois, la dernière réglementation étant la *Loi no. 2020-936 du 30 juillet 2020 – art. 1er*, en vigueur à partir du 1er août 2020, en reprenant les dispositions de l'ancien article 371 du Code pénal.
[1530] Sa rédaction a été modifiée par l'article 36 de la *loi no. 2011-267 du 14 mars 2011 relative à l'orientation et à la programmation pour la performance de la sécurité intérieure*, par l'article 44 de *l'ordonnance no. 2011-1012 du 24 août 2011 relative aux communications électroniques*, par l'article 23 de la *loi no. 2013-1168 du 18 décembre 2013 sur la programmation militaire pour les années 2014 - 2019 et diverses dispositions relatives à la défense et à la sécurité nationales,* ainsi que d'autres actes normatifs ultérieurs.
[1531] Avec référence à *l'art. 226-15 al. 2 du C. pén*.
[1532] Prévues par les *articles 706-102-1 du Code de procédure pénale* et *L. 853-2 du Code de la Sécurité Intérieure.*
[1533] Cour d'appel, Rennes, Chambre correctionnelle 3, 14 Novembre 2000 https://www-lexis360intelligence-fr.
[1534] L'article 44 de *l'ordonnance no. 2011-1012 du 24 août 2011 sur les communications électroniques* a modifié la formulation de l'article 226-3, précisant que l'infraction est constituée lorsque ces actes sont commis « *y compris par négligence* ».
Au départ, faute d'indication contraire, il a été considéré que l'infraction ne pouvait être commise que sous une forme intentionnelle, en ce sens que l'auteur agissait en sachant que le dispositif en question pourrait permettre les infractions visées à l'article 226-3 et que ce dispositif n'avait pas été autorisé.

législateur ayant pour objet de contrôler les dispositifs miniaturisés utilisés dans le commerce clandestin, également appelés « espions domestiques »[1535]. L'achat ou la possession d'un tel dispositif nécessite une autorisation et la demande exige l'engagement des contrôles et vérifications prévus[1536].

537. Sanctionner la promotion des dispositifs d'espionnage. L'article 226-3, paragraphe 2, sanctionne la publicité d'un dispositif susceptible de permettre la commission de l'acte de capture illicite de mots ou d'images, respectivement les opérations susceptibles de toucher le secret de la correspondance; comme nouveauté, il sanctionne également la publicité d'un moyen technique susceptible de produire les mêmes effets[1537].

L'acte de publicité peut être représenté par toute action (par des moyens écrits ou audiovisuels) dans la mesure où il maintient son but de faire connaître le dispositif en question au public. Toutefois, un acte de publicité qui se limite à la présentation des matériaux techniques d'un tel dispositif ne relève pas du contenu constitutif d'une infraction et il est essentiel qu'il constitue une incitation, sous forme de provocation ou d'incitation, à la commission d'actes illicites de capture prévus aux articles 226-1 et 226-15, alinéa 2 du Code pénal.

538. Définition des comportements illicites. Au moyen de ce règlement, à savoir en criminalisant les comportements qui sont susceptibles de toucher les éléments liés à la sphère privée de la personne, on peut constater le souci du législateur pour l'éducation pénale préventive. Étant donné que les limites de cette éducation préventive sont sensibles, le législateur a concrètement défini les comportements qu'il considère comme illicites et qu'il signale sanctionner si le résultat proposé à éviter s'est produit.

Toutefois, l'article limite la portée illicite en n'exigeant pas la possession ou l'acquisition par les opérateurs désignés[1538] pour exercer l'activité d'un opérateur de réseau de communications électroniques ouvert au public, ni les dispositifs soumis à l'autorisation du Premier ministre[1539].

[1535] La procédure d'autorisation de ces dispositifs a été modifiée par le *décret no. 2016-67 du 29 janvier 2016 relatif aux techniques de collecte de l'information*. Elle est régie par les articles R. 226-1 – R. 226-12 du Code pénal. L'article R. 226-1 stipule que la liste des dispositifs visés à l'article 226-3 est établie par l'arrêté du Premier Ministre et l'arrêté du 11 août 2016 (publié au JO le 25 août) vient compléter cette liste.

[1536] Selon *l'art. 226-8 du Code pénal*, modifié par la *loi no. 2016-67 du 29 janvier 2016*.

[1537] L'article 226-3, paragraphe 2, ne sanctionne que l'acte de publicité en faveur d'un dispositif susceptible de permettre la commission des infractions de capture illicite de mots ou d'images (C. Pen., art 226 1), ainsi que de la violation du secret de la correspondance (C. pen., art. 226-15, al. 2). La loi no. 2011-267 du 14 mars 2011 a étendu le champ d'application de cet article, visant non seulement « les dispositifs », mais aussi, désormais, « *les moyens techniques* ». Cela comprend, outre les dispositifs ou moyens techniques permettant la commission des infractions visées aux articles 226-1 et 226-15, les dispositifs ou moyens techniques « *destinés à capter les données informatiques visées aux articles 706102-1 du Code de procédure pénale et L. 853-2 du Code de sécurité interne* ».

[1538] Ils sont mentionnés à *l'article L.1332-1 du Code de la Défense*.

[1539] Il est fait référence à la loi no. 2019-80 du 1er août 2019, qui stipule au 3ème alinéa de l'article 226-3 que l'article « *ne s'applique pas à la possession ou acquisition par les opérateurs visés à l'article L. 1332-1 du Code de Défense, désignés en vertu de leur activité d'opérateurs d'un réseau de communications électroniques ouvert au*

B. Réglementation du délit d'atteinte à la vie privée par deepfake

539. Introduction du terme « deepfake » dans le droit pénal français. En se référant à la notion de *deepfake*[1540], le Code pénal français désigne, par les articles 226-1, 226-2-1 et 226-8 et 226-8-1, l'acte illicite de captation et de diffusion d'images ou de mots d'autrui dans certaines circonstances prédéfinies. Le terme *deepfake* vient de la combinaison des mots « deep learning » et « fake » et fait référence à une technologie avancée qui utilise des algorithmes d'intelligence artificielle dans le but de produire du contenu audio, vidéo et image qui montre une apparence réelle. Le but de la création d'un tel contenu n'est pas essentiellement négatif, comme la manipulation, la désinformation, le chantage, la manipulation de l'opinion publique ou la diffamation, *deepfake* peut être utilisé dans le domaine du divertissement ou de l'éducation.

540. Deepfake, utilisé dans des activités illégales. Cependant, lorsqu'il est utilisé à des fins illicites, *deepfake* peut sérieusement affecter certains aspects de la vie privée d'une personne. Afin de prévenir les préjudices et de protéger implicitement les droits de l'individu, la France, ainsi que d'autres États, ont criminalisé l'acte de violation de la vie privée en utilisant et en distribuant des documents à caractère de *deepfake*.

L`atteinte à la vie privée peut se produire par *deepfake* selon l'article 226-1 du Code pénal, sous les hypothèses suivantes : l'activité de capture, d'enregistrement ou de transmission, sans le consentement de leur auteur, des mots prononcés à caractère privé ou confidentiel est traitée à l'aide d'algorithmes d'intelligence artificielle pour créer un contenu faux; l'activité consistant à enregistrer ou à transmettre, sans le consentement de la personne, l'image d'une personne trouvée dans un lieu privé est traitée à l'aide d'algorithmes d'intelligence artificielle pour créer du faux contenu; l'activité de capture, d'enregistrement ou de transmission, par

---

public, aux dispositifs soumis à l'autorisation du Premier ministre en vertu de la section 7 du chapitre II du titre I du deuxième livre du Code des postes et des communications électroniques ».

[1540] Par ailleurs, sous l'impulsion de réprimer les effets engendrés par le phénomène deepfake, la France est actuellement à la tête du projet de *loi SREN,* adopté par une commission paritaire le 10 avril 2024.

Si l'on se réfère au manque de contrôle significatif et à la croissance du nombre de délits dans le contexte de l'utilisation de l'intelligence artificielle dans le travail de tromper la voix et l'image d'une personne, la nécessité d'un tel projet ne peut être contestée.

En particulier, cette initiative législative proposait de modifier le premier alinéa de l'article 226-8 du Code pénal comme suit : « *Elle est assimilée à l'infraction visée dans ce paragraphe et punie des mêmes sanctions, porter à la connaissance du public ou d'un tiers, par quelque moyen que ce soit, un contenu visuel ou sonore généré par un algorithme et représentant l'image ou les mots d'une personne, sans son consentement s'il n'est pas évident qu'il s'agit de contenu généré par des algorithmes ou si cela n'est pas explicitement indiqué* ».

Par ce projet, il n'a pas été jugé nécessaire de modifier la sanction prévue par le Code pénal actuel, en conséquence, la conduite infractionnelle reste à sanctionner comme auparavant, avec deux ans d'emprisonnement et une amende de 45.000, selon l'art. 226-8 Code pénal.

quelque moyen que ce soit, de la localisation en temps réel ou retardée d'une personne, sans son consentement, est traitée à l'aide d'algorithmes d'intelligence artificielle pour créer du faux contenu.

541. Les infractions numériques : nouveautés en droit pénal. La criminalisation officielle de l'acte d`atteinte à la vie privée commise par l'utilisation d'algorithmes d'intelligence artificielle à des fins de contrefaçon et de distribution sans consentement de l'image, du son, de la localisation d'une personne[1541], est une nouveauté en droit pénal français. À cet égard, la typicité vise l'acte de porter à l'attention du public ou d'un tiers, par quelque moyen que ce soit, un contenu visuel ou sonore traité au moyen d'algorithmes d'intelligence artificielle, aux fins de contrefaçon, de distribution de l'image, la voix ou la location d'une personne[1542].

Les dispositions de l'article 226-2-1, alinéa 1er du Code pénal français vise à renforcer le mur de protection de l'intimité de nature sexuelle de la personne, en sanctionnant le *deepfake* matérialisé par le traitement, au moyen d'algorithmes d'intelligence artificielle et afin de créer du faux contenu, de tout enregistrement ou transmission, sans le consentement du propriétaire, dans un lieu privé, des mots de nature sexuelle prononcés avec un caractère confidentiel ou privé; de toute action visant à enregistrer ou à transmettre, sans le consentement de la personne, l'image sexuelle dans un lieu privé; de toute action d`enregistrement ou transmission de nature sexuelle, par quelque moyen que ce soit, de la localisation en temps réel ou tardive d'une personne sans son consentement.

542. De l'algorithme à l'infraction. En outre, les dispositions de l'article 226-2-1, alinéa 2 du Code pénal français sanctionnent le *deepfake* réalisé par traitement à l'aide d'algorithmes d'intelligence artificielle pour créer du faux contenu, en l'absence du consentement qui aurait dû être donné pour la diffusion, l'activité consistant à faire connaître au public ou à un tiers tout enregistrement ou document faisant référence à des mots ou images de nature sexuelle, qu'ils aient été obtenus avec le consentement, le consentement présumé, ou même par lui-même, au moyen d'un des actes visés à l'article 226-1.

L'objectif principal de ces dispositions est de prévenir et de combattre les interférences dues à la diffusion de matériel vidéo ou audio privé de nature sexuelle par le biais des technologies numériques[1543]. Plus précisément, le règlement reflète l'engagement de protéger la dignité de nature sexuelle et de la placer dans la catégorie des libertés protégées dans l'espace numérique[1544].

[1541]D. Gridel, „*Dignité de la personne humaine et liberté de l'information d'actualité*", Dalloz, chron.872, 2001.
[1542] Ibidem.
[1543] Pour une analyse en détail, voir l`opinion de W. Burroughs, „*Révolution numérique*", Paris, Allia Éditions, 2017 versus 1970.
[1544] Pour une analyse en détail, voir l`opinion de D. Serinet, „*L'instauration d'une répression des atteintes à l'intimité sexuelle par la loi pour une République numérique*", Point de vue, 2016. pp.1711.

543. Attirer l'attention du public grâce à l'utilisation de deepfakes. Les dispositions de l'article 226-8 du Code pénal français criminalisent le deepfake commis par l'activité spécifique d'attirer l'attention du public ou d'un tiers, à l'exclusion des moyens, du montage réalisé avec les mots ou l'image d'une personne sans son consentement, dans le cas où il ne présente pas la preuve du montage, ou dans le cas où la mention expresse de l'existence d'un montage n'est pas faite; respectivement par l'activité de faire connaître au public, ou à un tiers, par quelque moyen que ce soit, de contenus visuels ou sonores générés par traitement algorithmique et qui représentent l'image ou les mots d'une personne, mais sans son consentement, soit dans le cas où il n'est pas évident qu'ils soient considérés comme des contenus générés par l'intelligence artificielle, ou dans le cas où aucune mention expresse n'est faite à cet égard. En outre, lorsque les faits mentionnés dans les hypothèses ci-dessus sont commis par le biais d'un service public de communication en ligne, le législateur criminalise la variante aggravée de l'infraction.

Ces règlements mettent en évidence le souci du législateur pour la protection de la dignité de la personne, implicitement la responsabilité de l'auteur pour l'acte de manipulation de la technologie, afin de nuire à d'autres personnes par la tromperie et la falsification de données privées réelles. Il est clair que la criminalisation du délit de *deepfake* vise à trouver un équilibre entre l'utilisation de la technologie et le respect des règles de conduite légales, éthiques et de conduite pénale.

Comme nous l'avons vu, la loi sanctionne la distribution de matériel truqué à l'aide d'algorithmes, contenant des éléments de la véritable identité d'une personne qui ne donne pas son consentement à l'acte de porter à l'attention d'autrui, étant donné que le matériel trompé ne présente pas suffisamment d'éléments évidents pour être présumé trompé, ni n'inclut pas la mention de réalisation d`un trucage[1545].

544. Non-incrimination des deepfakes explicitement étiquetés. *Per a contrario*, la loi n'inclut pas les documents *deepfake* marqués avec des mentions spécifiques, comme « le matériel généré par l'intelligence artificielle ». La raison réside dans le fait que, par exemple, semblable au processus d'un montage photographique, tant qu'il y a des preuves d'un matériel irréel généré par un algorithme, ou du moins aussi longtemps que l'origine de l'IA est explicitement mentionnée, l'acte n'a pas de typicité pénale. En ce qui concerne la pertinence et l'applicabilité de cette exception, certains auteurs considèrent que le règlement a la capacité de créer une confusion[1546], notamment sur les réseaux sociaux, où la mention de la source est

[1545] Voir en ce sens l`opinion de C. Gaillards, „*Secret et citoyen – les risques technologiques de l'information*", Entretiens de Nanterre, 1996.

[1546] Pour une analyse en détail, voir l`opinion de Philippe Mouron, affirmant que cette confusion est un sujet qui „ *devient encore plus sensible en contexte des élections européennes"*, dans l`article „*La loi visant à sécuriser et è réguler l'espace numérique est promulguée*", Revue européenne des médias et du numérique, no 69-70, 2024, pag.35-39.

souvent omise à l'activité de redistribution du matériel truqué, nombreux de ces traitements algorithmiques étant distribués par les utilisateurs sur un ton neutre, licite, ou en soutenant des idéologies politiques et sociales.

En plus de l'article analysé ci-dessus, le Code pénal français criminalise par l'article 226-8-1, alinéa 1, une nouvelle manière spécifique de type *deepfake*, à savoir la diffusion d'un montage sexuel, à savoir la diffusion d'un contenu visuel ou audio de nature sexuelle généré par le traitement algorithmique, ou la reproduction de l'image ou des mots d'une personne, sans son consentement.

545. Exclusion des sanctions pénales pour les professionnels de la presse. D'une part, le législateur exclut de sanctionner au titre du Code pénal les personnes des médias écrits ou audiovisuels responsables de l'acte commis au premier alinéa, justifiant ainsi qu'elles soient soumises aux sanctions propres à la législation spéciale.

546. Sanction aggravante par la publication en ligne. D'autre part, le législateur impose une sanction aggravante en cas de publication du montage ou du contenu généré par un traitement algorithmique effectué à l'aide d'un service public de communication en ligne.

547. Mise à jour de la doctrine traditionnelle face à la technologie. Il est nécessaire de mettre à jour les mesures juridiques traditionnelles afin de créer un cadre qui soit adapté pour être applicable même dans l'espace des technologies numériques, à ce titre, nous considérons que les réglementations en vigueur contribuent de manière substantielle à maîtriser la réaction aux risques et menaces générés par les nouvelles technologies. Cependant, certains auteurs sont sceptiques quant à la capacité de l'individu à s'adapter et à percevoir profondément la personnalité de la technologie numérique[1547]. Ainsi, ils soulèvent des questions sur le caractère utopique[1548] de l'applicabilité du nouveau cadre législatif, donnant à cet égard l'exemple du délit de contrefaçon commis dans le monde physique. En l'espèce, leur question porte sur la capacité d'adapter et d'appliquer le délit de contrefaçon traditionnellement commis par référence au même acte commis dans l'espace numérique[1549].

548. Systèmes technologiques modernes, système OASYS. Enfin, on ne peut manquer de remettre en cause les débats qui se tiennent au niveau international dans le domaine de la justice pénale[1550] sur la compétence absolue des autorités pour accéder aux algorithmes d'évaluation

---

[1547] Pour une analyse en détail, voir l`opinion de J. Bossan, „*La protection de la représentation à l'ère du numérique et du deepfake: le délit de montage version 2.0*", Légipresse n°426, 2024. www.legipresse.com/011-52531-la-protection-de-la-representation-a lere-du-numerique-et-du-deepfake-le-delit-de-montage-version-2-0.html

[1548] Ibidem.

[1549] L'infraction de falsification a été introduite à l'origine par la Loi Ancienne du 17 juillet 1970 sous le nom de « trucage », son objectif principal étant de protéger l'image des personnes contre les manipulations intentionnelles par des mots ou des images destinés à donner une perception fausse ou déformée de celles-ci.

[1550] En ce sens, nous donnons l`exemple de Grande Bretagne, qui travaille pour apporter des modifications essentielles à la Loi de la justice pénale (Criminal Justice and Immigration Act 2008 și LASPO Act 2012).

prédictive du risque, comme source d'information pour la condamnation des délinquants dangereux. À ce titre, la question se pose de savoir si les systèmes OASYS et d'autres systèmes technologiques utilisés par les organismes de justice pénale du monde entier pour évaluer le risque d'un délinquant diffèrent considérablement des technologies utilisées dans le contexte commercial. La première collecte des données limitées, spécifiques aux variables présélectionnées obtenues par les méthodes traditionnelles (telles que les enquêtes au sein des prisons)[1551], qui sont ensuite introduites et traitées par un système algorithmique automatisé. Le deuxième recueille des quantités massives de données sur toute personne, générées par leur activité en ligne, et ensuite les données sont saisies et traitées au moyen d'algorithmes automatisés. Les discussions portent sur l'étendue de la limite légale entre l`intérêt social[1552] et individuel, les deux situations incluant le traitement des données à travers l'intelligence artificielle. Sur ce point, nous estimons qu'un examen plus approfondi s'impose, car il n'est pas encore entièrement clarifié, dans l'un ou l'autre des deux contextes présentés, le risque d'utilisation de l'intelligence artificielle sur la vie privée de la personne, avec ou sans antécédents infractionnels[1553]. Jusqu'à présent, l'impact de ces calculs algorithmiques sur le risque des décisions judiciaires[1554] n'a pas encore été évalué et la mesure dans laquelle le système de justice pénale pourrait exploiter l'automatisation des données disponibles d'une

---

En outre, le projet de loi concernant la lutte contre le terrorisme (Sentencing and Release) et le Projet de loi concernant les jugements, présentés dans le Discours de la Reine en décembre 2019, apporterons de nouvelles modifications aux dispositions sur le danger au sein de Criminal Justice Act (CJA) (Bureau du Premier Ministre, 2019). Consulter https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/853886/Queen_s_Speech_December_ 2019_-_background_briefing_notes.pdf.

[1551] Consulter en ce sens la thèse „*Prison Reform Trust, Offender Management and Sentence Planning*", Prison Reform Trust, 2019. www.prisonreformtrust.org.uk/ForPrisonersFamilies/PrisonerInformationPages/ OffenderManagementandsentenceplanning.

[1552] Voir B.E. Harcourt, (*5.Généalogie du Doppelgänger numérique*), p.66, un projet de loi sur les effets des peines à l'aide d'algorithmes, visant « *à faire en sorte que les délinquants violents et sexuels les plus dangereux passent une période de temps en prison correspondant à la gravité de leurs dé.lits, protégeant ainsi les victimes et donnant confiance au public* ». Pour une discussion sur la frontière entre la justice rétributive et l'incapacité à punir, voir von Hirsch et Ashworth (n 24).

[1553] Pour une image d`ensemble sur les discussions de Grande Bretagne, consulter

- K. Hannah-Moffat, P. Maurutto. *Re-contextualizing pre-sentence reports: risk and race*, Punishment and Society, vol.12(3), 2010.
- S. B Starr, „*Evidence-based sentencing and the scientific rationalization of discrimination",* Stanford Law Review, vol.66, *2014.*
- J. Monahan, J. L Skeem, „*Risk assessment in criminal sentencing",* Annual Review of Clinical Psychology, 2016.

Pour une révision d`utilisation des algorithmes au niveau international, voir :

- G. van Eijk, „*Socioeconomic marginality in sentencing: the built-in bias in risk assessment tools and the reproduction of social inequality*", Punishment and Society, vol.19(4), 2017
- Annison (n 2) ch 8.

[1554] Cependant, la possibilité et la disponibilité de programmes d'évaluation qui permettraient à un détenu de réduire son niveau de risque pendant l'emprisonnement ne sont pas garanties, et en raison du manque de tels services, le Royaume-Uni a été sanctionné pour manquement à ses obligations en vertu de l'article 5 dans *l'affaire James, Wells et Lee c. UK (2012) 56 EHRR 159* ; pour une discussion plus approfondie, voir A. Ashworth, L. Zedner. "*Prevention and Criminalization: Justifications and Limits*", New Criminal Law Review, vol.15, no.4, 2012. pp. 542–71.

personne n'a pas été établie. À ce titre, nous devrions nous concentrer davantage sur la compréhension de l'effet de l'utilisation des systèmes d'évaluation automatisés généralement utilisés par rapport à l'effet de l'utilisation des systèmes prédictifs automatisés dans la justice pénale, afin d'établir clairement les limites dans lesquelles une personne peut exercer son droit à la vie privée.

C. Le régime juridique du délit d'atteinte à la vie privée envisagé sous l'angle de la privacy

549. Le concept anglo-américain de *privacy*. La notion de *privacy* est un pilier essentiel et déterminant des bonnes pratiques dans une société moderne. Cependant, bien qu'indispensable et omniprésent dans la vie privée d'une personne, le *privacy* nous apparaît comme ayant un caractère plutôt relatif en termes de son expression concrète et de son applicabilité dans la vie de la personne. À ce titre, nous tenterons de comprendre les raisons pour lesquelles, tout en subsistant dans la plupart des aspects de la vie privée humaine, le concept de *privacy* connaît des variations dans la façon dont il est réellement compris et appliqué.

Dans les relations entre personnes, la confidentialité est vue comme un principe concret, explicite, contractuel, compris et perçu dans le contexte de la manifestation d'une liberté, non d'une interdiction[1555]. Par exemple, dans la Common Law, la confidentialité est définie soit explicitement, en tant que terme contractuel, ou implicitement, comme une mesure d'équité par rapport aux autres. Tout comme le droit à la protection des données, le principe de confidentialité[1556] n'interdit pas un comportement, mais crée au contraire un environnement dans lequel certains comportements peuvent avoir lieu. Ainsi, d'une part, en ce qui concerne la définition du droit à la vie privée, l'article 12 de la Déclaration universelle des droits de l'homme[1557] établit que le droit à la vie privée n'est pas absolu[1558], il y a toujours des exceptions,

[1555] Voir *Francome c. Mirror Group Newspapers* Ltd, 1984.1, WLR 892, UK.

[1556] La Cour européenne des droits de l'homme a rendu de nombreuses décisions sur le droit au respect de la vie privée, établissant une norme pour résoudre les situations où les parties n'ont pas conclu d'accord. Les arrêts de la Cour ne donnent pas une définition complète de la confidentialité, reflétant ainsi toute la diversité des vulnérabilités humaines. Cependant, chaque décision définit un point précis dans l'éventail de ces vulnérabilités, en réponse à une situation particulière. La difficulté réside dans la tentative d'extrapolation de ces jugements pour définir la confidentialité comme un concept général, au-delà des cas concrets pour lesquels ils ont été formulés.

[1557] *L'article 12 de la Déclaration universelle des droits de l'homme* stipule : « *Nul ne peut être soumis à une ingérence arbitraire dans sa vie privée, sa famille, son domicile ou sa correspondance, ni à des atteintes à son honneur et à sa réputation. Toute personne a le droit à la protection de la loi contre de telles ingérences ou attaques*. »

[1558] Pour une analyse détaillée du fait que le droit au privacy n`est pas un droit absolu, consulter l`opinion de :

- A. Smith, *The Theory of Moral Sentiments*, ed. K. Haakonssen, Cambridge University Press, 2002
- J. S. Mill, *Despre libertate,* 3e éd., Humanitas, 2014.

et l'article 8 de la Convention européenne des droits de l'homme[1559] montre que le « respect de la vie privée » nécessite une plus grande clarification pour devenir applicable. Ces règlements nous montrent que le droit à la confidentialité est conditionnel au droit concurrent d'une autre personne, la législation reconnaissant que, dans certaines situations, la confidentialité cède la place aux besoins des autres.

550. Types de confidentialité. La compréhension du concept de *privacy* peut se faire à travers la théorie de Warren et Brandeis, qui ont contribué de manière significative à la reconnaissance de l'expression du droit légal à la vie privée, à savoir le droit de la personne d'être laissée tranquille[1560]. Toujours dans le domaine de la génétique, le spécialiste A. L. Allen propose une typologie plus large de confidentialité, à savoir « la confidentialité physique », « la confidentialité propriétaire », « la confidentialité informationnelle » et « la confidentialité des décisions »[1561].

Le concept de *privacy* est valorisé dans le droit français sous quatre formes, à savoir le droit humain, le droit à la confidentialité juridique, le droit à la protection des données et le droit au consentement du titulaire.

Ensuite, lorsque nous faisons référence au droit de la personne à la vie privée par *privacy*, nous ferons référence au droit de la personne de bénéficier de la protection de la confidentialité de ses données personnelles et d'un consentement librement exprimé, en concurrence avec les interférences qui font l'objet de la criminalisation de l`atteinte à la vie privée[1562]. Pour simplifier l'approche, nous utiliserons à la fois le terme de *privacy* et le terme confidentialité.

a). Droit à la protection de la confidentialité de la correspondance par courriel

551. Protection des communications électroniques par la CEDH. La Convention européenne des droits de l'homme considère la communication par courriel comme un droit

---

[1559] *L'article 8 de la Convention européenne des droits de l'homme* énonce ce droit comme suit :
„1.Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.
2.Aucune ingérence d'une autorité publique dans l'exercice de ce droit n'est permise, sauf si elle est légale et nécessaire dans une société démocratique, dans l'intérêt de la sécurité nationale, de la sécurité publique, du bien-être économique du pays, pour la prévention des troubles ou de la criminalité, pour la protection de la santé ou de la morale ou pour la protection des droits et libertés d'autrui. "

[1560] S. D. Warren, L. D. Brandeis,'*The Right to Privacy',* Harvard Law Review, éd. 4(5),1890. p.193-220.

[1561] A. L. Allen, „*Genetic Privacy: Emerging Concepts and Values*" et M. A. Rothstein, „*Protecting Privacy and Confidentiality in the Genetic Era*", Genetic Secrets, Yale University Press, 1997. p.31–60. En outre, M. Allen souligne également la nécessité de protéger l'information et la confidentialité de la réputation ainsi que la confidentialité des décisions, notamment dans le contexte du droit des femmes de choisir.

[1562] D. Townend et all., „*Privacy Interests in Biobanking: A Preliminary View on a European Perspective*", ainsi que J. Kaye, M. Stranger, „*Principles and Practice in Biobanking Governance*", Farnham: Ashgate Publishing Ltd., 2009. p.137–159.

privé à *privacy*[1563] manifesté par le droit à la vie privée. Cependant, la jurisprudence ne donne pas toujours à la correspondance personnelle par courrier électronique un caractère exclusivement confidentiel, certains considérant que le caractère privé d'une correspondance ne peut être retenu qu'à travers le prisme d'un lien clair, individuel et personnalisé entre l'expéditeur et le destinataire[1564].

552. Protection pénale française des communications électroniques. Pertinent pour la protection de la confidentialité de la correspondance par courriel, le Code pénal français mentionne l'article 226-15. Elle prévoit que toute interception, détournement, utilisation ou divulgation illicite de la correspondance transmise par voie électronique, ou même par d'autres moyens, constitue une infraction. En outre, le Code pénal français criminalise également l'acte de mauvaise foi consistant à ouvrir, supprimer, retarder ou détourner une correspondance qui est arrivée ou non à destination et qui a été adressée à des tiers. Même la prise à la connaissance frauduleuse d'une correspondance est considérée comme un délit. Dans le même contexte, selon la loi française, est également incriminé l'acte de mauvaise foi consistant à intercepter, détourner, utiliser ou divulguer une correspondance transmise ou reçue par des moyens électroniques ou l'installation de dispositifs capables de permettre de telles interceptions.

La jurisprudence française considère qu'il est essentiel pour déterminer le caractère privé d'une communication par courrier électronique de démontrer un intérêt commun suffisamment clair entre ses destinataires, au titre de la notion de « communauté d'intérêts ». Autrement, lorsqu'il n'y a pas d'intérêt commun évident entre les destinataires de la communication, le contenu du courriel peut être apprécié par le tribunal comme étant destiné au domaine public, la correspondance perdant le droit à la confidentialité.

553. Communication à caractère public. Si la correspondance a lieu entre plusieurs destinataires, il est indispensable de prouver l'intérêt commun qui lie les destinataires afin de commettre l'infraction d'atteinte à la vie privée. À cet égard, la jurisprudence française considère comme une communication publique le courriel dans lequel « il n'existe pas de communauté d'intérêts » entre ses destinataires, notamment si le contenu du courriel mentionne des faits graves tels que la pédophilie, voyeurisme, possession de matériel pornographique interdit, usage de drogues pour commettre des actes pédophiles[1565].

[1563] Protégé par *l`article 8 de la CEDH*.

[1564] Dans la *décision no 143, au point 21*, la Cour de cassation française considère, dans l'affaire Nikon France, qu'une distinction supplémentaire doit être faite entre la correspondance personnelle et la correspondance professionnelle, seulement les courriels « personnels » pouvant être protégés par le droit à la vie privée de la personne au moyen de la confidentialité.

[1565] Voir en ce sens la Décision de la Chambre Criminelle de la Cour de cassation française *no. 13-87.885 du 6 janvier 2015*, analysée en Légipresse, no. 324, p.75,2015. condamnant à la diffamation publique la correspondance ciblant plusieurs destinataires qui n'étaient pas liés à un intérêt commun, représentant un grand nombre de personnes, d'entreprises, d'institutions publiques et des médias.

b). Droit à la protection des données personnelles et droit à l'oubli

554. Garanties de confidentialité grâce à la protection des données personnelles. L'expression des droits privés se reflète également dans le respect des données personnelles, le législateur visant à équilibrer les intérêts liés au traitement des données personnelles, respectivement de créer des conditions juridiques pour leur bon traitement[1566].

Les plus grands défis actuels concernent la confidentialité informationnelle, respectivement la confidentialité décisionnelle, toutes deux basées sur l'existence d'un consentement éclairé garantissant le respect du droit de l`homme à une liberté de choix libre et éclairée.

Le droit à la vie privée obtenu par la protection des données à caractère personnel, et implicitement le droit à l'oubli numérique, n'est pas clairement stipulé dans le Code pénal français, étant plutôt un droitdérivé de la législation européenne sur la protection des données personnelles, suite à la transposition du Règlement sur la protection des données personnelles et le droit à l'oubli[1567].

555. Le droit à l'oubli : fondement et garanties procédurales. L'utilité d'introduction du droit à l'oubli dans le contenu des dispositions visant la protection des droits privés, notamment aux articles 226-13 et 226-16 à 226-24[1568] du Code pénal français, ne peut être niée, sur le principe qu'elle peut intervenir dans tout contexte d'effacement de données à caractère personnel qui sont susceptibles d'affecter la zone privée de la personne. Bien que dérivé de la jurisprudence et de la législation européenne, le droit à l'oubli numérique est étroitement lié à la protection de la vie privée, car il permet aux individus de prendre la priorité dans la gestion des données qui pourraient nuire à leur réputation ou à leur vie privée en ligne. A cet égard,

---

[1566] Pour une image détaillée consulter Organization for Economic Co-operation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*", 1980. Voir également : *The OECD Privacy Framework*, OECD, 2013.

[1567] Voir l`opinion de l`auteur S. Engeman, J. Muhanna, „*Penal Protection of The Right to Digital Oblivion*", 3rd International Humanitarian Conference, Baghdad vol.001, issue01, 2024. p.001-337, qui considère que, au niveau européen, le droit à l'oubli est considéré comme un élément du droit au respect de la vie privée, protégé par l'article 8 de la Convention européenne des droits de l'homme, et la jurisprudence de la Cour de justice de l'Union Européenne (comme l'affaire Google Espagne de 2014) a renforcé l'applicabilité de ce droit aux moteurs de recherche et autres entités numériques.

[1568] Ces articles font partie de *l'article 5 - Atteintes aux droits des personnes résultant de fichiers ou traitements informatiques*, du *Code pénal français* qui comprend les articles 226-16 à 226-24.
L'article 226-16 a été modifié par la loi no 2024-449 du 21 mai 2024 - art. 59, comme suit : « *Le fait, y compris par négligence, d'effectuer ou d'avoir effectué un traitement de données à caractère personnel sans avoir accompli les formalités préalables à leur réalisation prévues par la loi est puni de cinq ans d'emprisonnement et de 300.000 euros d'amende. Les mêmes peines s'appliquent à l'acte, y compris de la négligence, d'effectuer ou d'avoir effectué un traitement qui a fait l'objet de l'une des mesures prévues à l'article 3° IV de l'article 20 de la loi 78-17 du 6 janvier 1978 relative au calcul, aux fichiers et aux libertés* ».

selon l'article 226-18, l'utilisation non autorisée de données compromettant ces droits est sanctionnée.

556. Incriminations spécifiques : conservation au-delà du délai, refus de suppression, divulgation. Afin de mettre en évidence la nécessité d'établir un rapport équilibré entre le droit à la protection des données et le droit à la vie d'une personne, nous renvoyons à un cas notable datant de 1997[1569], qui se situe aux origines de la norme de protection même après la mort, dans le cadre du livre « Le Grand Secret », écrit par le docteur Claude Gubler, médecin personnel de l'ancien président français François Mitterrand. Dans ce contexte, la Cour de cassation de France a jugé que toutes les informations publiées dans le livre par le médecin sont des données personnelles protégées par le principe de confidentialité[1570], les divulgations dans les pages du livre constituant une atteinte à la vie privée de l'ancien président. Cette décision constitue un précédent dans l'établissement du respect prioritaire de la confidentialité des données personnelles en tant qu'élément du droit à la vie privée[1571].

557. Droit à l'effacement des données. Droit à l'oubli numérique est un droit personnel, qui appartient à la catégorie des droits non patrimoniaux qui se réfèrent à la composante de la personnalité. Il donne aux internautes le pouvoir de contrôler les données et les informations précédemment publiées sur le réseau, avec la possibilité de les supprimer et de s'opposer à leur publication après une période déterminée[1572].

Bien qu'il ait ses origines dans le passé, le droit à l'oubli est devenu de plus en plus pertinent dans les débats actuels, si nous devons considérer l'évolution de la technologie et la propagation croissante des appareils électroniques. En conséquence, de nombreuses législations nationales devraient se concentrer sur la protection plus efficace de ce droit dans la sphère privée de la personne.

Cependant, la mise en œuvre pratique de la protection pénale dans ce domaine est compliquée, car le monde virtuel est difficile à réglementer et l'absence d'expertise technique parmi les autorités compétentes affaiblit la barrière protectrice offerte par ce droit.

[1569] Voir la Décision de la Cour de cassation du *16 juillet 1997*, *éditions Plon et Gubler*, 142 – Legicom nr. 20 – 1999/4, Annexe 6. La décision de la Cour constitue un précédent dans le domaine du respect de la vie privée, d'une part, la Cour accordant de l'importance à la liberté d'expression de la personne, mais, d'autre part, en établissant la priorité du respect du droit à la vie privée par rapport aux autres droits. A titre de sanction, la Cour maintient l'interdiction temporaire de distribution du livre et ordonne des dommages-intérêts de 10.000 francs aux consortiums Mitterrand, partagés entre la Maison d`édition Plon et Dr. Gubler.

[1570] J.P. Gridel, A. Lacabarats, „*Droit à la vie privée et liberté d'expression : fond du droit et action en justice*", Gaz. Pal., doctr.1632, 2002.

[1571] Parmi les infractions liées au droit à l'oubli numérique par référence au droit à la vie privée, le droit français énumère la conservation des données au-delà du délai autorisé, le non-traitement des demandes d'effacement, la divulgation illégale de données et l'absence de mesures de sécurité. Contrairement à la législation roumaine, qui ne comporte que des références succinctes, la législation française traite de ces questions plus en profondeur.

[1572] S. Sontag-Koenig. „*Sonorisation et fixation d'images: que reste-t-il de la vie privée*?", Revue AJ pénal, 2023. p.27.

558. Les limites de la loi. Une limite à la protection de la vie privée par le droit d'utiliser et de décider des données privées d'une personne a été fixée par la Cour de cassation le 10 septembre 2014, affirmant que l'utilisation d'un nom de famille en tant que méta-tag[1573] ne constitue pas une violation du droit au respect de la vie privée, à condition qu'il ne soit pas associé à d'autres données personnelles. L'acte risque d'être sanctionné uniquement de manière contraventionnelle, lorsque le contenu de la page à laquelle ce mot clé est associé est jugé inapproprié.

559. La nécessité de réglementations rigoureuses. À titre de suggestion, le législateur français et le législateur roumain devraient introduire des réglementations plus claires qui définissent précisément les conditions et paramètres de ce droit, compte tenu de la protection des données à caractère personnel et des particularités des interactions en ligne, puisque la fragmentation des textes juridiques sur le droit à l'oubli numérique par rapport au droit à la vie privée reflète le manque de réglementation claire et explicite de ce droit dans les deux législations.

c). Réglementation du délit d'atteinte à la vie privée par le biais du cyber-harcèlement

560. L'accès illimité à Internet, partie intégrante du droit à la liberté d'expression. Internet, au sens large, est un moyen indispensable pour réaliser le droit fondamental à la liberté d'expression, dans un monde globalisé et interconnecté, l'accès libre à Internet n'est plus perçu comme un privilège, mais plutôt comme une condition, une nécessité essentielle pour la libre expression des opinions.

Le Conseil constitutionnel de la France a souligné le lien étroit entre le droit à la vie privée et le libre accès à internet[1574], reconnaissant l'internet comme une plate-forme fondamentale pour promouvoir la diversité des points de vue et faciliter le dialogue. Sa position est également soutenue par le Conseil d'État[1575], qui affirme qu'Internet est devenu un moyen essentiel pour assurer l'égalité des chances dans l'expression des idées et la participation à la

[1573] Le terme « *méta-tag* » désigne une étiquette HTML utilisée pour fournir des informations sur le contenu d'une page web, mais qui n'est pas directement visible aux utilisateurs. Ces étiquettes sont placées dans la section « *en-tête* » de la page Web et peuvent contenir des informations telles que la description de la page, les mots-clés de recherche ou l'auteur de la page.

[1574] Le 10 juin 2009, le Conseil constitutionnel de France a débattu de l'importance du libre accès à internet dans le respect des droits à la vie privée, reconnaissant de l'importance des services de communication en ligne comme éléments essentiels pour promouvoir la démocratie et faciliter la liberté d'expression („*Regard au développement généralisé des services de communication au public en ligne ainsi qu'à l'importance prise par ces services pour la participation à la vie démocratique et l'expression des idées et des opinions*"), CEDH, *18 décembre 2012, nr. 3111/10*, commentaires de L. Marino.

[1575] Consulter l`opinion du Conseil d`État français, „*Le numérique et les droits fondamentaux"*, Documentation française, 2014, p.146.

vie publique et privée[1576], avec le droit d'accéder à Internet comme un droit fondamental[1577]. Laure Marino note également que le Conseil constitutionnel a élevé la liberté d'accès à internet au rang de droit fondamental. Marino explique que cette liberté a été « annexée » à la liberté d'expression, ce qui signifie que l'accès à internet est désormais intégré et enchâssé dans cette liberté. Ainsi, le Conseil constitutionnel a créé un nouveau « droit - liberté » : le droit d'accès à l'Internet, directement dérivé de l'article 11 de la Déclaration des droits de l'homme.

561. Accès à Internet et censure dans différents pays. En analysant la qualité de l'accès à Internet dans d'autres États, on constate que la liberté d'accès à celui-ci dépend de chaque État, certains optant pour la variante de l'utiliser[1578], d'autres pour l'option de le censurer[1579], en bloquant les noms de domaine ou les adresses IP. Ces limitations sont suffisantes pour comprendre la valeur du droit d'accès à la liberté d'expression dans l'environnement numérique[1580].

À l'échelle mondiale, il est difficile de protéger le droit à la vie privée dans l'environnement numérique, motivé par le manque de consensus des États sur le concept de protection de la vie privée en référence au droit à la liberté d'expression dans l'environnement

---

[1576] Voir l`opinion partiellement contraire du spécialiste V. Cerf qui soutient en „*Internet access is not a human right*", New-York Times, 2012, qu`Internet n`est pas un droit autonome, mais plutôt un outil facilitant l`exercice d`autres droits.

[1577] À cet égard, L. Marino, « *Le droit d'accès à internet, nouveau droit fondamental* », Recueil Dalloz, 2009, p.2045, soutient que l'accès à internet a été annexé au droit à la liberté d'expression, étant un nouveau « *droit-liberté* », dérivé de l'art. 11 de la Déclaration des droits de l'homme. Laure Marino était une spécialiste du droit public et numérique, très connue pour ses recherches approfondies sur les libertés fondamentales et les nouvelles technologies.

[1578] Consulter les propositions faites par la Commission française dans le « *Rapport du Haut Commissaire aux droits de l'homme* », 2011, A/HRC/17/27, qui montrent que les Etats ont pris connaissance distinctement et conformément à leur politique intérieure, l'accès de la personne à la liberté d'expression dans l'environnement numérique. Nous donnons quelques exemples pour montrer la tendance mondiale des États à associer l'accès à internet dans la catégorie des droits essentiels.

L'Estonie a été parmi les premiers pays à entreprendre la réforme du respect des droits de l'homme dans l'environnement numérique, offrant à chaque abonné un accès à internet à un coût uniforme, quel que soit le lieu, depuis 2000.

En rattrapage est venue la Finlande qui, en plus de la téléphonie et des services postaux, a reconnu l'Internet comme ayant la valeur d'un service universel essentiel depuis 2009. Par la suite, en 2010, le droit d'accès à l'environnement numérique est devenu un droit opposable à tout citoyen du pays, en ce sens que les fournisseurs étaient tenus de leur fournir une connexion minimale de 1 Mbit/s à un prix jugé raisonnable par la majorité.

L'Italie aussi a initié une réforme qui soutenait la réduction, voire l'élimination totale, des inégalités et des obstacles sous forme d'inégalités numériques.

[1579] Un exemple de censure peut être le cas de Raïf Badawi d'Arabie Saoudite qui a été condamné à 10 ans de prison, 1000 coups de fouet et une amende, simplement parce qu'il a commencé un blog sur l'influence néfaste de la religion dans son pays. Dans la même affaire, y compris son avocat, a été condamné à 15 ans de prison, uniquement pour avoir exercé son activité de défense pour son client. Voir la jurisprudence de la Cour de justice de Nouadhibou, décision du 24 décembre 2014.

Par contre, le 17 décembre 2023, le ministre-délégué en charge de la réforme numérique, Jean-Michel Barrot, a annoncé l'accès à l'internet haut débit pour tous les Français, même s'ils ne sont pas encore tous éligibles à la fibre. L'annonce s'inscrivait dans le cadre du projet initié en 2013, qui visait à assurer d'ici 2025 une couverture de toute la France par l'internet très haut débit. Le matériel est disponible à l'adresse www.dalloz actualite.fr/flash/constitutionnaliser-droit-d-access-nouvel-eldorado-du-navigateur-20.

[1580] Pour une opinion détaillée, voir l`opinion de M. Bardin, „*Le droit d'accès à internet: entre « choix de société » et protection des droits existants",* RLDI, 2013. nr. 91.

numérique. Ainsi, dans la jurisprudence et la législation nationales, les États ont choisi des interprétations différentes de la loi en question. Par exemple, la Cour constitutionnelle de l'Afrique du Sud définit le droit à la vie privée comme « le droit de vivre comme chacun veut »[1581]. La Cour suprême du Canada élève la protection de la vie privée à la sphère limitée de l'autonomie personnelle, où des choix privés et intimes sont organisés[1582]. Le Royaume-Uni reconnaît l'absence d'une définition claire[1583], tandis que les États-Unis se concentrent sur l'identification des comportements qui constituent des violations de ce droit, tels que l'intrusion dans la vie privée d'autrui, la divulgation d'informations pouvant fausser l'image réelle d'une personne, ou l'exposition publique abusive des aspects liés à la vie privée.

562. Réglementation du harcèlement par des moyens informatiques. L'article 222-33 du Code pénal français réglemente le harcèlement en ligne, ou « cyber-harcèlement », par les articles 222-33 et 222-33-2-2, alinéa 4 du Code pénal français, respectivement la publication répétée sur internet d'enregistrements sexuels, d`images ou de vidéos, cet acte étant considéré comme du harcèlement sexuel en ligne. Cette pratique est en constante évolution et suscite de plus en plus d'inquiétudes, y compris au niveau international. Par exemple, un tribunal des États-Unis a reconnu coupable de meurtre une jeune femme de 22 ans qui avait encouragé son petit ami à se suicider au moyen d'une série de messages texte envoyés les années précédentes.

563. Intimidation, circonstance aggravante. La loi renforçant la lutte contre les violences sexuelles et sexistes[1584] estimait que l'article 222-33-2-2 du Code pénal devait être modifié, dans le sens où l'infraction d'intimidation doit être reconnue comme une circonstance aggravante si un groupe de personnes agit ou incite ensemble la même victime, même si toutes les personnes du groupe n'ont pas contribué au comportement répété.

564. La répétition, circonstance aggravante. De même, la législation française représente comme une hypothèse le harcèlement en ligne et l'acte du groupe de personnes d'agir successivement contre la même victime, étant conscient que les actions représentent une répétition. Soulignant l'importance de la protection des droits privés de la personne, le

[1581] À cet égard, voir la décision de la Cour constitutionnelle d`Afrique de Sud du 4 avril 2007 en „Butterworths Constitutional Law Reports" concernant l`affaire „*NM and Other versus Smith and Others*", tome 7, 2007, p.751, pf.33.

[1582] Consulter en ce sens la Décision de la Cour suprême du Canada du 31 octobre 1997 en Rapports de la Cour suprême du Canada, tome 1997, no. 3, p. 844, pf 97.

[1583] Voir, à cet effet D. Calcutt, „*Report of the committee on privacy and related matters*", Cabinet de Sa Majesté (Her Majesty's Stationery Office), Londres, 1990, qui examine plusieurs décisions judiciaires, en mettant en évidence les difficultés que rencontrent la France et le Royaume-Uni pour établir un régime de protection de la vie privée adéquat. Parmi ces décisions, nous pouvons en citer une importante, celle du Tribunal de la Haute Cour de Nanterre, le 5 septembre 2017.

[1584] Il s`agit de la *loi no. 2018-703 du 3 août 2018*, sur le combat des violences sexuelles et sexistes, parur en JO du 5 août 2018, no. 7.

législateur prévoit des sanctions plus sévères lorsque les actes sont commis par le biais d'un service de communication en ligne ou d'un support numérique.

565. Menaces, chantage, cybervengeance : les composantes du harcèlement en ligne. En lien étroit avec ce type d'infraction, le Code pénal sanctionne, par l'infraction de chantage (article 312-10 C. pén.) et par l'infraction de menace avec violence (article R.623-1 C.pén.), l'acte de menacer un ancien partenaire par la publication d'enregistrements audio, d'images ou de vidéos à caractère sexuel dans le but de lui nuire. La commission même de ce type d`acte en contexte numérique a un correspondant à travers le concept de « cyber-harcèlement » et de « cyber-vendetta ».

566. Harcèlement psychologique. Afin de porter à la connaissance du public les affaires criminelles de « cyber-harcèlement » et de « cyber-vendetta, une communauté privée a été créée en France, portant le nom du groupe « Ligue du LOL ». Ainsi, par exemple, le groupe a évoqué le cas d'une jeune femme qui s'est suicidée suite au fait que des images indécentes, avec elle nue, ont été postées par d'anciens compagnons sur les réseaux sociaux. Ou le cas d'un jeune homme gay de 18 ans qui s'est jeté d'un pont à New York après que son colocataire a partagé une vidéo prise sans son consentement et dans lequel il était avec un partenaire.

Dans le même contexte et en relation avec le phénomène du « cyber-harcèlement » et de la « cyber-vendetta », la jurisprudence française considère qu'il est essentiel de sanctionner, par l'article 222-14-3 du Code pénal français[1585], les auteurs commettant des actes de violence psychologique manifestés dans le domaine du numérique[1586], quelle que soit la nature de ces actes.

§3. SANCTIONS PÉNALES

567. Peines. La version actuelle de l'article 226-1 du Code pénal français met en évidence, dès le premier alinéa, l'attitude de sévérité du législateur à l'égard de l'auteur de l'atteinte à la vie privée. Ainsi, à un niveau objectif, la volonté du législateur d'ajouter de la valeur à l'objectif de protection de la vie privée de la personne en augmentant la peine à « un an d'emprisonnement et une amende de 45 000 euros », par rapport à la version précédente du Code pénal[1587] qui

[1585] Il s`agit de la *loi no. 2010-769 concernant les violences spécifiques contre les femmes, les violences au sein des couples et leur impact sur les enfants*, parue en MO du 10 juillet 2010, p. 12762.
[1586] Nous faisons référence à l`infraction saisie dans le Code pénal par la loi du 9 juillet 2020, ayant pour finalité le combat plus efficace de la violence domestique.
[1587] Le 17 juillet 1970, le législateur français a introduit dans le Code pénal français les articles 368 et 369 qui punissaient l'atteinte à la vie privée d'une personne, à savoir la conservation, la divulgation ou l'utilisation non

prévoyait : pour la même infraction, soit une peine « d'emprisonnement de deux mois à un an et une amende de 2 000 F à 60 000 F, soit une seule de ces deux peines »[1588].

En matière d'opinion, bien que nous considérions raisonnable et contextuelle la nécessité d'imposer une sanction plus sévère, justifiée dans le contexte du souci d'assurer une protection de plus en plus efficace, cependant, le texte de la loi soulève des questions sur l'absence de la possibilité d'alterner entre la sanction carcérale et l'amende, dans la version en vigueur le législateur considérant qu'il est nécessaire d'appliquer une seule peine cumulative consistant en « emprisonnement et amende ». A ce titre, nous considérons que, dans certaines hypothèses, le texte de la loi pourrait risquer de dépasser le principe de proportionnalité des sanctions appliquées. D'autant plus qu'il existe actuellement une proposition de loi en discussion au Parlement Européen, concluant que la législation européenne n'est pas très développée sur cette question non plus. Sans faire de commentaires utopiques, nous nous demandons si la loi actuelle est suffisante pour protéger efficacement la vie privée. D'autant plus que le Code pénal français comporte des sanctions multiples[1589] qui peuvent paraître imparfaites à première vue.

A. Peines aggravantes dans le Code pénal français

568. Circonstances aggravantes: utilisation d'images intimes. Cherchant à souligner l'intérêt de protéger ce « noyau dur de la vie privée »[1590], le législateur a jugé impératif que les infractions touchant la sphère sexuelle de la personne comprennent des peines plus sévères.

Par la loi no. 2016-1321 du 7 octobre 2016, une sanction plus sévère a été introduite dans le cas où l'acte est commis sous l'effet d'une circonstance sexuelle. Ainsi, l'article 226-2-1, alinéa 1er du Code pénal prévoit que lorsque les infractions visées aux articles 226-1 et 226-2 concernent des mots ou images de nature sexuelle pris dans un lieu public ou privé, les peines

autorisée de mots ou d'images illégalement obtenus. L'introduction de dispositions légales intervenait pour compléter la protection esquissée par d'autres règles existantes : violation du domicile, atteinte au secret professionnel, atteinte à la correspondance.

[1588] Pour une analyse comparative de l'ancien Code pénal et le nouveau Code pénal, voir les opinions des spécialistes A. Chavannes, „*Protection de la vie privée dans la loi du 17 juillet 1970*", RSC, 1971 p.605; R. Badinter, „*La protection de la vie privée contre l'écoute électronique clandestine*", Semaine juridique, 1971. Chronique 2435 ; D. Bécourt, „*Réflexions sur le projet de loi relatif à la protection de la vie privée*", Gazette du Palais, 1970.

[1589] L'Article 226-1 sanctionne par un an d'emprisonnement et une amende de 45.000€ ces actes lorsqu'ils portent atteinte à la vie privée. L'article 226-2-1 sanctionne de deux ans d'emprisonnement et une amende de 60.000€ la diffusion de telles images qui, en plus de cela, sont sexuelles. L'article 226-8 semble le plus approprié, punissant d'un an d'emprisonnement et d'une amende de 15.000€ « *le montage réalisé avec l'image ou la voix d'une personne sans son consentement, s'il n'est pas évident que c'est un ajustement ou si cela n'est pas explicitement indiqué* ».

[1590] Voir le point de vue d'A. Lepage, *L'article 226-2-1 du Code pénal, une nouvelle strate dans la protection pénale de la vie privée*, Dr. Pénal, 1ère étude, 2017.

sont portées à deux ans d'emprisonnement et 60.000 euros d'amende ». Si l'on exclut les critiques sur la durée et le quantum de la peine, on peut toutefois constater une incohérence dans le texte de la loi visant à contraindre par des mesures sévères les atteintes causées « dans un lieu public ou privé », tandis que l'article 226-1, alinéa 2, relatif aux infractions sexuelles prévoit qu'elles ne peuvent être commises que dans un lieu public. Par conséquent, le texte de la loi doit être compris et appliqué strictement en ce qui concerne l'atteinte à l'image d'une personne dans un lieu privé.

De même, l'infraction définie à l'article 226-3-1 du Code pénal a porté les peines à 2 ans d'emprisonnement et 30.000 euros d'amende « si commise par une personne abusant de l'autorité conférée par ses fonctions ; (...) si elle est commise sur un mineur ; (…) lorsqu'elle est commise sur une personne dont l'auteur a connaissance ou qui est particulièrement vulnérable, en raison de son âge, de sa maladie, de son infirmité, de ses déficiences physiques ou mentales ou de son état de grossesse; (...) lorsqu'elle est commise par plus d'une personne agissant à titre d'auteur ou de complice; (…) lorsqu'elle est commise dans un véhicule destiné au transport collectif de passagers ou dans un lieu destiné à l'accès à un moyen de transport collectif de passagers ; (…) lorsque les images ont été fixées, enregistrées ou transmises »[1591].

B. Peines complémentaires dans le Code pénal français

569. Peines complémentaires. La liste des peines complémentaires applicables aux personnes physiques portant atteinte à la vie privée humaine peut être analysée dans l'article 226-31 du Code pénal, qui prévoit ce qui suit : « l'interdiction des droits civiques, civils et familiaux, tels que prévus à l'article 131-26 ; (…) l'interdiction d'exercer une activité professionnelle ou sociale dans le cadre ou à l'occasion de laquelle l'infraction a été commise, ou conformément à l'article 131-27; (…) l'interdiction, pour une période n'excédant pas cinq ans, de détenir ou de porter une arme soumise à autorisation; (…) l'affichage ou la diffusion de la décision rendue, dans les conditions prévues à l'article 131-35; (…) la confiscation de l'objet qui a servi ou était destiné à commettre l'infraction ou de celui qui représente son produit ». La jurisprudence considère qu'il est justifié de prendre la mesure de confiscation des objets utilisés pour commettre l'acte, les juges appréciant ainsi, après avoir trouvé dans l'ordinateur et sur la clé USB de l'auteur de l'acte pénal, les objets utilisés pour le commettre[1592].

[1591] Les peines étaient majorées par la *Loi no. 2018-703 du 3 août 2018*.
[1592] Consulter la jurisprudence pénale du 25 juillet 2018, par la Décision *no. 17-84.032*.

En particulier, la sanction de confiscation est facultative pour les infractions visées aux articles 226-1 à 226-2-1 du Code pénal, mais obligatoire pour les infractions commises au titre de l'article 226-3.

570. Le cas des personnes morales. En ce qui concerne les personnes morales, les sanctions complémentaires prévues à l'article 226-7, alinéas 2 et 3 du Code pénal consistent à interdire, de façon définitive ou pour une durée maximale de cinq ans, l'exercice direct ou indirect d'une activité professionnelle ou sociale dans le cadre ou à l'occasion de laquelle l'infraction a été commise et la présentation ou la diffusion de la décision rendue, conformément aux conditions prévues à l'article 131-35[1593].

C. Criminalisation de la tentative

571. Réglementation pénale de la tentative. Contrairement au droit roumain, en cas d'atteinte à la vie privée d'une personne, le droit français sanctionne expressément la tentative dans le cas des faits par lesquels les droits privés sont violés. Concrètement, le législateur précise que toute conduite illégale doit être sanctionnée ou suspendue pour des raisons indépendantes de la volonté de l'auteur. Bien qu'une exécution interrompue, caractérisée par le caractère défectueux du résultat concret produit, ne constitue pas matériellement une violation effective de la vie privée, cependant, le législateur considère que le début de l'exécution de l'acte est suffisant pour la reconnaissance du comportement infractionnel chez la personne qui

[1593] L'article 131-35, la version en vigueur du 19 mai 2011, modifiée par la *Loi no. 2011-525 du 17 mai 2011 – art. 148*, dispose que :
„*La peine pour l'affichage ou la diffusion du jugement est à la charge de la personne condamnée. Toutefois, les frais d'affichage ou de distribution recouvrés sur ce dernier ne peuvent excéder le montant maximal de l'amende encourue. Le tribunal peut ordonner l'affichage ou la diffusion intégrale ou partielle du jugement ou d'un communiqué de presse informant le public des motifs et du dispositif. Il détermine, le cas échéant, les extraits du jugement et les termes du communiqué de presse à afficher ou diffuser.*
L'affichage ou la diffusion du jugement ou du communiqué de presse ne peut comporter que l'identité de la victime avec son consentement ou celle du représentant légal ou de leurs bénéficiaires.
La sentence d'affichage est exécutée dans les lieux et pour la durée indiqués par le tribunal; sauf disposition contraire prévue par la loi punissant la commission, l'affichage ne peut excéder deux mois. En cas d'enlèvement, de dissimulation ou de rupture des affiches affichées, les affiches seront à nouveau exposées aux frais de la personne reconnue coupable de ces faits.
Le jugement est diffusé par le Journal officiel de la République française, par l'une ou plusieurs publications de presse ou l'un ou plusieurs services publics de communications électroniques. Les publications ou services de communications électroniques chargés d'une telle diffusion sont désignés par le tribunal. Ils ne peuvent pas s'opposer à cette diffusion. L'affichage et la diffusion peuvent être commandés cumulativement ".

l'initie, en tant que tel, celui-ci devant être éradiqué[1594]. L'article 226-5 du Code pénal stipule que la tentative est punissable, ainsi que l'infraction elle-même[1595].

572. La simple intention est punie, même si l'enregistrement n'a pas abouti. Ainsi, en ce qui concerne l'article 226-1, le Code pénal établit que l'installation de tout appareil visant à permettre la capture illicite de mots prononcés par une personne revête la valeur d'une intention de mauvaise foi dans la représentation psychique de son auteur. Si l'intention reste au stade de l'achat des appareils nécessaires à la capture, alors nous sommes en présence d'un acte préparatoire non puni. De plus, le maintien du comportement infractionnel de l'auteur n'est pas conditionné par l'incapacité technique de l'appareil utilisé pour la capture, par conséquent, l'infraction est considérée comme consommée indépendamment du manque de performance technique de l'appareil[1596].

573. Caractère typique de la tentative : existence d'un dispositif d'enregistrement caché. Ainsi, la jurisprudence établit que le fait de dissimuler un magnétophone techniquement utilisable dans un bureau commun utilisé avec une autre personne pourrait constituer une tentative d'atteinte à la vie privée, même si aucun mot n'a été capturé ou transcrit en relation avec la vie privée de cette personne[1597]. Dans le même sens, lorsque les mots enregistrés sont imperceptibles, y compris dans cette hypothèse nous sommes sur le territoire de la tentative ; sur l'argument que, bien qu'interrompue par des causes externes, respectivement sur le fond d'imperfections techniques, l'exécution a été déclenchée par son auteur sur la base d'une résolution infractionnelle intentionnelle[1598].

La tentative peut également être prise en compte dans le cadre de l'acte préparatoire consistant à photographier ou filmer une personne révélant des parties intimes de son corps dans le vestiaire d'un lieu public, tel qu'une piscine municipale, lorsque l'enregistrement de l'image ou de la vidéo a été interrompu exclusivement par la réaction du propriétaire de droit

---

[1594] Cour de cassation, Chambre criminelle, *19 mai 1981, 80-94634*. https://juricaf.org/arret/FRANCE-COURDECASSATION-19810519-8094634

[1595] Cour de cassation - Chambre criminelle *31 octobre 2017 / n° 16-87.411.* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_2017-10 31_1687411&FromId=HCDROITPRESSE_DOC_51#texte-integral

[1596] Voir la note de Mayer en *Crim. 19 mai 1981, D. 1981. 544*, concernant l'installation d'un dispositif permettant à capturer d'une façon illégale les mots qui représentent un début d'exécution punissable, tandis que l'acquisition de l'équipement n'est qu'un acte préparatoire.

[1597] À cet égard, voir la jurisprudence Crim. *15 février 2011, no. 10-82.808,* par laquelle il a été décidé que le fait de cacher dans une rampe d'éclairage un dictaphone en activité dans le bureau d'accueil du cabinet médical que l'auteur avait loué avec un collègue chirurgien-dentiste, pourrait caractériser une tentative d'atteinte à la vie privée même si dans ce cas aucun mot concernant sa vie privée n'a été capturé ou transcrit.

[1598] Voir la jurisprudence de l'époque en *Crim. 19 mai 1981, Bull. crim. nr. 161*; et Dalloz 1981. p. 544, par la note de Mayer ; ainsi que RSC 1982. paragraphe125, par les observations de Levasseur.

privé, considérant que la vie privée de cette personne[1599] a été atteinte. Cette façon de commettre[1600] est susceptible d'être sanctionnée[1601] notamment par le délit de capturer une image indécente[1602], par la violence volontaire ou par l'agression sexuelle.

§4. JURISPRUDENCE SUR LA PROTECTION DE LA VIE PRIVÉE EN FRANCE

574. Transformations législatives dictées par la numérisation. Au cours de la dernière décennie, le paysage juridique français a connu des transformations importantes dans le domaine de la protection de la vie privée[1603]. L'interprétation des articles 226 et suivants du Code pénal français s'est continuellement adaptée aux enjeux de la numérisation et du développement des systèmes basés sur l'intelligence artificielle.

Les juridictions françaises ont adopté une vision globale de la sphère de protection de la vie privée, reconnaissant l'environnement numérique comme un prolongement naturel de l'espace personnel. Par conséquent, toute utilisation non autorisée de renseignements personnels dans le domaine numérique peut constituer une violation du droit à la vie privée[1604]. En ce qui concerne la surveillance électronique non autorisée, y compris l'utilisation illégale de systèmes de vidéosurveillance ou de logiciels de surveillance, ils ont été sanctionnés conformément aux dispositions des articles 226-1 et 226-2 du Code pénal. La jurisprudence a constamment souligné la nécessité d'obtenir un accord explicite pour de telles activités. Dans le cadre de la mise en œuvre du RGPD, les tribunaux français ont résolu de nombreuses affaires concernant des traitements non conformes de données à caractère personnel, imposant des sanctions pour leur collecte et utilisation non autorisées.

[1599] À cette fin, la jurisprudence dans l'affaire Crim. *31 oct. 2017, no 16-87.41*, qui montre qu'une personne qui se révèle dans le vestiaire d'une piscine municipale entraîne la retenue du caractère de tentative au délit d'atteinte à la vie privée en touchant la vie privée de la personne.

[1600] Voir le point de vue de V. Tellier – Cayrol, concernant la « *Loi du 3 août 2018 sur le renforcement de la lutte contre les violences sexuelles ou sexistes* », AJ pénal, 2018. p.400

[1601] Cette conduite est susceptible d'être poursuivie sur la base d'un nouveau délit de prise d'images indécentes défini par l'article 226-3-1 du Code pénal. Par l'article 16 de la loi no 2018-703 du 3 août 2018, une nouvelle infraction a été introduite dans le Code pénal français, criminalisant les faits de personnes filmant, photographiant ou même regardant sous les jupes des femmes à l'aide d'un miroir, en particulier dans les centres commerciaux. Pour une jurisprudence per a contrario, voir la décision de Montpellier du 28 février 2008 dans RG no. 07/01002, qui relate que dans une affaire semblable, la Cour d'appel de Montpellier a prononcé l'acquittement au motif que « *bien que les faits soient contraires à la morale et démontrent un véritable manque de dignité* », la loi ne punit pas « *la simple violation de la délicatesse d'une personne* ».

[1602] L'article 226-3-1 du Code pénal français criminalise actuellement « *le fait d'utiliser tout moyen pour observer les parties intimes d'une personne que celle-ci, par ses vêtements ou par sa présence dans un lieu fermé, les a dissimulées à la vue de tiers, lorsqu'il a été commis sans le consentement ou le consentement de la personne*. »

[1603] J.-C. Saint-Pau, *Droit au respect de la vie privée et droit pénal*, Dr. penal, 2011.

[1604] A. Rallet, F. Rochelandet, *Protéger la vie privée à l'ère numérique*. Réseaux: communication, technologie, société, n°189, p.9, 2015. shs.cairn.info/revue-reseaux-2015-1?lang=fr

575. Équilibre entre sécurité publique et droits fondamentaux. La mise en œuvre de technologies d'identification faciale basées sur l'intelligence artificielle a suscité des débats complexes dans le domaine de la protection de la vie privée. Les tribunaux ont cherché à trouver un équilibre optimal entre les impératifs de la sécurité publique et les droits fondamentaux de la personne, en fixant des limites claires sur l'utilisation de ces technologies en l'absence d'un consentement explicite[1605]. Selon les données fournies par le Ministère de la Justice de France, les atteintes à la vie privée dans l'environnement numérique ont augmenté de 35% au cours des cinq dernières années. Cette tendance à la hausse est attribuée à la prolifération des appareils connectés et des plateformes en ligne, qui ont amplifié la vulnérabilité aux attaques cybernétique et aux attentes à la vie privée[1606].

Dans un contexte marqué par l'évolution accélérée des technologies de surveillance, 2023 a été un moment déterminant pour la jurisprudence française. Les décisions prises au cours de cette période ont redéfini les paramètres de la protection de la vie privée à l'ère numérique, reflétant le souci des tribunaux de maintenir un juste équilibre entre l'innovation et les droits fondamentaux.

576. Arrêt de la Cour de cassation no. 19-24.780 du 17 février 2021[1607]. Devant la Cour de cassation une affaire est pendante traitant d'une question d'intérêt général, à savoir l'équilibre entre le respect de la vie privée et la liberté d'expression. La convention pour la défense des droits de l'homme et des libertés fondamentales régit le respect de la vie privée à l'article 8 et la liberté d'expression à l'article 10[1608]. D'un point de vue civil, la vie privée est protégée par l'article 9 du Code civil. Les deux droits fondamentaux ont la même valeur normative et sont extrêmement importants dans une société démocratique, le juge d'un tel cas ayant un rôle proactif dans le maintien de l'équilibre entre les 2[1609].

L'affaire en cause concerne le recours formé par Monsieur MK contre une décision de la Cour d'appel de Paris du 25 septembre 2019, qui a rejeté ses prétentions à l'encontre de l'auteur d'un site Internet se référant à ses condamnations pénales antérieures, violant ainsi sa confidentialité (partie de sa vie privée).

[1605] *Les infractions liées au numérique enregistrées par les services de sécurité en 2024,* Ministè de l'Intérieur, 2025. https://www.interieur.gouv.fr/actualites/communiques-de-presse/infractions-liees-au-numerique-enregistrees-par-services-de-securite-en-2024

[1606] A/*HRC/51/17 : The right to privacy in the digital age*, United Nations Humans Rights, 2022. https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age

[1607] Cour de cassation, civile, Chambre civile 1, *17 février 2021, 19-24.780*, publié au bulletin https://www.legifrance.gouv.fr/juri/id/JURITEXT000043200262

[1608] *Convention de la CEDH*, 2024. https://www.echr.coe.int/documents/d/echr/convention_ron

[1609] C. Caron, *Le caractère anodin de l'information chasse la vie privée,* Dalloz, 2004. p.1633 https://www dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=RECUEIL/OBS/2004/0420

577. L'analyse juridique, aspects essentiels. Le cadre juridique invoqué vise à délimiter le droit au respect de la vie privée et à établir si des informations, apparemment anodines, par leur cumul ou dans un certain contexte peuvent atteindre la vie privée d'une personne. La Cour souligne que ce droit fondamental doit être mis en balance avec la liberté d'expression[1610]. L'invocation du caractère banal de l'information pour supprimer l'idée d'atteinte à la vie privée a été utilisée dans d'autres situations[1611], et en l'espèce les tribunaux inférieurs ont considéré que la divulgation de données mineures, déjà partiellement accessibles au public, ne constitue pas une atteinte à la vie privée[1612].

La Cour de cassation constate que la simple publicité préalable de certaines informations ne les exclut pas automatiquement de la protection de la vie privée. *Per a contrario*, leur utilisation doit répondre aux attentes raisonnables de la personne concernée et servir un intérêt public légitime. *Ratio decidendi* de la Cour relève que le tribunal d'appel a omis d'examiner si la publication de ces informations s'inscrivait dans un débat d'intérêt général qui aurait pu justifier la reproduction de condamnations pénales. *A fortiori*, la présence d'informations dans le domaine public ne dispense pas de l'obligation de respect de la vie privée lorsqu'elles sont republiées dans un contexte différent[1613].

Par conséquent, la Cour de cassation rejette l'arrêt attaqué pour absence de fondement juridique, car le tribunal inférieur n'avait pas réalisé l'équilibre nécessaire entre les droits fondamentaux en conflit, selon les critères jurisprudentiels établis par la CEDH.[1614]

Dans des cas similaires, la CEDH rappelle que, dans l'analyse d'un tel cas, la Cour tient compte d'un certain nombre de critères tels que l'objet de l'affaire et sa contribution au débat public, la notoriété de la personne concernée, son comportement antérieur, l'impact de la publication sur la vie privée[1615].

[1610] Fasc. 1010: *Personnes - Famille. – Personnalité juridique*, JurisClasseur Roulois, Lexis360 Intelligence, 2022. par.47. https://www-lexis360intelligence-fr.docelec.u-bordeaux.fr/encyclopedies/JurisClasseur_Roulois/.

[1611] C. Bigot, *Protection de la vie privée: la Cour de cassation pose de nouvelles règles*, Recueil Dalloz, 2002. p.3164. https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=RECUEIL/JURIS/2002/2266

[1612] Cour d'appel de Paris, *25 septembre 2019, 18/04688.*

[1613] Cour de cassation, civile, Chambre civile 1, *17 février 2021, 19-24.780*. https://www.legifrance.gouv.fr/juri/id/JURITEXT000043200262

[1614] Cour de cassation, 1re chambre civile, *17 Février 2021 – n° 19-24.780* https://www-lexis360intelligence fr.docelec.u-bordeaux.fr/document/JP_KODCASS-0010329_1_0KRH?source_nav=EN_KEJC 215406_0QRG&source=related.

[1615] Case of *M.L. et W.W. c. Germany*, applications *nos. 60798/10 and 65599/10.* https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-183947%22]} en l'espèce, les requérants, deux citoyens allemands reconnus coupables de la crime, ont demandé par la suite l'exécution de la peine, la suppression ou l'anonymisation du contenu des articles de presse qui leur étaient adressés, au motif que cela touche à leur vie privée, en entravant la réinsertion sociale et la stigmatisation. Toutefois, les autorités judiciaires nationales ont considéré que le sujet était d'intérêt public et la liberté de l'information a priorité en l'espèce. La CEDH, en analysant l'équilibre entre le droit à la vie privée et le droit à l'expression et à l'information, décide de la même chose.

578. Arrêt no. 2210578 du Tribunal administratif de Nantes du 19 août 2022[1616]. Devant le tribunal administratif est présentée une affaire qui met en balance le droit fondamental à la vie privée et l'intérêt public de l'accès au patrimoine culturel, dans une affaire qui soulève des questions juridiques complexes concernant les mesures provisoires en droit administratif[1617].

Sur le plan procédural, le litige concerne la demande de Monsieur B., propriétaire d'une maison adjacente aux remparts médiévaux de la ville de Guérande, visant à obtenir des mesures provisoires contre la municipalité pour la protection de la vie privée et de la sécurité, dans le cadre de l'ouverture au public de la route médiévale protégeant sa propriété.

L'argumentation de la Cour est basée sur l'article L.521-3 du Code de justice administrative français, qui permet au juge d'ordonner des mesures provisoires en cas d'urgence, à condition qu'elles soient utiles et ne fassent pas l'objet de contestation sérieuse[1618].

Le tribunal examine l'accomplissement de la condition d'urgence à la lumière du préjudice allégué par le demandeur - le dommage à la vie privée causé par la visibilité directe de sa propriété sur la route médiévale, ouverte au public pour les visites pendant la période estivale. Au contraire, le juge estime que, en l'absence de preuve concrète de l'occupation réelle de la propriété et de photographies démontrant une vue directe sur la terrasse ou la maison, la condition d'urgence n'est pas remplie. Par conséquent, le tribunal rejette la demande du requérant, considérant que les conditions pour ordonner les mesures provisoires demandées ne sont pas remplies, laissant ainsi prévaloir l'intérêt public d'accès au patrimoine culturel médiéval de la ville[1619].

579. Jurisprudence pénale. Si la jurisprudence civile inclut dans le concept de vie privée des aspects intimes et secrets liés à la famille, la vie sentimentale[1620], l'image personnelle, l'état

---

[1616]Tribunal administratif de Nantes *19 août 2022, n° 2210578* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=TA_NANTES_2022-08-19_2210578

[1617] *Ordonnance n° 2020-324 du 25 mars 2020 portant mesures d'urgence en matière de revenus de remplacement mentionnés à l'article L. 5421 2 du code du travail.* https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042012905/

[1618] *Code de justice administrative*, *Article L521-3* https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006449328 permet une décision rapide, mais temporaire, utilisée d'habitude contre une mesure administrative violant un droit fondamental : la protection de la vie privée, la liberté d'expression, la libre circulation.

[1619] Tribunal administratif, Nantes, *19 Août 2022, n° 2210578,* https://www-lexis360intelligence-fr.docelec.u bordeaux.fr/

[1620] Le Collectif Onze, *Chapitre 2. Ce que la justice fait à la vie privée. Au tribunal des couples : Enquête sur des affaires familiales*, Odile Jacob, 2013, p. 67-121. https://droit.cairn.info/au-tribunal-des-couples--9782738130532-page-67?lang=fr.

de santé[1621], la protection offerte par la jurisprudence pénale semble se limiter aux seules atteintes à la vie privée, selon les articles 226-1 et suivants du Code pénal[1622].

Une situation qui a suscité des controverses et conduit la Cour de cassation à proposer des avis contradictoires, mais qui a aussi contribué de manière significative à l'évolution de l'interprétation du concept de vie privée en France, est le besoin (ou non) de l'atteinte réelle à la vie privée pour déterminer le délit d'atteinte à la vie privée par espionnage auditif ou visuel, tel que stipulé à l'article 226-1 du Code pénal[1623].

580. Équilibre entre intention et conséquences. Dans l'arrêt de la Cour de cassation no. 19742 du 27 janvier 1981[1624], l'accent est mis sur l'équilibre entre l'intention de l'auteur et les conséquences de son action. Puis, dans l'arrêt no. 80-94634 du 19 mai 1981, la Cour de cassation détermine que l'infraction d'espionnage auditif est constituée indépendamment de la qualité ou de l'audibilité de l'enregistrement[1625]. Par la suite, dans l'arrêt no 80-95226 du 3 mars 1982, cette position a été rejetée, soulignant que l'élément matériel de l'infraction constitue une atteinte à la vie privée »[1626].

581. Arrêt de la Cour de cassation no. 16-87.411 du 31 octobre 2017[1627]. Dans ce cas, la Cour examine la situation juridique d'une personne qui a tenté l'enregistrement d'une personne dans un espace privé (vestiaire), sans son consentement, un délit régi par l'article 226-1 du Code pénal. L'action est demeurée au stade de tentative parce qu'elle a été interrompue par la réaction de la victime. La tentative est incriminée en France à l'article 226-5 du Code pénal. La Cour confirme donc que l'acte constitue une atteinte à la vie privée, peu importe le résultat et l'intention de l'acte.

Il est à noter qu'actuellement cet acte pourrait constituer une nouvelle infraction, le fait de capturer des images de nature indécente, tell que défini à l'article 226-3-1 du Code pénal[1628].

[1621] Conseil d'Etat, Section, *du 5 décembre 1997, n° 112888*, Dalloz. 1998. IR32 https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=RECUEIL%2FIR%2F1998%2F0168&FromId=PEN_RUB000324_DOC_1

[1622] N. Cazé-Gaillarde, *Atteintes à la vie privée*, Dalloz, 2019 .(actualisation: 2023), pf. 21. https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ENCY/PEN/RUB000324/2020 02/PLAN/0005

[1623] J.-C. Saint-Pau, *Le délit d'atteinte à l'intimité de la vie privée exige-t-il une atteinte effective à l'intimité de la vie privée?* Dalloz, 1999. p.152 https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=RECUEIL/NOTE/1999/0054

[1624] Cour de cassation, Chambre criminelle, *27 janv.1981*, *no.19742*, 1982.

[1625] Cour de cassation, Chambre criminelle, *19 mai 1981, 80-94634* https://juricaf.org/arret/FRANCE COURDECASSATION-19810519-8094634

[1626] Cour de cassation, Chambre criminelle, *19 mai 1981, 80-94634* https://juricaf.org/arret/FRANCE COURDECASSATION-19810519-8094634 COURDECASSATION-19820303-8095226

[1627] Cour de cassation, Pourvoi n° *16-87.411.* https://www.courdecassation.fr/decision/5fcaa9e2a24730a0fdb69340

[1628] V. Tellier-Cayrol, *Loi du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes,* AJ pénal 2018. p.400 https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=AJPEN/CHRON/2018/0266

582. Arrêt de la Cour de cassation no. 08-85983 du 26 mai 2009[1629]. Dans cette affaire, il est souligné l'accomplissement des conditions typiques du délit d'atteinte à la vie privée, quel que soit le but de l'action. La prévenue est initialement accusée d'espionnage auditif en enregistrant des conversations de collègues, sans consentement (élément matériel), dans l'intention de recueillir des preuves sur le comportement de son supérieur (élément intentionnel)[1630].

L'article 122-7 du Code pénal français stipule que la personne qui, face au danger, commet un acte pour se protéger elle-même, un autrui ou un bien ne peut être pénalement responsable, tout en maintenant, bien sûr, une proportionnalité entre la gravité de la menace et les moyens de défense utilisés[1631]. Toutefois, la Cour de cassation rejette le recours fondé sur l'état de nécessité au titre de l'article précité, au motif qu'il n'a pas été porté devant la cour d'appel et ne peut donc être invoqué dans l'appel[1632].

583. Arrêt de la Cour de cassation no. 16-80820 du 20 septembre 2016[1633] Le présent jugement porte sur les circonstances justifiant les enregistrements clandestins et leur utilisation dans des enquêtes criminelles. En résumé, une personne privée, représentant de la victime enregistre sans consentement les conversations privées des personnes soupçonnées de tentative de chantage et d'extorsion, les autorités publiques étant informées à ce sujet. Par la suite, les enregistrements ont été utilisés dans le cadre de l'enquête.

La Cour de cassation rappelle que le principe de loyauté s'applique en l'espèce et rejette la suppression des enregistrements obtenus illégalement[1634]. Cette décision a suscité des controverses dans la doctrine parce qu'elle viole les principes d'un procès équitable tels que définis à l'article 6 de la CEDH. D'autre part, la CEDH ne réglemente pas clairement la recevabilité de la preuve, laissant cette dernière à la disposition du droit national. Selon l'article 427 du Code de procédure pénale[1635], les infractions peuvent être prouvées à travers des preuves obtenues par n'importe quelle méthode et le juge décide de leur légalité et de leur administration loyale.

[1629] Cour de cassation, Chambre criminelle, *26 mai 2009, 08-85983* https://juricaf.org/arret/FRANCE COURDECASSATION-20090526-0885983

[1630] Cour d'appel de Chambéry, *22 mai 2008, 07/02077* https://juricaf.org/arret/FRANCE COURDAPPELDECHAMBERY-20080522-0702077

[1631] *Code pénal Article 122-7* https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006417220?init=true&page=1&query=1227&searchField=ALL&tab_selection=all

[1632] Cour de cassation - Chambre criminelle *26 mai 2009, n° 08-85.983* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_2009-05-26_0885983

[1633] Cour de cassation, Chambre criminelle, *20 septembre 2016*, *n° 16-80.820.* https://www.courdecassation.fr/decision/5fd92162db2ccbbeab0f1d02

[1634] Cour de cassation - Chambre criminelle *20 septembre 2016, n° 16-80.820.* https://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document?id=CASS_LIEUVIDE_2016-09-20_1680820

[1635] *Code de procédure pénale*. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037108959/2016-06-01 Article 427

Section 2. CADRE JURIDIQUE D'INCRIMINATION DE L'ATTEINTE À LA VIE PRIVÉE EN DROIT PÉNAL ROUMAIN

584. Débat sur le délit d'atteinte à la vie privée. Le délit d`atteinte à la vie privée est réglementé par l'art. 226 du Code pénal et il est un délit légèrement atypique, car il présente plusieurs contenus alternatifs, c'est-à-dire qu'il inclut sous le même nom marginal plusieurs délits. Plus précisément, le législateur a, à mon avis, réglementé quatre délits distincts, à l`alinéa ($1^{er}$), à l`alinéa (2), à l`alinéa ($2^1$) et à l`alinéa (5), que nous présenterons lorsque nous examinerons l'aspect objectif de ce délit. Il est donc possible de retenir les quatre délits en concours, bien qu'elles soient couvertes par le même article et sous le même titre marginal.

Aussi, aux alinéas (4) et (4^1) sont présentées les causes atypiques du délit, et alinéa (3) précise la question du déclenchement de l'action pénale.

§1. DÉLIT D'ATTEINTE À LA VIE PRIVÉE DANS LE CODE PÉNAL ROUMAIN

A. Éléments de typicité de l'infraction d'atteinte à la vie privée

Objet juridique

585. La délimitation pénale de la notion de vie privée. Bien que l'art. 226 du Code pénal réglemente plusieurs délits, ils sont similaires en ce qu'ils protègent les relations sociales concernant la vie privée de la personne physique, mais seuls certains aspects de la vie privée sont protégés, à savoir le droit au respect de son image, le droit à la vie privée, ainsi que le droit au respect de la vie privée en matière sexuelle.

On voit que le Code pénal actuel ne définit pas la vie privée et, comme l'a également souligné la Cour européenne des droits de l'homme[1636], il n'est pas possible ou nécessaire de définir la vie privée de façon exhaustive. Il serait plutôt trop restrictif de limiter la vie privée à un « cercle » intime dans lequel la personne peut mener sa vie personnelle comme elle l'entend et exclure le monde extérieur. Le respect de la vie privée devrait également inclure, dans une certaine mesure, le droit d'établir et de développer des relations avec d'autres personnes.

[1636] La Cour européenne des droits de l`homme, Décision du 16 décembre 1992 dans l`affaire *Niemietz c. Allemagne,* pf. 29, document consulté à https://hudoc.echr.coe.int/eng?i=001-57887.

Objet matériel

586. Étant donné que l'objet juridique de l`atteinte à la vie privée n'a pas d'existence matérielle, c'est-à-dire le caractère privé de la vie privée, il s'ensuit que ce délit n'a aucun objet matériel[1637].

Sujets du délit

587. Définition de l'auteur de l'infraction. Le sujet actif n'est pas circonstancié dans tous les contenus constitutifs de l`atteinte à la vie privée, l'acte pouvant être commis par toute personne physique ou morale.

La participation pénale est possible sous toutes ses formes pour les quatre faits distincts suivants : co-auteur, instigateur et complice.

588. Définition de la victime. Le sujet passif des infractions prévues à l'art. 226 du Code pénal ne peut être que la personne physique (vivante), et non pas celle morale, ce qui résulte des règles mêmes de criminalisation[1638]. La responsabilité pénale ne sera pas engagée si les faits concernent une personne décédée, auquel cas la responsabilité civile délictuelle pourrait être encourue pour ne pas avoir accordé le respect dû aux personnes décédées selon l'art. 78-79 du Code civil[1639]. Une personne morale ne peut être un sujet passif, étant une construction abstraite qui n'a pas de vie privée au sens de l'art. 226 du Code pénal. Hypothétiquement, si le contrevenant devait écouter par des moyens techniques une discussion entre deux associés d'une entreprise, la classification juridique dépend de l'information soumise par les deux associés : si la discussion concernait un secret d'entreprise, nous parlerions de la divulgation du secret professionnel, qui peut constituer une concurrence déloyale[1640]. Si la discussion concernait la vie privée des associés, alors les dispositions de l'art. 226 du Code pénal s`appliqueront.

[1637] En même sens, V. Cioclei*, op. cit*., p.239; M. Udroiu, vol.I *op. cit*., p.397. Au contraire, Al. Boroi, *op.cit*., p. 205.

[1638] Ainsi, à l`alinéa (1er), il s'agit de l`atteinte à la vie privée « *d'une personne* », située dans un logement, une pièce ou une dépendance (donc sans référence aux sièges), en obtenant des renseignements - conversations, photos, etc. L`alinéa (2) fait référence, en substance, à la publication de renseignements relatifs à la personne physique, obtenus conformément à l`alinéa (1er) et l`alinéa (2l) fait référence à la publication d'une image intime « *d'une personne* », qui ne peut être que physique, ainsi qu'il ressort également de la définition donnée à l'image intime selon l`alinéa (22). Enfin, l`alinéa (5) traite de l'utilisation de moyens techniques d'enregistrement pour commettre un des actes visés à l`alinéa (1er) ou à l`alinéa (2), lorsque le sujet passif est, comme nous l'avons établi, la personne physique.

[1639] M. Udroiu, vol.I *op. cit*., p.398. Selon l'art. 78 Code civil sur le respect dû aux personnes décédées, « *on doit du respect pour sa mémoire, ainsi que pour son corps* ». En outre, l`art. 79 du code civil interdit de porter atteinte à la mémoire du défunt et stipule que « *la mémoire du défunt est protégée dans les mêmes conditions que l'image et la réputation du vivant* ».

[1640] Le fait est criminalisé par l`art. 5 lettre c) de la Loi no.11/1991 concernant la lutte contre la concurrence déloyale, publiée dans le Journal Officiel np. 24 du 30 janvier 1991.

589. Victimes multiples : infractions multiples. Il convient de noter que, en principe, la pluralité des victimes attirerait, au moins théoriquement, une pluralité de délits, quel que soit l'acte commis[1641] - celui des alinéas (1er), (2), (21) ou de l`alinéa (5), puisque ce sont tous des délits contre la personne. De toute évidence, une telle solution peut sembler profondément injuste pour l'auteur si, par exemple, il enregistre simultanément les conversations audio de 8 personnes, auquel cas nous aurions 8 délits distincts d`atteinte à la vie privée. Nous croyons qu'une solution possible, comme nous l'avons apprécié dans le cas de la violation du domicile, serait la retenue d'une unité naturelle collective, si l'exemple susmentionné est commis contre plus d'une personne, dans la même circonstance. En même temps, il est possible que l'auteur soit reconnu coupable de tous ces délits, commis contre le même sujet passif.

Côté objectif

590. Controverses concernant la doctrine pénale. En ce qui concerne l'aspect objectif, nous traiterons séparément l'élément matériel des quatre infractions visées par l'art. 226 du Code pénal, car certains d'entre eux ont des façons différentes de commission.

Toutefois, il faut préciser que dans la doctrine il y a une controverse sur le nombre d'infractions prévues à l'art. 226. D'une part, dans un avis[1642], il est démontré que l'art. 226 du Code pénal consiste en une seule infraction - art. 226 alinéa (1er), alinéa 2 étant une forme aggravée, et l`alinéa (5) une forme assimilée, sanctionnée plus sévèrement. Cet avis ne remet pas en cause l`art. (21), étant donné qu'il n'existait pas au moment de la publication de l'ouvrage cité. Un autre avis[1643] considère que l'art. 226 inclut la forme de base dans le par. (1) et deux formes aggravées aux par. (2) et (5). Dans un autre point de vue[1644], il est considéré que l'article 226 contient trois infractions distinctes : celle de l`alinéa (1er), de l`alinéa (2) et de l`alinéa (5). Aussi, dans un article plus récent du même auteur, qui inclut également des mentions concernant l`alinéa (21) de l'art. 226 du Code pénal[1645], on considère que la disposition susmentionnée n'est qu'une forme aggravée de l`art. (2). Enfin, dans un dernier avis[1646], il est estimé que, *de lege lata*, l'atteinte à la vie privée comprend quatre infractions autonomes prévues à l`article 226 alinéas (1), (2), (21) et (5). Nous considérons que cette dernière opinion

[1641] Sauf les cas où des mentions expresses seront faites à cet égard.
[1642] R. Slăvoiu, *op.cit*., p.108.
[1643] Al. Boroi, *op.cit*., p. 207; T. Toader, *Drept penal român. Partea specială*, vol. I, Ed. Universul Juridic, Bucarest, 2019. p.244 - 246.
[1644] M. Udroiu, vol.I op.cit., p.395.
[1645] M. Udroiu, *Résumé des modifications législatives opérées par les lois 171/2023, no. 213/2023, no. 217/2023 et no. 248/2023 dans le cas de délits contre la personne et contre le patrimoine* (ci-après dénommé M. Udroiu, Sinteza modificarilor), Annales de l'Université de Bucarest - série Droit, Forum juridique, no. 2, 2023 p.124
[1646] T. Manea, H.Ș. Tiugan, *Sancționarea exploatării sexuale prin imagini- dezideratul protecției penale si carențele incriminării*, Revue Universul Juridic nr. 6, 2023. p.73-82

est correcte, suivant à présenter les arguments de cette opinion lorsque nous analysons la loi de l'art. 226 alinéa (2^1).

591. L'infraction visée à l'article 226, alinéa (1er) du Code pénal Il s'agit d'une infraction à contenu alternatif, ayant plusieurs moyens équivalents de commettre (ce qui signifie que si l'auteur commet les deux modes, une seule violation d'une atteinte à la vie privée serait retenue). Ainsi, l'acte consiste en : 1. « l`atteinte à la vie privée, sans droit, par la photographie, la capture ou l'enregistrement d'images, l'écoute avec des moyens techniques ou l'enregistrement audio d'une personne dans un logement ou une pièce ou la dépendance y liée »; 2. « l`atteinte à la vie privée, sans droit, en écoutant avec des moyens techniques ou en enregistrant une conversation privée ». On peut dire, par référence aux autres délits incriminés à l'art. 226 du Code pénal, que l'acte visé à l`alinéa (1er) consiste essentiellement à obtenir et/ou à stocker des renseignements sur une personne ou une conversation privée.

a). Espionnage visuel

592. 1. Photographie et filmage : atteinte à la vie privée. La première façon de commettre ce délit se fait par plusieurs actions, que nous décrirons tour à tour. La photographie est le processus de fixation d'une image sur un support, qu'il soit analogique (par exemple, papier, pellicule ou film) ou numérique (sur un appareil électronique- portable). La capture d'image désigne l'obtention de représentations visuelles au moyen de moyens techniques (caméra web, drones, satellites). Ainsi, si la capture n'est pas effectuée par des moyens techniques, nous ne conserverons pas le délit (par exemple, nous n'avons pas de capture d'image si elle est faite « à l'œil nu », en espionnant la victime avec une jumelle). L'enregistrement d'image fait référence à l'action de capture d'images, sur laquelle est ajouté le stockage, la mémorisation des images capturées. L'écoute par des moyens techniques désigne l'obtention de sons par des moyens techniques, tels qu'un magnétophone, un microphone, etc., et l'enregistrement audio consiste à écouter avec des moyens techniques et à stocker les sons ainsi obtenus[1647]. Si l'auteur d'une

[1647] En ce qui concerne les deux dernières actions, une partie de la doctrine (V. Cioclei, *op.cit.,* p.239; S. Bogdan, D.A. Serban, *op. cit*., p.438) considère qu'elles font référence à des conversations privées, ne pouvant pas regarder une personne. Par conséquent, la photographie, la capture ou l'enregistrement d'images ne concernerait que la personne dans un logement, une pièce ou une dépendance, et l'écoute avec des moyens techniques et l'enregistrement audio seraient uniquement subsumés aux conversations privées. Nous ne croyons pas que ce point de vue soit correct, car la loi ne prévoit pas une telle séparation. De plus, nous croyons que la vie privée serait également atteinte lorsque nous avons une écoute technique ou un enregistrement audio d'une personne sans l`existence de la conversation. Par exemple, nous aurions l`atteinte à la vie privée dans ce cas où la victime serait écoutée pendant qu'elle parle seule tout en effectuant des activités domestiques. C'est pourquoi nous croyons que l'écoute et l'enregistrement audio peuvent également regarder la personne, pas seulement ses conversations. Dans le même sens, M. Udroiu, vol.I, *op.cit*., p.398-399.

infraction commet plusieurs des actions énumérées (par exemple, photographie et écoute avec des moyens techniques sur le même sujet passif), une seule infraction sera retenue.

593. Conditions pour commettre l'infraction. En ce qui concerne cette façon de commettre le délit, la loi nous impose deux conditions. La première est que l'acte d'exécution doit être effectué sans droit, c'est-à-dire sans autorisation légale. Ainsi, si l'auteur a la permission de la victime ou de la loi pour photographier, capturer, enregistrer des images, etc., le fait ne sera pas un délit.

La deuxième condition sur laquelle nous devons insister concerne le fait de commettre l'acte envers une personne *dans un logement ou une pièce* (qui peut être ou ne pas être possédée par la personne lésée) ou *la dépendance y liée*. Il convient de noter que, de cette façon, la photographie, la capture d'images, l'enregistrement d'images, l'écoute ou l'enregistrement audio doivent regarder une personne qui est en fait dans une maison, une pièce ou une dépendance y liée, et il ne suffit pas que l'élément matériel soit dirigé uniquement sur le bâtiment. Nous remarquons à cet égard une certaine proximité avec la violation du domicile, à la seule différence que l'art. 226 alinéa (1er) ne fait pas référence au lieu clôturé par rapport à un logement/pièce/dépendance[1648]. Par conséquent, selon la règle de criminalisation, si l`atteinte à la vie privée devait être effectuée dans un tel endroit clôturé - un jardin d'une maison, dans une dépendance qui n'appartient pas à un logement ou une pièce ou un lieu dans l'espace public (un parc, une rue, etc.), nous ne pourrions pas retenir l`atteinte à la vie privée de cette façon, mais peut-être une responsabilité délictuelle en vertu de l'art. 74 du Code civil.

594. La nécessité de définir la notion de domicile. En raison de la similitude susmentionnée entre l'atteinte à la vie privée et la violation du domicile, la question suivante a été soulevée : si les notions de logement, de pièce ou de dépendance de l'article 226 alinéa (1er) ont-elles un sens plus large que les mêmes termes de l'article 224, y compris les lieux qui ne peuvent être qualifiés de domicile (par exemple, le groupe sanitaire d'une clinique, où plus de personnes ont accès, le vestiaire d'une salle de sport, une cabine d'essai dans un magasin), ou elles revêtent la même signification. C'est précisément cette question qui a été résolue par l'ICCJ, qui a rendu une décision à cet égard[1649].

595. Critiques adressées à la doctrine. Avant de procéder à l'analyse de ladite décision, il faut préciser que dans la doctrine ont été formulées des critiques concernant la limitation

[1648] Dans un avis (V. Cioclei, *op.cit*., p.239), il a été considéré que l'article 226 alinéa (1er) inclut également le lieu clôturé. Formellement, nous ne partageons pas ce point de vue, car si la loi voulait mentionner le lieu clôturé, elle l'aurait fait expressément. Cependant, nous ne pouvons pas ne pas admettre que l'option du législateur est au moins à critiquer, puisque la vie privée d'une personne (par l`enregistrement audio, vidéo, photographie, etc.) peut également être atteinte lorsqu'elle se trouve dans la cour de la maison, et non seulement à l'intérieur de la maison.
[1649] *Décision no. 18 du 22 avril 2024*, parue dans le Journal Officiel, 1ère partie no.446, 15 mai 2024.

imposée par l'article 226 alinéa (1er) du Code pénal. Ainsi, dans un avis[1650], il a été considéré que la restriction opérée par le législateur, en limitant la commission de l'acte à une personne se trouvant dans un logement, une pièce ou une dépendance, est injustifiée et qu'il aurait été plus utile d'utiliser une notion plus large, qui aurait inclus le caractère privé de l'espace dans lequel se trouve la victime. Un autre auteur[1651] considère que les notions de logement, de pièce ou de dépendance de l'art.226 ont une signification plus large que les mêmes notions de l`art. 224 du Code pénal, de sorte que ces espaces soient également inclus, bien qu'ils ne puissent être classés comme domicile, *« offrent une protection temporaire de la vie privée de la personne (par exemple, les toilettes d'un lieu public*). »

b). Haute Cour de cassation et de justice : difficultés à définir *le logement*

596. La préoccupation de la Haute Cour dans la définition pénale de la notion de logement/dépendance/pièce. Enfin, pour en revenir à la décision de la Haute Cour, la situation évoquée dans la présente affaire est la suivante : l`inculpé a installé deux appareils d'enregistrement audio-vidéo électroniques, cachés dans des désodorisants qu'il a placés, sans droit, dans les deux toilettes d'une clinique médicale, afin d'obtenir des images des personnes qui ont utilisé les deux toilettes. Le jour même où il a installé ces appareils d'enregistrement audio-vidéo, il a enregistré les images capturées tout au long de la journée, portant ainsi atteinte à la vie privée de trois personnes lésées. Nous notons que les actes de l`inculpé seraient conformes aux dispositions de l`article 226 alinéas (1er) et (5), commettant ainsi deux infractions distinctes. Cependant, la première juridiction a jugé que pour affirmer l'existence des faits commis, il est nécessaire que la photographie, la capture ou l'enregistrement d'images, l'écoute avec des moyens techniques ou l'enregistrement audio se faire contre une personne dans un logement ou une chambre ou dépendance y liée, donc un espace subsumé à la notion de domicile d'un point de vue pénal (à l'exception évidente du lieu clôturé). Ou, le premier tribunal a déclaré que les deux toilettes de la clinique médicale ne rentrent dans aucun des trois espaces prévus par l'art. 226 du Code pénal. Pour cette raison, le tribunal a prononcé l'acquittement, alléguant que l'acte de l'art. 226 alinéa (1er) sur laquelle l`inculpé était accusé n'est pas prévu par la loi pénale car les toilettes de la clinique ne représentent pas un domicile au sens pénal. L`inculpé a également été acquitté pour l'acte en vertu de l'article 226 alinéa (5), puisqu`ils ne sont pas réalisés les conditions de typicité pour le délit finalité – auquel cas ils ne

[1650] S. Bogdan, D.A. Șerban *Drept penal. Partea specială*, Universul Juridic, 2022. p.437.
[1651] M. Udroiu, vol.I, *op.cit*., p.400.

sont pas respectés ni les conditions de typicité de l`acte prévues par l`art. 226 alinéa (5) du Code pénal.

La décision même de la Haute Cour souligne la controverse concernant l'application de l'article 226 alinéa (1er), montrant le point de vue des tribunaux sur la question du droit soumis à l'absolution. Il y a deux lignes directrices majoritaires qui ont été adoptées par les tribunaux.

597. Interprétation stricte, sans élargissement de la notion d'espace privé. La première opinion soutient que les notions de logement, de pièce ou de dépendance de l'art. 226, alinéa (1er) revêtent le même sens par rapport aux notions homonymes de l'art. 224 alinéa (1er) du Code pénal. L'argument en discussion indique que le législateur a utilisé une terminologie claire, également utilisée pour la violation du domicile, de sorte qu'elles devraient avoir la même signification. Si nous devions interpréter différemment le sens de ces notions, cela élargirait la portée, sans exister une norme juridique à cet égard, et une telle interprétation violerait également le principe de légalité de l'incrimination et créerait une situation défavorable à l`inculpé.

598. Espace privé fonctionnel, pas formel. La deuxième orientation de certains tribunaux considère que les concepts de logement/pièce/dépendance dans le cadre de l'article 226 alinéa (1er) du Code pénal a une signification plus large que les mêmes notions dans l'article 224 alinéa (1er) du Code pénal, étant donné que le but de criminaliser l`atteinte à la vie privée est de protéger la vie privée d'une personne, peu importe où elle se trouve, dans la mesure où cet espace peut être délimité pour assurer à la personne un minimum d`intimité.

599. La nécessité d'une interprétation uniforme de la notion d'espace privé. En ce qui concerne l'analyse du problème juridique effectuée par la Haute Cour, elle souligne l'importance d'une interprétation uniforme des termes communs issus des règles sur la criminalisation de la violation du domicile et de l`atteinte à la vie privée, une condition imposée par l'article 37 de la loi 24/2000 sur les règles de technique législative pour l'élaboration des actes normatifs[1652], qui stipule que, dans le langage normatif, « *les mêmes notions ne sont exprimées que par les mêmes termes et si une notion ou un terme n'est pas consacré ou peut avoir des significations différentes, sa signification dans le contexte est établie par l'acte normatif qui les établit* ». Un argument avancé par la Haute Cour pour démontrer l'équivalence des termes « logement », « pièce » et « dépendance » utilisés pour la violation du domicile et l`atteinte à la vie privée est le lieu de criminalisation des deux délits. Ainsi, l`art. 224 et l`art.

[1652] *Loi 24/2000 sur les règles de technique législative pour l'élaboration des actes normatifs*, parue dans le Journal Officiel no. 260 du 21 avril 2010, avec les modifications et les compléments ultérieurs. https://legislatie.just.ro/Public/DetaliiDocument/21698

226 du Code pénal sont réglementés dans le même chapitre ; par conséquent, les termes utilisés ont la même signification que celle qui était tirée de l'ancien Code pénal.

En outre, montre la Haute Cour, selon l'article 48 alinéa (3) de la loi no. 24/2000, si un article utilise une expression ou un terme qui a dans le contexte de l'acte normatif une signification différente de celle habituelle, cette signification spécifique doit être définie dans un paragraphe ultérieur. « *Comme l'article 226 du Code pénal qui criminalise l`atteinte à la vie privée ne définit pas un sens spécifique pour les termes de pièce ou de dépendance de son contenu, il s'ensuit qu'ils ont le sens habituel dans le contexte de l'acte normatif, celui du domicile au sens pénal* ». Pour cette raison, souligne la Haute Cour, il est évident que les concepts de logement, de pièce ou de dépendance sont utilisés par le législateur dans le sens consacré dans la criminalisation de la violation du domicile. En outre, il montre le sens actuel des trois notions : par logement, nous entendons le lieu, la maison, la construction dans laquelle une personne vit ou peut vivre; par pièce, nous entendons chambre; par dépendance, nous faisons référence à une pièce accessoire (cuisine, salle de bains, etc.).

600. Extension de la notion de logement : à la discrétion du législateur. Dans le même temps, la Haute Cour souligne que l'interprétation extensive de la notion de pièce dans le contenu de l`atteinte à la vie privée, dans le sens que par la pièce il doit être compris tout espace qui peut être délimité afin d'assurer à la personne un degré minimal d`intimité (donc y compris les toilettes d'une clinique médicale) ne tiendrait pas compte du fait que ce sens n'est inscrit ni par le législateur, ni dans la signification ordinaire du terme. Pour que les actions prévues à l'article 226 alinéa (1er) du Code pénal, commises dans des espaces autres que le logement, la pièce ou la dépendance, puissent constituer une infraction, une telle décision appartient exclusivement au législateur, comme cela a été fait également par l'introduction de l`alinéa (2^{1}) dans le texte de l'art. 226.

En conclusion, la Haute Cour établit que les notions de logement, de pièce ou de dépendance du contenu du délit d'atteinte à la vie privée, prévues par l'article 226 alinéa 1er du Code pénal, ont la même signification que les notions de logement, de pièce ou de dépendance du contenu du délit de violation du domicile, prévues par l'art. 224 alinéa 1er du Code pénal, étant subsumées à la notion de domicile au sens du droit pénal ».

601. Une terminologie plus appropriée : les notions de logement, pièce, dépendance. À notre avis, l'absolution prononcée par la Haute Cour de cassation et de justice est, du moins en théorie, correcte compte tenu des dispositions expresses de la règle de criminalisation. Nous sommes également d'accord qu'une interprétation contraire de la disposition juridique (en étendant le sens donné au logement, à la pièce ou à la dépendance) signifierait de violer le principe de légalité de l'incrimination, ainsi que celui de la prévisibilité du droit pénal, en

arrivant à la situation où les mêmes termes auraient des définitions différentes, des significations différentes. En outre, par la solution opposée, nous arrivons à la situation où l'interprétation du droit pénal serait faite, par rapport au sujet actif, *in mala partem*, interprétation qui est, en principe, interdite. Cependant, nous ne pouvons nier l'iniquité qui est produite par les dispositions restrictives de l'article 226 alinéa (1er), qui protège la vie intime de la personne seulement dans un logement, une pièce ou des dépendances, à l'exclusion d'autres endroits où la vie privée de la personne pourrait être affectée. En effet, il y a aussi les dispositions de l'article 74 du code civil qui couvriraient les lacunes de l'article 226 alinéa (1er) concernant la protection de la vie privée dans des espaces autres que ceux prévus par la norme pénale. Nous croyons cependant que le législateur pénal avait la possibilité de protéger, efficacement et opportunément (étant donné l'objet juridique de l'art. 226 du Code pénal), la vie privée de la personne, en utilisant des syntagmes plus complets que les notions de logement, pièce et dépendance tirées des dispositions de l'article 224 alinéa (1er) du Code pénal.

c). Protection pénale de la vie privée dans les espaces publics

602. Protection pénale limitée au domicile ; en dehors de celui-ci – responsabilité civile. Il est également utile de remettre en cause la décision de la Cour constitutionnelle de Roumanie no. 33 du 19 janvier 2017[1653], qui a rejeté une exception d'inconstitutionnalité, dans laquelle l'auteur contestait la constitutionnalité de l'art. 226 alinéa (1er) du Code pénal, au motif qu'il n'assurerait pas le même niveau de protection de la vie privée dans le cas où l'atteinte à la vie intime est commise dans des espaces extérieurs au logement, à la pièce ou à la dépendance, plus particulièrement dans des espaces liés à un bien public, où les autorités ou institutions publiques mènent leur activité. Pour soutenir le rejet de l'exception, la Cour constitutionnelle a déclaré que par la disposition juridique contestée, « *l'État ne nie pas le droit de la personne à la vie intime, familiale et privée, mais offre une protection accrue aux actes antisociaux qui affectent ce droit, lorsqu'ils sont commis dans un logement, une pièce ou une dépendance, donc un domicile au sens pénal, dans les autres situations la partie lésée ayant ouvert la voie à une action civile en justice* ».

Concluant sur la présente question, à la lumière des décisions rendues par la Haute Cour de cassation et de justice moyennant la décision no. 18/2024, respectivement par la Cour constitutionnelle moyennant la décision no. 33/2017, il s'ensuit que cette modalité de

[1653] Cour constitutionnelle, décision n° 30/2017 relative à l'exception d'inconstitutionnalité des dispositions de l'article 374, paragraphe 7, du Code de procédure pénale, Journal Officiel, 1e partie, no.327, 5 mai 2017. https://euroavocatura.ro/monitorul_oficial_act.php?id=6541

l'infraction visée à l'article 226 alinéa (1er) du Code pénal est typique uniquement lorsque l'action est commise contre une personne dans un logement, une pièce ou une dépendance y liée (à l'exclusion d`un endroit clôturé et d'autres espaces extérieurs, y compris ceux trouvés dans les propriétés publiques de l'État), les trois espaces ayant la même signification qu'en cas de violation de domicile, c'est pourquoi nous ne les redéfinirons pas.

d). Espionnage auditif

603. Écoute et enregistrement : atteinte à la vie privée. La deuxième façon de commettre l'infraction prévue à l'article 226, alinéa (1er) du Code pénal fait référence à l`atteinte à la vie privée, sans droit, en écoutant par des moyens techniques ou l'enregistrement audio d'une conversation privée. Il est de l`essence de cette modalité que les actions de l'écoute ou l'enregistrement s`orientent vers une conversation privée. C'est précisément pour cette raison que nous ne rencontrons ainsi que deux des actions prévues dans la première manière de commettre le délit : l'écoute par des moyens techniques, respectivement l'enregistrement audio. Par les autres voies (photographie, capture d'image ou enregistrement d'image), on ne considérerait pas une conversation privée, mais des interlocuteurs, des personnes qui parlent.

604. Absence de consentement. Comme tous les autres délits d`atteinte à la vie privée, il est nécessaire que l'action typique soit effectuée sans droit. Un aspect très important de cette modalité se réfère au fait que le lieu où la conversation privée a lieu n'est plus important, un aspect essentiel à la première modalité de ce délit. Ainsi, la discussion privée ne doit pas seulement avoir lieu dans un logement/une pièce/une dépendance, mais elle peut aussi avoir lieu dans un lieu public, et l'acte constituera un délit si l'une des deux actions est exercée.

605. Nécessité d'utiliser des dispositifs techniques. Il est également nécessaire pour la rétention de l'infraction que l'écoute ou l'enregistrement soit effectué par des moyens techniques, faute de quoi la typicité objective de l'acte fait défaut. Par exemple, si l'auteur de l'infraction est proche des personnes qui parlent et écoutent ce qui se dit, l'acte n'est pas typique.

606. Le caractère privé de la conversation concernée. Dans le même temps, l'acte doit concerner une conversation privée directe, d`ambiance. Si l'écoute ou l'enregistrement est fait en relation avec une conversation faite par des moyens techniques (par exemple, un portable), l'acte constituera une infraction, mais pas l`atteinte à la vie privée prévue à l'article 226 alinéa (1er) du Code pénal, mais l'infraction de violation du secret de la correspondance, prévue par l'art. 302 alinéa (2) du Code pénal.

607. Victimes multiples : infraction unique. Il est nécessaire de faire une mention sur la pluralité des sujets passifs. Comme nous l'avons déjà mentionné, dans le cas d`atteinte à la vie privée et de délits contre la personne en général, la pluralité des victimes (accomplissement de l'acte contre plusieurs personnes en même temps) entraîne la rétention d'une pluralité de délit. Cependant, comme l'a montré la doctrine[1654], ce type de délit met l'accent sur une pluralité naturelle de sujets passifs, puisque dans une conversation deux ou plusieurs personnes sont nécessaires. Par conséquent, si l'on écoute ou enregistre une conversation privée, sans droit, de plusieurs personnes, nous retiendrons, à notre avis, un seul délit d'atteinte à la vie privée, prévu à l'article 226 alinéa (1er).

e). Divulgation de sons, de conversations et d'images

La présente infraction, contrairement à celle de l'art. 226 alinéa (1er) du Code pénal consistant à obtenir et/ou stocker des informations, des données, cette infraction se réfère à la publication, en faisant connaître au public de ces informations. Par conséquent, l'infraction visée à l'article 226 alinéa (2) porte sur l'utilisation du produit obtenu à la suite d'une activité réglementée par l`alinéa 1er.

608. Délimitation des termes « divulgation », « diffusion » et « transmission ». L'élément matériel de ce délit consiste en : la divulgation, la diffusion, la présentation ou la transmission, sans droit, des sons des conversations ou des images visées à l'article 226 alinéa (1er) du Code pénal, à une autre personne ou au public. La divulgation fait référence à l'affichage direct de sons, de conversations ou d'images à un tiers spécifique, tandis que la diffusion fait référence à la divulgation indirecte de cette information à un public indéterminé par quelque moyen que ce soit (presse écrite, télévision, sites en ligne, réseaux sociaux, etc.). La présentation renvoie à la communication de l'information directement à un public indéterminé, tandis que la transmission renvoie, en principe, à la soumission du support sur lequel les conversations ou images sont stockées ou d'un autre support sur lequel elles ont été rendues[1655]. Si l'auteur commet plusieurs actes envers la même victime, dans le même contexte, une seule infraction sera retenue.

Une condition essentielle pour le maintien de la typicité objective de l'infraction est la commission de l'élément matériel (divulgation, diffusion, présentation ou transmission) sans droit. Il est également nécessaire que la divulgation, la diffusion, la présentation ou la

[1654] S. Bogdan, D.A. Șerban, *op.cit*., p.438.
[1655] Dans le sens que la transmission se réfère à la communication de sons, conversations, images à une autre personne au moyen de la communication à distance, S. Bogdan, D.A. Serban, *op.cit.*, p.447.

transmission aient pour objet des données qui sont de nature privée. Si l'auteur commet l'élément matériel contre des informations qui étaient déjà publiques, l'acte ne constitue pas un délit.

609. Collecte personnelle et divulgation ultérieure. Comme nous l'avons précisé, pour pouvoir commettre une telle atteinte à la vie privée, il est nécessaire de commettre l'acte prévu à l'article 226 alinéa (1er) du Code pénal[1656]. Bien qu'à première vue il semblât que la norme d'incrimination de l'article 226 alinéa (2) nous impose que les sons, les conversations ou les images obtenus proviennent d'une conduite illicite, typique de l'art. 226 alinéa (1er) du Code pénal, une telle condition n'existe pas en réalité. En se référant à l`alinéa (1er) dans le texte de l'article 226 alinéa (2), le législateur n`a souhaité que mettre en évidence l'origine de ces données intimes.

f). Controverse : est-il important que les images soient obtenues avec ou sans droit ?

610. Importance de l'accord dans la détermination de l'infraction. Cette question a également été traitée par la Haute Cour de cassation et de justice dans une décision antérieure[1657]. Le problème qui a été soumis à la Haute Cour était le suivant : « *si la typicité du délit d`atteinte à la vie privée dans la manière incriminée par l'art. 226 alinéa (2) du Code pénal est conditionnée par la possession de sons, de conversations ou d'images faites sans droit, en photographiant, capturant ou enregistrant des images, ou en écoutant par des moyens techniques ou en enregistrant l'audio d`une personne dans une maison ou une pièce ou une dépendance ou d'une conversation privée.* » En d'autres termes, la question en cause vise à clarifier si les dispositions de l'article 226 alinéa (2) du Code pénal sanctionne la divulgation, la diffusion, la présentation ou la transmission, sans droit, de sons, d'images ou de conversations, peu importe comment ces derniers ont été obtenus ou seulement quand ils ont été obtenus sans droit.

Dans son arrêt, la Haute Cour a déclaré que le législateur, par l'art. 226 alinéa (1er), protège « l'atteinte portée, sans droit, à la vie privée par des moyens alternatifs prévus par la loi, alors que la protection offerte par le législateur par l'article 226 alinéa (2) du Code pénal porte, entre autres, sur les modalités de divulgation ou de diffusion, sans droit à une certaine personne ou à un nombre indéterminé de personnes de sons, conversations ou images obtenues

[1656] Il est possible que la personne qui fait connaître les renseignements intimes au public soit aussi celle qui les a obtenus (dans ce cas, elle sera responsable de deux délits d'atteinte à la vie privée - l'un selon l`alinéa 1er et l'autre selon l`alinéa 2), tout comme il est possible qu'une autre personne ait commis l'acte d'art. 226 alinéa (1er). Dans ce dernier cas, la personne qui a obtenu les données sensibles ne sera pas responsable de l`atteinte à la vie privée prévue à l'article 226 alinéa (2).

[1657] Décision *no. 51 du 24 juin 2021*, Journal Officiel, 1ère partie, no.1050, 3 novembre 2021.

avec ou sans droit, par l'une des modalités alternatives stipulées par l'art. 226, alinéa (1er) - photographie, capture, enregistrement d'images, écoute avec des moyens techniques ou enregistrement audio ».

611. Responsabilité pour divulgation, indépendante de la responsabilité pour détention. L'article 226 (2) est donc une règle de référence qui reprend des éléments de l'article 226 alinéa (1er), mais n'emprunte pas toute la disposition, de référant uniquement aux sons, conversations, images visés dans ce paragraphe, dont la divulgation, diffusion, présentation ou transmission, sans droit, est punissable. Par conséquent, l'exigence « sans droit » de l`alinéa (2) concerne l'élément important de ce fait. En même temps, le tribunal constate qu'afin de retenir l'infraction prévue à l'article 226 alinéa (2) du Code pénal, il suffit de commettre au moins une des actions, et il n'est pas nécessaire pour le sujet actif de détenir des sons, des conversations ou des images faites sans droit.

612. Le principe de séparation des pouvoirs pour la définition de l'infraction. Par conséquent, la typicalité objective de l`atteinte à la vie privée, incriminée à l'article 226 alinéa (2), n'exige pas comme condition essentielle la possession d'informations intimes (sons, conversations ou images) sans droit, en photographiant, capturant et ainsi de suite une personne (dans un logement, une pièce ou une dépendance) ou d'une conversation privée. L'acte de l'article 226 alinéa (2) devient typique par la réalisation de l'élément matériel sans droit, que l'auteur détient, possède ou a en sous sa garde ou non les sons, les conversations ou les images. « *Toute condition supplémentaire imposée par des moyens jurisprudentiels (par exemple, la condition de détention sans droit) affecterait la séparation des pouvoirs dans l'État, conduirait à la restriction de l'élément matériel aux actes de conduite non envisagés par le législateur* ».

Par conséquent, afin de retenir l'infraction prévue à l'article 226 alinéa (2) du Code pénal, en ce qui concerne l'aspect objectif, il doit y avoir divulgation, diffusion, présentation ou transmission, sans droit, de sons, conversations ou images obtenues avec ou sans droit par la photographie, la capture ou l'enregistrement d'images, l'écoute avec des moyens techniques ou l'enregistrement audio d'une personne (dans une maison ou une pièce ou une dépendance y connexe) ou d`une conversation privée.

613. L'infraction n'est pas subordonnée à la détention. Pour ces raisons, la Haute Cour a admis la plainte formée et a établi que l`atteinte à la vie privée prévue à l'article 226 alinéa (2) du Code pénal « *n'est pas conditionné par la possession de sons, de conversations ou d'images faites sans droit, en photographiant, capturant ou enregistrant des images, l'écoute par des moyens techniques ou l'enregistrement audio d'une personne dans une maison ou une pièce ou la dépendance y liée ou d`une conversation privée* ».

B. Réglementation récente dans le Code pénal : divulgation d'images intimes

614. Réglementation pénale du phénomène *revenge porn*. L'infraction d`atteinte à la vie privée, prévue à l'article 226 alinéa (2^1), est une incrimination récemment introduite par le législateur pénal par la loi 171/2023 modifiant le Code pénal[1658], suite à l'évolution de l'espace numérique et à la survenance du phénomène de *revenge-porn* (« pornographie de vengeance »). Bien que cette criminalisation sanctionne également la pornographie de vengeance, le nom n'est pas tout à fait exact, car la loi ne montre aucun mobile spécifique de l'auteur. On pourrait dire, plus correctement, que la norme en question sanctionne la « pornographie non consensuelle ». En tout état de cause, les deux dénominations font référence au même phénomène, à savoir la publication, sans le consentement de la victime, d'images sexuelles, même si elles ont été obtenues avec ou sans le consentement de la personne lésée. Nous croyons que la criminalisation de ce comportement était nécessaire, car la publication d'images intimes d'une personne affecte non seulement son image publique, mais crée également le risque que la victime soit harcelée ou même agressée par des personnes qui voient ces images. De plus, les victimes d'un tel comportement indésirable vivent constamment avec une souffrance mentale (anxiété, dépression, peur), en plus des blessures professionnelles qui peuvent survenir (dans le cas où l'employeur trouverait les images de la victime sur Internet). En outre, la protection pénale est beaucoup plus efficace que les moyens de défense[1659] civile ou administrative. Pour ces raisons, nous considérons utile la nouvelle incrimination qui sanctionne plus drastiquement la pornographie non consensuelle car, jusqu'en 2023, l'acte était sanctionné par le châtiment plus doux prévu par l'art. 226 alinéa (2) du Code pénal, bien que nous parlons d'un comportement sensiblement plus dangereux que celui prévu à l'article 226 alinéa (2), compte tenu des conséquences qu'il produit.

615. Divulgation, diffusion, présentation ou transmission d'images intimes : actes incriminés de manière autonome. Ensuite, nous montrerons pourquoi l'acte prévu à l'article 226 alinéa (2^1) du Code pénal constitue une criminalisation autonome. Tout d'abord, bien que la disposition précitée, similaire aux autres infractions pénales, ait pour objet juridique la vie privée, contrairement à cette dernière, elle protège la vie privée du point de vue de l'intimité sexuelle de la personne, qui justifie l'autonomie de cette norme juridique. De plus, le simple fait que l'alinéa (2^1) emprunte l'élément matériel de l`alinéa (2) ne justifie pas l'idée que l`alinéa

[1658] *Loi no. 171 du 14 juin 2023* modifiant et complétant l'article 226 de la loi no 286/2009 relative au Code pénal, publiée dans Journal Officiel, no 532, 15 juin 2023.
[1659] En même sens, R. Stoica, *Mult așteptata modificare adusă Codului penal: incriminarea fenomenului de „revenge porn",* 2023. Article paru sur le site https://www.juridice.ro/689652/mult-asteptata-modificare-adusa codului-penal-incriminarea-fenomenului-de-revenge-porn.html

(2^1) serait uniquement une simple variante aggravée de l'alinéa (2). Après tout, ce dernier alinéa, qui criminalise un délit autonome, renvoie à l`alinéa (1er), pas dans son intégralité, mais se réfère aux moyens d'obtention de l'information : prise de photographies, capture ou enregistrement d'images, etc. (sans compter, comme nous l'avons noté ci-dessus, si l'information a été obtenue avec ou sans droit. Nous devons aussi garder à l'esprit que l'art. 226, alinéa (2^1) prévoit des dispositions sur le sujet passif et le suivi immédiat, qui sont différentes des autres incriminations. Enfin, il faut souligner que le législateur a établi une cause d'atypicalité uniquement pour l'art. 226 alinéa (2^1), distinctes des causes d'atypicalité communes aux autres incriminations. Pour ces raisons, nous considérons que l'acte de « pornographie non consensuelle », prévu à l'article 226 alinéa (2^1) constitue un délit autonome.

Comme l'élément matériel de cet acte coïncide avec celui de l'article 226 alinéa (2), nous ne reprendrons pas la définition des termes dans cette partie de la thèse, en mentionnant seulement que la commission de plusieurs actions de l'élément matériel ne conduira pas à la rétention d'autres délits, mais d'un seul acte. Dans ce qui suit, nous nous concentrerons sur d'autres questions liées à l'aspect objectif.

616. Nécessité d'identifier la victime. Nous notons, suite à l'analyse de l'article 226 alinéa (2^1), que la divulgation, diffusion, présentation ou transmission, par quelque moyen que ce soit, d'une image intime est commise envers une personne identifiée ou identifiable par les informations fournies. Par personne identifiée, nous faisons référence à la personne dont l'identité est certaine, claire. Lorsque nous parlons d'une personne identifiable, nous comprenons que son identité n'est pas claire, mais elle peut être découverte par référence aux particularités de la personne lésée, telles qu`elles apparaissent de l'image intime (par exemple, bien que le visage de la victime ne soit pas entièrement observé à partir de l'image, un ou plusieurs signes distinctifs tels qu'un tatouage, une caractéristique faciale, etc., ou, lors de la publication de l'image, l'auteur indique le nom de la victime). À notre avis, une personne ne peut être identifiée uniquement sur la base du nom, il existe des cas de personnes portant le même nom et, en outre, il est possible qu'après la publication de l'image intime, le nom complet de la victime ne soit pas montré. Par conséquent, nous croyons qu'à côté du nom, il doit y avoir une autre caractéristique ou particularité qui permet d'identifier la personne (par exemple, le lieu où l'action de l'image intime s'est produite, un trait de la victime ou de l'auteur qui ressort de la photo, etc.).

a). Définition pénale de *l'image intime*

617. Les deux aspects de la notion d'image intime. Nous faisons référence ci-après à la définition donnée par le législateur à la notion « d'image intime ». Ainsi, selon l'art. 226 alinéa (2^2), « image intime » désigne toute reproduction, sur quelque support que ce soit, de l'image d'une personne nue qui expose totalement ou partiellement ses parties génitales, son anus ou sa zone pubienne ou, dans le cas des femmes, les seins, ou qui est impliquée dans une relation sexuelle ou un acte sexuel. En analysant le texte de la loi, nous considérons qu'il comprend deux hypothèses : 1. L'image représente une personne nue; 2. L'image montre une personne impliquée dans une relation sexuelle ou un acte sexuel.

En ce qui concerne la première thèse, la nudité peut être totale, de sorte que l'image regarde soit le corps entier, soit une ou plusieurs parties du corps, mais dans leur intégralité : les organes génitaux, l'anus ou la zone pubienne, et dans le cas des femmes également les seins. La nudité peut également être partielle, l'image comprenant partiellement une ou plusieurs parties du corps mentionnées ci-dessus. Ainsi, nous ne croyons pas que l'expression « qui expose totalement ou partiellement ses parties génitales, son anus ou sa zone pubienne ou, dans le cas des femmes, également les seins » serait une thèse autonome, justifiée par le simple fait que l'expression est précédée de la virgule. Au contraire, nous considérons que le législateur a voulu ainsi mettre en évidence quelles parties du corps, qui sont dans une image, pourraient qualifier cette image d'intime. Par conséquent, nous croyons que les images qui comprennent d'autres parties du corps que celles expressément mentionnées ne peuvent être considérées comme des images intimes représentant une personne nue. Il faut noter que le législateur fait une mention expresse dans le cas des femmes, à savoir que seuls les seins de personnes féminines pourraient qualifier une image d'intime. Par conséquent, bien que les images exposant le tronc supérieur des personnes de sexe masculin soient formellement exclues, elles pourraient être légalement classifiées en vertu de la loi prévue à l'article 226 alinéa (2) du Code pénal. De plus, dans la doctrine[1660], il a été reconnu que les dispositions de l'article 226, alinéa 2(2^2) du Code pénal s'applique également aux personnes non binaires, si leurs seins sont montrés dans une image, même si ces personnes sont présentées dans les documents officiels comme étant de sexe masculin. Enfin, il convient de noter que, pour retenir cette première thèse de l'article 226 alinéa (2^2), il n'est pas nécessaire que la personne exposée dans l'image soit impliquée dans une relation sexuelle ou un rapport sexuel.

La deuxième thèse de l'art. 226 alinéa (2^2) montre que par « image intime » on entend aussi les images qui montrent l'implication de la personne lésée dans une relation sexuelle ou

[1660] M. Udroiu, *Sinteza modificărilor legislative operate prin Legile 171/2023, n° 213/2023, n° 217/2023 și n° 248/2023 în cazul infracțiunilor contra persoanei și a celor contra patrimoniului,* Analele Universității din București – seria Drept, Forum juridic, n° 2, 2023. p.126.

un acte sexuel. Dans cette hypothèse, la personne lésée n'est pas obligée d'être nue et peut même être habillée pendant les rapports sexuels. Jugeant par les dispositions expresses, il semblerait que, du moins formellement, l'art. 226 alinéa (2^2) la deuxième thèse ne considère pas qu'une image est intime lorsqu'elle dépeint d'autres actes de pénétration vaginale ou anale - art. 218 alinéa (2) du Code pénal (par exemple, pénétration vaginale ou anale avec des objets) - ou actes sexuels propres à une agression sexuelle (comme toucher ou embrasser les seins, l`organe génital, etc.). Nous supposons que cette omission apparente du législateur est prévue soit par les dispositions de l'article 226 alinéa (2^2) thèse I, soit par les dispositions de l'article 226 alinéa (2). Nous croyons qu'une disposition plus complète aurait été salutaire, étant donné que tout autre acte de pénétration vaginale ou anale ou d'agression sexuelle est tout aussi dangereux dans le contexte de la protection de la vie intime de la personne. Nous proposons, à titre d'exemple, le libellé suivant : « Par image intime, on entend toute reproduction, quel que soit le support, de l'image d'une personne (…) qui est impliquée dans un des actes prévus par l'art. 218 ou l'art. 219 Code pénal ».

618. L'accord de détention n'implique pas implicitement l'accord de diffusion. En ce qui concerne l'image intime, nous attirons l'attention sur le fait qu'elle peut provenir même du sujet passif de ce délit, l`art. 226 alinéa ($2^1$) n`imposant pas que l'image intime ait nécessairement été obtenue par l'auteur, avec ou sans droit. Ainsi, il est possible que la victime ait envoyé à l'auteur l'image intime volontairement et que le sujet actif la rende publique sans le consentement de la victime. Nous mentionnons également que l'art. 226 alinéa (2^1) se réfère à la divulgation, diffusion, présentation ou transmission d'une image exclusivement (intime), donc la loi ne fait pas référence aux sons ou conversations.

619. Possibilité d'identifier la victime : condition essentielle pour définir l'infraction. Une autre condition essentielle, exigée par la règle de criminalisation de l'article 226 alinéa (2^1) concerne essentiellement la publication de l'image intime de la personne identifiée ou identifiable sans le consentement de celle-ci. À cet égard, il importe peu que la victime ait consenti ou non à la réalisation d'images intimes, car, comme nous l'avons montré ci-dessus, il est possible que l'image provienne de la personne lésée elle-même. Par conséquent, même si la personne consent à obtenir des images sexuelles, ce consentement n'implique pas nécessairement la divulgation, la diffusion, la présentation ou la transmission de ces images (donc si la personne a donné son consentement à la publication des images, l'acte ne répondra pas à la typicalité objective du délit).

b). Conséquences immédiates : souffrance mentale

620. Atteinte à l'image et provocation de souffrances psychiques. Une dernière mention que nous allons faire est la conséquence spécifique immédiate de ce délit. Ainsi, la disposition juridique de l'article 226 alinéa (2^1) montre que la divulgation, la diffusion, la présentation ou la transmission de l'image intime dans l'espace public doit être de nature à causer au sujet passif une détresse mentale (par exemple dépression, anxiété, peur, etc.) ou de nuire à son image. Il n'est donc pas nécessaire que les souffrances psychiques ou l`atteinte apportée à l'image de la personne lésée soient concrètes, et il suffit que l'action de l'auteur soit capable, apte de produire de telles conséquences.

C. Installation de moyens techniques d'enregistrement audio-vidéo

621. La dernière infraction prévue à l'art. 226 du Code pénal concernant l`atteinte à la vie privée est celle prévue à l`alinéa (5), qui stipule qu'il sera considéré une infraction l`installation, sans droit, des moyens techniques d'enregistrement audio ou vidéo, dans le but de commettre les actes prévus par l'art. 226, alinéas (1) et (2) du Code pénal. Nous notons que la règle de criminalisation de l`article (5) constitue une infraction - moyen, qui suit la commission des infractions visées aux alinéas (1) ou (2)[1661], sans affecter en aucune façon l'autonomie des infractions.

622. Incrimination tant de la préparation que de la commission de l'infraction. En faisant une comparaison entre les quatre infractions, nous constatons que, alors que l'acte de l'article 226 alinéa (1er) sanctionne pratiquement l'obtention d'informations sur une personne ou une conversation privée, et les faits de l'article 226 alinéas (2) et (2^1) sanctionnent la publication des renseignements obtenus en vertu de l`alinéa (1er), l'infraction visée à l'article 226, alinéa (5) du Code pénal sanctionne les actes de préparation, en tant qu'acte consommé, afin de commettre les actes visés aux alinéas (1) ou (2).

623. Incrimination de l'installation de dispositifs d'espionnage, même en cas de non-fonctionnement. En ce qui concerne l'élément matériel, la loi prévoit une seule action : l`installation. Par « installation » de moyens techniques, nous entendons la pose, l`implantation, l'installation d'appareils capables d'obtenir et/ou de stocker des sons, des images ou des conversations (tels que microphones, caméras vidéo, portable, etc.). Nous croyons que l'acte sera typique même lorsque l'équipement technique ne fonctionne pas après l`installation, car,

[1661] Il convient de noter que l'infraction visée à l'article 226 alinéa (5) vise à commettre les infractions visées aux articles (1) et (2) du même article, à l'exclusion de l`art. (2^1).

afin de retenir le délit, il n'est pas obligatoire que le but de commettre l'acte - les actes de l'article 226 alinéas (1) et (2) - soit atteint. Si toutefois l'objectif est atteint, nous allons retenir une concurrence des infractions entre l`acte de l`alinéa (5) et celui/ceux de l`alinéa (1er) et/ou (2)[1662].

Comme pour toutes les autres infractions d`atteinte à la vie privée, l'élément matériel (mise en place de moyens techniques) doit également être exécuté sans droit.

624. Controverses concernant la norme d'incrimination : les infractions-but. Nous voulons souligner ci-après un problème concernant la norme de l'incrimination. L`art. 226 alinéa (5) précise que l`installation de moyens techniques est effectuée afin de commettre les actes visés aux alinéas (1) et (2) du même article. Il est à noter que le législateur a utilisé le terme « et » pour indiquer les délits dont la commission est poursuivie. Ainsi, il est suggéré qu'en commettant l'élément matériel d`installation, l'auteur doit chercher à obtenir des sons, des images ou des conversations - alinéa (1er), ainsi que la divulgation, la diffusion, la présentation ou la transmission de celles-ci - alinéa (2). Nous ne considérons pas que l'auteur doive envisager de commettre les infractions visées dans les deux alinéas, mais il suffit qu'il poursuive au moins l'acte de l'article 226 alinéa (1er) du Code pénal. Toutefois, il n'est pas possible que par l'infraction prévue à l`alinéa (5) de l'art. 226 du Code pénal de poursuivre uniquement la commission de l'acte visé à l`alinéa (2), parce que, pour pouvoir rendre publique une information intime, l'auteur doit avoir cette information, avec ou sans droit.

Un dernier aspect sur lequel nous voulons attirer l'attention est le fait que les délits – finalité visés aux alinéas (1) et (2) sont liés à des sons, à des images ou à des conversations. Par conséquent, l`installation de moyens techniques pour localiser une personne ne constituera pas un délit, pouvant éventuellement discuter d'abus de pouvoir lorsque l'acte est commis par un agent public/privé.

a). Éléments typiques des variantes du délit d`atteinte à la vie privée

625. Conséquences immédiates La conséquence immédiate de la variante prévue par l'article 226 alinéa 1er consiste à l`atteinte à la vie privée. Étant donné qu'il s'agit d'une « atteinte », nous concluons que c'est un délit de résultat. En ce qui concerne les faits visés aux alinéas (2) et (5) de l'article 226, la conséquence immédiate des faits est qu'un état de danger

[1662] De plus, si l`installation des moyens techniques est effectué dans un logement, une pièce ou une dépendance ou dans un établissement professionnel, nous conserverons l'infraction d'atteinte à la vie privée en vertu de l'article 22, alinéa (5) du Code pénal en concurrence avec la violation du domicile ou de l'établissement professionnel de l'art. 225 Code pénal, ne pouvant pas affirmer que l'acte d`atteinte à la vie privée absorberait celui d'atteinte au domicile ou à l`établissement professionnel.

résulte d'une ingérence dans la vie privée de la personne, de sorte que les deux faits autonomes sont des infractions de danger abstrait.

En ce qui concerne l'infraction visée à l`alinéa (2^1), sa conséquence immédiate est la création d'un état de danger en ce qui concerne le droit à la vie privée, un état de danger qui survient lorsque l'action dangereuse est commise - divulgation, diffusion, présentation ou transmission. Cela ferait de l'infraction actuelle un danger abstrait. Cependant, nous rappelons que l'élément matériel de cet acte doit être capable de produire (et non pas réellement produire) une souffrance mentale ou un préjudice à l'image de la personne lésée, et la capacité de l'élément matériel de produire un tel danger doit être prouvée (comme dans le cas des infractions de danger concret). Par conséquent, comme il a également été indiqué dans la doctrine[1663], l'infraction prévue à l'article 226 alinéa (2^1) constitue un délit de danger potentiel, c'est-à-dire de danger abstrait - concret[1664].

626. Lien de causalité. En ce qui concerne le lien de causalité, dans le cas de l'infraction visée à l'article 226 alinéa (1er) du Code pénal, celle-ci doit être prouvée, étant une infraction de résultat, alors que dans le cas des infractions visées à l'article 226 alinéas (2) et (5) du Code pénal, étant des infractions de danger abstrait, le lien de causalité résulte de la commission même de l'acte prévu par la norme pénale (lien de causalité *ex re*). Dans le cas de l'infraction visée à l`alinéa (2^1) du même article, il n'est pas nécessaire de prouver l'état de danger, mais il doit être prouvé que les actes prévus par la règle de criminalisation auraient été susceptibles de produire des souffrances mentales/d'affecter l'image du sujet passif.

627. Côté subjectif. En ce qui concerne le caractère subjectif, les infractions visées à l'article 226 alinéas (1), (2) et (2^1) sont commises avec une intention directe ou indirecte, sans pertinence, dans le but de conserver la typicité subjective, le motif ou le but, qui peuvent être pris en compte lors de l'individualisation de la peine. En ce qui concerne l'infraction visée à l'article 226 alinéa (5) du Code pénal, celle-ci est commise exclusivement avec une intention

---

[1663] M. Udroiu, *Sinteza modificărilor legislative operate prin Legile 171/2023, n° 213/2023, n° 217/2023 și n° 248/2023 în cazul infracțiunilor contra persoanei și a celor contra patrimoniului,* Analele Universității din București – seria Drept, Forum juridic, n° 2, 2023. p.127.

[1664] Ainsi, dans la doctrine (F. Streteanu, D. Nitu, *Drept penal. Partea generale*, vol.I, Universul Juridic, Bucarest, 2014. p.298), on a montré qu'entre les délits de danger abstrait et concret, il y a une catégorie intermédiaire, mixte de délits, qui emprunte des éléments à la fois de l'infraction de danger abstrait et de l'infraction de danger concret, qu'on appelle infraction de danger potentiel ou danger abstrait - concret. Il entre dans cette dernière catégorie d'infractions que les faits pour lesquels la règle de criminalisation exige que l'acte indésirable soit susceptible de mettre en péril l'objet juridique du délit, sans exiger au contraire que la valeur sociale protégée ait effectivement été, concrètement en danger. Ce type de délit ne peut pas être considéré comme une infraction abstraite, puisque la capacité de l'acte matériel à créer un état de danger n'est pas présumée par la loi (car l'existence même d'un état de danger est présumée), mais doit être prouvée. En outre, les infractions potentiellement dangereuses ne peuvent être classées comme des infractions réellement dangereuses, parce que l'existence de l'état de danger ne doit pas être prouvée, ce qui entraîne *ex re*, et il suffit de montrer qu'elle aurait pu intervenir.

directe, parce que l'action d`installation est commise dans le but de commettre les actes des alinéas (1er) et (2).

628. Formes du délit. En ce qui concerne les actes préparatoires et la tentative, nous notons qu'ils sont théoriquement possibles, mais non spécifiquement incriminés, sauf pour la disposition de l'article 226 alinéa (5), où le législateur pénal a clairement criminalisé les actes de préparation.

La consommation de l'infraction a lieu au moment où est commis l'élément matériel de l'infraction, dans le cas des infractions d'atteinte à la vie privée prévues aux articles 226 alinéas (1er), (2) et (5), et dans le cas de l'acte visé à l'alinéa (21), la consommation se produit lorsque la victime a appris la commission de l'article matériel.

En outre, en cas d`atteinte à la vie privée, nous pouvons parler d'une forme continue[1665] de celle-ci, lorsque, par exemple, une conversation privée est enregistrée, auquel cas l'infraction sera épuisée, à notre avis, aux moments suivants : soit au moment de l`arrêt de l'enregistrement (si les moyens techniques d'enregistrement, par exemple, ont cessé d'enregistrer en raison de certaines limitations techniques ou des défauts), s'il survient avant la fin de la conversation, soit au moment de la fin de la conversation.

629. Sanctions. En ce qui concerne les sanctions prévues par la loi : pour l'acte visé à l'article 226 alinéa (1er), la peine est une peine d'emprisonnement de un mois à six mois ou l'amende pénale; pour l'acte visé à l'article 226 alinéa (2), la peine est une peine d'emprisonnement de trois mois à deux ans ou une amende pénale; pour l'acte visé à l'article 226 alinéa (21), la peine est une peine d'emprisonnement de six mois à trois ans ou une amende pénale; pour l'acte visé à l'article 226 alinéa (5) , la peine est de un à 5 ans d'emprisonnement. Il est curieux de savoir pourquoi le législateur a jugé plus juste d'imposer une peine plus sévère pour une infraction consistant en un acte de préparation, par rapport aux autres infractions constituant l'objectif poursuivi.

630. Aspects procéduraux. Analyser le positionnement des alinéas dans le cadre de l'art. 226 du Code pénal, nous déduisons ainsi que l'ouverture de la procédure pénale est effectuée sur plainte préalable de la personne lésée dans le cas des infractions visées à l'article 226 alinéas (1er), (2) et (21) du Code pénal, et dans le cas de l'infraction visée à l`alinéa (5), l'ouverture d'une procédure pénale est effectuée d'office.

D. Causes particulières atypiques de délits

[1665] M. Udroiu, *Sinteze de drept penal. Partea specială*, vol.I, C.H. Beck, 2022.p.409.

631. Causes justificatives spéciales. Dans cette sous-section, nous visons à atteindre les derniers alinéas de l'art. 226 du Code pénal que nous n'avons pas abordé jusqu'à présent, notamment les alinéas (4) et (4[1]) sur les causes atypiques spéciales des délits d`atteinte à la vie privée[1666]. Nous mentionnons d'avance que les deux alinéas concernent les situations où, bien que l'acte soit typique du point de vue objectif, en raison des circonstances dans lesquelles il est commis, l'acte est dépourvu de la première caractéristique essentielle du délit : la typicité. En même temps, nous soulignons qu'il y a aussi des arguments pour interpréter l'expression du législateur comme *une cause de justification spéciale*[1667].

632. Cause justifiée par un intérêt légitime. Nous commençons l'analyse par les situations réglementées par l'article 226 alinéa (4) du Code pénal, qui s'applique aux infractions visées aux alinéas (1er) et (2) du même article. Selon la lettre a), l'acte ne constitue pas une infraction s'il est commis par la personne qui a participé à la rencontre avec la personne lésée au cours de laquelle les sons, les conversations ou les images ont été capturés, si cela justifie un intérêt légitime. Le manque de typicité est motivé par le fait que la personne lésée a permis à l'auteur d'assister à la réunion et à l`atteinte à la vie privée. Toutefois, cet accord ne s'étend qu'à la simple participation, non pas à la photographie, à la capture et ainsi de suite, par conséquent le sujet actif doit justifier d'un intérêt légitime et licite pour lequel il veut « superviser » l'événement. Par exemple, l'auteur justifie un intérêt licite lorsqu'il veut utiliser des sons, des images ou des conversations dans un processus contre la personne lésée (que ce soit au civil ou au pénal).

633. Cause justifiée par l'intention explicite de la victime. De plus, selon la lettre b), l'acte visé aux alinéas (1er) ou (2) ne constitue pas une infraction si la victime a agi explicitement dans l'intention d'être vue ou entendue par l'auteur. La raison de l'élimination de la typicité est basée sur l'idée que la personne lésée veut s'exposer en public, donc, selon l'opinion de l'auteur du délit, la victime a délibérément renoncé à sa vie privée. En d'autres termes, l'attitude explicite de la personne lésée est assimilée à une présomption de consentement à l'attitude (théoriquement illicite) de l'auteur. Par exemple, nous pouvons penser à la situation où la victime parle à haute voix du voisin d'à côté, dans l'intention qu'il l'entende, le voisin qui a ensuite entendu la discussion et a commencé à la filmer.

[1666] La doctrine a établi des noms différents pour les situations réglementées dans les deux alinéas : « *hypothèses spéciales pour éliminer la typicité de l'acte* » (M. Udroiu, *Sinteze de drept penal. Partea specială*, vol. I, C.H. Beck, 2022., p.407), « *cas d'exclusion du délit* » (V. Cioclei, *Drept penal. Partea specială I. Infracțiuni contra persoanei și infracțiuni contra patrimoniului*, 2e éd., C.H. Beck, 2017. p.242), et même dans une autre opinion ont été considérés comme des « conditions négatives de typicité » (S. Bogdan, D.A. Serban, *Drept penal. Partea specială*, Universul Juridic, 2022. p.439-443).

[1667] T. Toader, *Explicațiile Noului Cod Penal*, vol. IV, Universul Juridic, 2016. p.247.

634. Cause justifiée par la preuve d'une infraction. Conformément à l'article 226 alinéa (4) lettre c), l'acte visé aux alinéas (1er) ou (2) ne constitue pas une infraction si l'auteur de l'infraction constate qu'elle a été commise ou contribue à la preuve de la commission d'une infraction. Le manque de typicité dans cette situation se justifie par le fait que, dans certains contextes, l'intérêt général à la justice est plus important que la vie privée de la personne « surveillée ». Par exemple, il ne sera pas typique l`atteinte à la vie privée lorsque l'auteur filme les actes de violence commis par son voisin sur son enfant et sa femme. Nous croyons que cette cause particulière d'atypicité fonctionnera également lorsque l'auteur ne capture que la commission d'un acte prévu par le droit pénal (lorsqu'il manque un élément constitutif de l'infraction) et non seulement lorsque l'acte est un délit, mais aussi lorsque l'acte est un délit alors que l'auteur qui « commet » l`atteinte à la vie privée n'est pas un spécialiste dans le domaine juridique et ne peut déterminer si l'acte qu'il capture est un délit ou simplement un acte prévu par le droit pénal. Il est également possible d'invoquer l'erreur sur le caractère infractionnel du fait surpris - art. 30 alinéa (1er) du Code pénal, auquel cas la typicité subjective de l'atteinte à la vie privée sera supprimée. Il n'importe pas non plus, pour retenir ce cas d'atypicité, que l'acte qui a été commis ait été commis dans des conditions justificatives, non imputables, non-punitives ou d`un autre empêchement au déclenchement de l'action pénale (comme l'absence ou le retrait de la plainte antérieure). Il convient de noter que si l'ingérence dans la vie privée a eu lieu sur une période plus longue, au cours de laquelle l'auteur capture la commission d'un délit/fait prévu par le droit pénal, nous aurons un manque typique d`atteinte à la vie privée seulement pour la période dans laquelle l'infraction a été prise et non pour toute l'activité d`atteinte à la vie privée.

635. Cause justifiée par la défense de l'intérêt collectif. La dernière lettre de l'article 226 alinéa (4), lettre d), indique que l'acte visé aux alinéas (1er) ou (2) ne constitue pas une infraction si des faits d'intérêt public qui ont une importance pour la vie de la collectivité sont pris et dont la divulgation présente des avantages publics supérieurs au préjudice causé à la personne lésée. Cette cause d'atypicité vient résoudre l`atteinte à la vie privée par les journalistes, étant donné que la presse a le droit à la liberté d'expression (dans les limites de la bonne foi).[1668] En l`espece, nous donnerons un exemple de situation examinée par la Cour européenne des droits de l'homme[1669]. Dans le cas présent, plusieurs journalistes ont enregistré une conversation avec un

[1668] C. Massis de Solere*, La délicate frontière entre le délit d'usurpation d'identité numérique et la loi de 1881*, Légipresse, 2019. Dans le contexte juridique actuel, la protection de la vie privée ne peut être considérée comme un droit absolu, car elle doit se plier aux exigences imposées par la liberté d'expression. Ainsi, lorsque les informations divulguées contribuent à un débat d'intérêt public, l'ingérence dans la sphère privée peut être admise, à condition qu'elle reste proportionnée et ne dépasse pas ce qui est nécessaire dans une société démocratique.
[1669] La Cour européenne des droits de l`homme, Décision du 24 février 2015 dans l`affaire *Haldimann et autre c. la Suisse.*

courtier sans savoir qu'il était enregistré. Par la suite, ces journalistes ont fait un reportage sur la mauvaise qualité de l'information fournie par les courtiers d'assurance privés, ce qui entraîne des préjudices pour le consommateur. La CEDH a souligné que bien que le courtier ait été enregistré à son insu, sans donner son consentement à l'enregistrement et sans être une personne publique, il était apprécié que le reportage fait ne concerne pas la personne du courtier, mais les pratiques commerciales qu'ils appliquent. La Cour a établi que l'ingérence des journalistes dans la vie privée du courtier n'est pas suffisamment grave pour priver le public de son droit d'être informé.

636. Capture, sans diffusion, d'images intimes justifiée par la preuve d'un délit. La dernière disposition de l'art. 226 du Code pénal à analyser se réfère à l`alinéa ($4^1$) sur la cause spéciale d'atypicité de l'infraction prévue à l'art. 226 alinéa ($2^1$) – « la pornographie non consensuelle ». Selon l`alinéa (4^1), il ne constitue pas un délit de « pornographie non consensuelle » si l'auteur saisit la commission d'un délit ou contribue à prouver qu'un délit a été commis. Nous notons la similitude entre cet alinéa et les dispositions de l'alinéa (4) lettre c). Par conséquent, pour l'identité de raison, les questions présentées en (4) lettre c) sont applicables également à l`alinéa (4^1). Par exemple, cette cause d'atypicité sera retenue lorsque l'auteur capture la commission d'une infraction de viol en enregistrant vidéo l'acte.

§2. ANALYSE DE LA JURISPRUDENCE ROUMAINE: 2014 – 2024

637. Évolution de la jurisprudence roumaine par rapport à l'évolution technologique. Le but de cette analyse est d'examiner l'évolution de la jurisprudence roumaine dans le domaine de la protection de la vie privée, en se concentrant sur la façon dont les tribunaux roumains ont abordé le délit d`atteinte à la vie privée, réglementé par l'art. 226 du Code pénal roumain. L'analyse vise à identifier et mettre en évidence les principales tendances dans la résolution de ces cas, qui soulèvent des questions juridiques de plus en plus controversées.

Il sera question de la manière dont les tribunaux nationaux ont traité les difficultés spécifiques rencontrées dans le règlement de ces affaires, telles que les conflits entre la protection de la vie privée et d'autres droits fondamentaux, ainsi que l'interprétation des règles juridiques face aux nouveaux défis technologiques. L'analyse explorera également les solutions prononcées (acquittement ou condamnation), ainsi que les justifications des tribunaux dans le contexte des technologies émergentes qui permettent des intrusions de plus en plus profondes dans la vie privée des citoyens, telles que l'utilisation de données personnelles, la surveillance numérique et l'accès non autorisé à des renseignements sensibles.

638. Analyse de l'interprétation et de l'application de la doctrine. À cet égard, il sera analysé non seulement l'application des dispositions légales, mais aussi la façon dont les juges ont interprété et appliqué les normes internationales et nationales de protection de la vie privée face aux nouveaux défis posés par le progrès technologique et son impact sur la vie privée des individus. En particulier, la recherche portera sur la manière dont les tribunaux ont traité l'intrusion technologique et ses limites par rapport aux droits fondamentaux des individus.

639. Utilisation de la plateforme Rejus. Les données utilisées dans cette analyse ont été extraites de la plateforme Rejus[1670], un système national qui donne accès à l'information sur les décisions judiciaires rendues par les tribunaux roumains. Ainsi, *le portail de la jurisprudence est une application conçue et développée par le Conseil supérieur de la magistrature pour permettre aux citoyens et aux praticiens de la justice un accès plus facile aux jugements rendus par les tribunaux nationaux*.[1671]

L'analyse porte sur la période 2014 - 2024, considérant que 2014 marque une étape importante dans l'évolution des réglementations juridiques en Roumanie, en criminalisant le délit d'atteinte à la vie privée. Cette réforme a introduit de nouvelles réglementations qui répondent aux défis posés par les technologies émergentes. Ainsi, la période choisie reflète non seulement l'impact de la nouvelle réglementation sur la jurisprudence nationale, mais aussi ses

[1670]Consiliul Superior al Magistraturii, Portalul de Jurisprudenta Rejust. https://www.rejust.ro/info/despre
[1671] Ibidem

récents développements dans le contexte technologique, où les technologies avancées permettent des invasions toujours plus profondes dans la vie privée des citoyens.

640. Alignement de la doctrine roumaine sur les exigences européennes. L'article 226 du Code pénal intitulé *Atteinte à la vie privée* est une composante essentielle de la protection pénale des droits fondamentaux de la personne en Roumanie, prévoyant un règlement spécifique sur la protection de la vie privée face à l'intrusion, notamment dans le contexte d'un développement technologique rapide. Par ce règlement[1672], le législateur national complète le cadre de la protection pénale des valeurs garanties à l'article 8 de la Convention européenne des droits de l'homme qui garantit le droit de toute personne à la protection de sa vie privée et de ses données personnelles, son domicile et sa correspondance.

641. De nouvelles façons de violer la vie privée. Dans le contexte des technologies émergentes qui permettent un accès de plus en plus facile et approfondi aux informations personnelles, l'article 226 s'avère essentiel pour combattre les délits d'invasion de la vie privée qui peuvent être commis par des moyens technologiques avancés tels que le cyber-espionnage, le piratage et la surveillance numérique. Ce nouveau règlement reflète un souci constant d'adaptation des législations nationales aux évolutions technologiques, qui rendent de plus en plus difficile la protection des données personnelles à l'ère numérique. À cet égard, les dispositions du Code pénal restent structurées pour combattre les faits qui, par l'utilisation des technologies modernes, permettent de profondes invasions dans le domaine de la vie privée individuelle, affectant directement la confidentialité des communications et la sécurité des données personnelles.

642. Interdépendance entre droit national et droit international. Compte tenu de ces interdépendances entre le droit national et les normes internationales, la protection de la vie privée en Roumanie est renforcée et l'article 226 devient un lien essentiel dans un système de protection complexe qui répond aux défis posés par les technologies modernes. L'évolution de la jurisprudence dans ce domaine reflète également une adaptation constante de l'interprétation du droit aux réalités d'une société de plus en plus interconnectée sur le plan numérique, où l'invasion de la vie privée ne provient plus uniquement de sources physiques, mais aussi des délits cybernétiques de plus en plus sophistiqués[1673].

Dans le cadre de l'analyse de la jurisprudence nationale, l'accent sera mis sur la typologie des solutions apportées par les juridictions nationales. Les cas où des solutions de condamnation, de sursis à l'application de la peine, d'exonération de la peine, d'acquittement

[1672] G. Antoniu, T. Toader (coor), V. Brutaru, C. Duvac, I. Ifrim, D. I. Lămășanu, I. Pascu, M. Safta, C. Sim, I. Vasiu, *Explicațiile Noului Cod penal*, vol.III, Universul Juridic, Bucarest, 2015 p.226

[1673] M. Udroiu, *Fișe de drept penal. Partea specială*. Universul Juridic, București, 2014, p. 52.

ou même d'arrêt de la procédure pénale seront choisies de manière à refléter la diversité des approches judiciaires. Ces solutions seront analysées dans le contexte spécifique des technologies émergentes, afin de mettre en évidence la manière dont les tribunaux ont interprété et appliqué les règles juridiques, notamment face aux nouveaux défis découlant de l'invasion de la vie privée par des moyens technologiques. Il sera analysé également comment chaque tribunal a pris en compte les particularités de chaque affaire, y compris l'impact des nouvelles technologies sur le droit à la vie privée et la protection des données personnelles.

Ainsi, un total de 45 décisions pertinentes au sujet de la thèse a été identifié dans la plateforme Rejust, toutes liées au délit d'atteinte à la vie privée, réglementé par l'article 226 du Code pénal. Ces décisions émanent des tribunaux de différents départements de Roumanie et reflètent une variété de solutions, y compris les condamnations, les reports de peines, les renonciations à la peine, les acquittements et l'arrêt des procédures pénales. Cette sélection a pour but de mettre en lumière la manière dont les tribunaux roumains ont interprété et appliqué les réglementations pénales dans le contexte de l'évolution technologique, posant ainsi de nouveaux défis à la protection du droit au respect de la vie privée et la protection des données personnelles.

A.Nombre d'affaires d'atteinte à la vie privée, en augmentation

643. Augmentation des infractions contre la vie privée. Si l'on examine leur répartition au fil des années, on constate une augmentation importante du nombre de cas d'atteinte à la vie privée depuis 2020, le sommet étant atteint en 2023 et 2024, ce qui suggère un accroissement des préoccupations et une plus grande application de la législation dans ce domaine. Plus précisément, en 2024, 11 jugements ont été rendus et en 2023, un total de 13 jugements, ce qui indique une tendance claire à l'augmentation des atteintes à la vie privée et une prise de conscience croissante des risques posés par les technologies émergentes par les tribunaux. Cette augmentation du nombre de jugements traduit, d'une part, une plus grande application de la législation dans le domaine et, d'autre part, une adaptation de l'appareil judiciaire aux défis posés par la numérisation rapide de la vie quotidienne. En revanche, les années précédentes, le nombre de jugements était beaucoup plus faible : seulement 6 jugements en 2022, 3 jugements en 2020 et un seul en 2016 et 2017, suggérant une approche moins active des tribunaux face aux phénomènes technologiques émergents.

a). Adaptation de la jurisprudence aux défis de l'évolution technologique

644. La nécessité d'une adaptation législative continue. Les chiffres suggèrent une augmentation du nombre de cas et une tendance à une application plus cohérente de la réglementation de l'art. 226 du Code pénal à partir de 2020 et jusqu'à ce jour. Ces jugements traduisent également une approche de plus en plus approfondie des tribunaux, qui sont de plus en plus conscients de la complexité et de l'impact des technologies avancées sur les droits fondamentaux des citoyens, notamment en ce qui concerne le droit à la vie privée. Les tribunaux roumains ont commencé à intégrer les défis posés par le développement rapide des technologies numériques et des moyens de communication modernes, reconnaissant qu'ils peuvent faciliter des invasions profondes dans la sphère personnelle des individus. Dans ce contexte, les jugements analysés reflètent non seulement l'application des réglementations existantes, mais illustrent également une adaptation constante de la jurisprudence aux nouvelles réalités technologiques afin d'assurer une protection adéquate des droits fondamentaux contre les risques émergents.

645. Analyse de la jurisprudence nationale. Ces jugements ont été rendus par des tribunaux de diverses régions du pays, notamment à Bucarest, Cluj, Sibiu, Craiova, Timisoara, Iasi et bien d'autres. Cette diversité géographique suggère que le phénomène de l'atteinte à la vie privée ne se limite pas à un certain type de juridiction ou de zone, mais est un problème d'actualité dans toute la Roumanie. En même temps, cela reflète une application uniforme de la législation et un souci constant des tribunaux pour la protection des droits fondamentaux des citoyens, quel que soit le lieu du délit.

En ce qui concerne la typologie des solutions rendues, les tribunaux ont appliqué différentes sanctions selon la gravité de l'acte et les circonstances de chaque affaire. Ainsi, les condamnations ont été enregistrées à la fois avec des peines privatives de liberté et avec sursis de l'exécution de la peine sous surveillance, dans la plupart des affaires étant appliquées des peines reflétant la gravité du délit, compte tenu de leur impact sur le droit à la vie des personnes concernées.

b). Clémence dans la punition du délit d'atteinte à la vie privée

Au total, 29 solutions de condamnation ont été enregistrées dans les affaires d'atteinte à la vie privée soumises à l'analyse, dont 4 condamnations à l'emprisonnement, dans 16 autres affaires les tribunaux ont appliqué des solutions de condamnation avec sursis de l'exécution de

la peine sous supervision, et dans 9 autres affaires, les tribunaux ont opté pour l'application d'une amende.

646. Application de peines privatives de liberté. Ainsi, les solutions de condamnation avec emprisonnement ont été appliquées spécifiquement dans deux situations principales. La première a été lorsque les prévenus ont commis plusieurs infractions en compétition, commises sur la base des mêmes résolutions infractionnelles, qui ont un impact significatif sur la vie privée des victimes. Dans de tels cas, les tribunaux ont estimé que le nombre et la gravité des infractions commises justifiaient l'application d'une peine plus sévère, à savoir la peine d'emprisonnement, pour refléter la complexité et les effets cumulatifs de l'acte, et d'assurer une réponse proportionnée à la gravité des dommages causés aux victimes.

La deuxième situation dans laquelle des peines privatives de liberté avec exécution ont été appliquées était lorsque les prévenus avaient un casier judiciaire, commettant un délit d'atteinte à la vie privée, après qu'une condamnation pour des délits qui étaient préjudiciables à la vie privée ou d'autres délits qui protègent d'autres droits fondamentaux soit restée définitive. Dans de tels cas, les tribunaux ont estimé que l'application d'une peine d'emprisonnement est nécessaire pour décourager la récidive et protéger plus efficacement les droits des victimes.

647. Causes et critères de réduction de peine. En revanche, les tribunaux n'ont pas appliqué de peines privatives de liberté lorsque les infractions d'atteinte à la vie privée ont été commises de façon isolée, sans circonstances aggravantes. Par exemple, lorsque l'acte était un acte ponctuel commis par une personne sans antécédents criminels pertinents ou sans l'existence d'un concours des délits, les tribunaux ont estimé que l'application d'une peine privative de liberté n'était pas nécessaire. Dans ces situations, des sanctions plus légères, comme le sursis de l'exécution de la peine sous surveillance ou l'application d'une amende, ont été préférées, étant donné que l'infraction n'était pas considérée comme suffisamment grave pour justifier une peine privative de liberté.

Ainsi, les condamnations pour l'exécution de la peine privative de liberté étaient réservées aux cas où la conduite infractionnelle de la personne était répétée ou avait un impact significatif sur la victime, et l'application d'une peine plus légère n'était pas suffisante pour assurer la protection des droits fondamentaux de la victime et empêcher la poursuite des délits.

648. Trois solutions d'acquittement en dix ans. Il y a eu d'autres jugements d'acquittement, habituellement dans les affaires où il n'y avait pas suffisamment de preuves pour étayer les accusations ou lorsque le tribunal a conclu que toutes les conditions juridiques pour prouver la culpabilité n'étaient pas remplies. Étant donné que le nombre de jugements d'acquittement n'est que de trois, ces solutions reflètent un faible pourcentage dans les affaires

analysées, ce qui suggère que la plupart des procès se sont terminés par des solutions de condamnation.

Le report de la peine et l'exonération de celle-ci ont été prononcés comme solutions dans les cas où les tribunaux estimaient que l'infraction commise est de faible gravité, compte tenu de la nature et de l'étendue des conséquences, les moyens utilisés, la manière et les circonstances dans lesquelles elle a été commise, le motif et l'objectif poursuivis. Les tribunaux ont également évalué le comportement de la personne après que le délit ait été commis, ce qui a eu une influence importante sur l'établissement d'une solution plus favorable.

649. Sept jugements de différenciation de la peine. Dans le cas de 7 solutions de différenciation de l'application de la sanction et d'une solution pour renoncer à l'exécution de la peine, les juridictions nationales ont estimé que les infractions commises par les prévenus n'avaient pas eu d'impact significatif sur les victimes ou sur l'ensemble de la société en ensemble et leur gravité était jugée faible. Ces solutions reflètent une approche proportionnée des tribunaux qui, selon les circonstances de chaque affaire, ont jugé que des mesures plus douces, telles que le report de l'exécution d'une sanction ou la dispense de l'exécution d'une sanction, sont appropriées pour répondre à des délits graves sans compromettre le but préventif du droit pénal.

De plus, des solutions pour mettre fin au procès pénal ont même été prononcées, celles-ci étant présentes dans les cas où il a été constaté que la victime avait retiré sa plainte antérieure contre le prévenu[1674]. Ainsi, dans les 5 affaires spécifiques où une solution pour la clôture de la procédure pénale a été ordonnée, le retrait de la plainte antérieure a conduit à la conclusion de la procédure pénale, soulignant que dans de telles situations, la procédure pénale peut être close lorsqu'il n'y a pas de volonté de la victime de poursuivre la procédure, c'est-à-dire le droit de renoncer à la procédure pénale devant les autorités judiciaires.

650. Tendances. La diversité des solutions apportées par les juridictions nationales met en évidence une nette tendance à l'adaptation aux nouvelles réalités technologiques, traduisant un effort continu pour assurer la bonne application des règles juridiques dans un contexte dynamique et en constante évolution. Les tribunaux ont démontré une capacité accrue à réglementer et sanctionner les infractions visant la protection de la vie privée, compte tenu de l'impact croissant de la numérisation et des technologies émergentes sur la vie privée des individus.

[1674] Le délit d'atteinte à la vie privée prévu et puni par l'art. 226 du Code pénal appartient à la catégorie des infractions pour lesquelles le retrait de la plainte préalable de la personne lésée élimine la responsabilité pénale. À cet égard, selon l'art. 226 alinéa (3) du Code de procédure pénale « *L'action pénale est engagée sur plainte préalable de la personne lésée.* »

651. Protection des droits fondamentaux vs lutte contre la criminalité. Cette dynamique met en évidence les préoccupations justifiées du système judiciaire roumain face aux défis posés par l'évolution rapide des technologies numériques, qui ont modifié non seulement le comportement infractionnel, mais aussi la façon dont les droits fondamentaux des citoyens, en particulier le droit à la vie privée, sont protégés. Ainsi, les tribunaux sont confrontés à la nécessité de trouver un équilibre entre la protection des droits fondamentaux de l'individu et la prévention et la sanction des comportements illégaux qui peuvent menacer la vie privée et la sécurité des données personnelles.

La pratique judiciaire roumaine évolue dans une direction où l'application des règles pénales ne reconnaît pas seulement les risques technologiques sur le respect de la vie privée, mais les adapte également en fonction des particularités de l'affaire. Dans un contexte où les technologies émergentes peuvent amplifier les vulnérabilités individuelles, les tribunaux doivent trouver un équilibre entre la protection des droits fondamentaux et la nécessité de lutter contre les délits qui menacent la vie privée.

Pourtant, dans l'analyse de situations factuelles concrètes, l'application et l'interprétation des dispositions légales relatives à l'atteinte à la vie privée présentent des difficultés importantes, qui conduisent inévitablement à diverses controverses et différentes solutions des tribunaux. Ainsi, nous entendons souligner dans les lignes suivantes les principales questions controversées auxquelles sont confrontées les juridictions roumaines dans l'interprétation et l'application des dispositions de l'art. 226 du Code pénal.

B. Les controverses jurisprudentielles relatives au délit d'atteinte à la vie privée

652. Les défis liés à l'accès instantané et illimité à l'information. À une époque où la technologie fait partie intégrante de la vie quotidienne et où l'accès à l'information et aux médias a atteint un niveau sans précédent, la protection de la vie privée devient un sujet d'importance majeure. L'accès rapide et quasi illimité à l'information via Internet, les réseaux sociaux et les appareils connectés posent un certain nombre de dilemmes juridiques et éthiques liés à la confidentialité des données personnelles. Dans ce contexte, « le droit à la vie n'est plus une simple sphère intime de l'individu, mais un droit essentiel, menacé par les nouveaux outils et pratiques numériques »[1675]. Dans ce contexte plutôt dynamique, les décisions des tribunaux

[1675] L'atteinte à la vie privée prévue par l'art. 226 du Code pénal est destinée à combler un vide réglementaire et à apporter une réponse spécifique aux nouvelles formes d'atteinte à la vie privée, elle complète « *le cadre de protection pénale des valeurs garanties par l'article 8 de la Convention européenne des droits de l'homme* », conformément à l'exposé des motifs de la loi no. 286/2009 sur le Code pénal. La loi fondamentale et le Code pénal ne définissent pas la notion de vie intime, familiale et privée, mais dans la jurisprudence de la Cour européenne

ont le rôle de représenter un petit guide de bonnes pratiques concernant l'interprétation des aspects controversés concernant l'infraction prévue par l'art. 226 du Code pénal.

653. Controverses et contestations. L'atteinte à la vie privée est une question largement débattue dans le contexte juridique actuel, avec des implications importantes pour la protection du droit à la vie privée de l'individu. Dans ce sens, l'interprétation et l'application des dispositions légales relatives à l'atteinte à la vie privée, constatées dans la jurisprudence nationale, ont généré de multiples controverses et contestations.

Bien que la loi sur l'atteinte à la vie privée semble claire en théorie, dans la pratique, les tribunaux nationaux ont des difficultés à appliquer uniformément les règlements juridiques, compte tenu de la nature et de la complexité du délit d'atteinte à la vie privée prévu par l'article 226 du Code pénal. Ainsi, dans la jurisprudence nationale, il existe différentes solutions qui reflètent des différences importantes dans l'approche des sanctions appliquées, allant des peines privatives de liberté aux solutions d'acquittement ou même d'arrêt du procès pénal.

Dans ce contexte, cette section vise à analyser les questions controversées rencontrées dans l'interprétation et l'application de la législation sur l'atteinte à la vie privée, de nuancer la manière dont les juridictions roumaines traitent ces situations et d'identifier des solutions possibles pour une meilleure harmonisation de la jurisprudence dans ce domaine.

a). Conditions objectives de réalisation du délit - pratique de la Haute Cour de Cassation

654. La typicité de l'infraction n'est pas conditionnée par le résultat. Dans le contexte de la typicité de l'atteinte à la vie privée, en référence à l'article 226 alinéas (1er) et (5) du Code pénal, une autre question controversée portée à l'attention des tribunaux concerne les conditions objectives pour réaliser le délit. A cet égard, « les tribunaux ont établi que la typicité objective des infractions d'atteinte à la vie privée prévues à l'article 226 alinéas (1er) et (5) du Code pénal n'est pas conditionnelle à l'obtention d'un résultat pour le stockage de la conversation privée sur un support particulier, et il suffit que les moyens techniques d'enregistrement audio soient placés, sans droit pour l'enregistrement d'une conversation privée. »[1676]

---

des droits de l'homme (l'affaire Niemietz c. Allemagne, 1992) il a été décidé que la protection de la vie privée couvre non seulement la sphère intime des relations personnelles, mais aussi « *le droit de l'individu à lier et à développer des relations avec ses semblables* », parce « *qu'il serait trop restrictif de limiter la notion de vie privée à un cercle restreint dans lequel l'individu vit sa vie personnelle comme il le juge bon* ». Par conséquent, au sens de la jurisprudence de la Cour européenne, l'élément déterminant du droit à la vie intime, familiale et privée se réfère à la sphère des relations humaines.

[1676] I.C.C.J, Section pénale, décision *n° 92/A du 1er mars 2023. La typicité objective du délit d'atteinte à la vie privée prévu par l'article 226, paragraphes (1) et (5) du Code pénal n'est pas subordonnée à l'obtention d'un résultat au sens du stockage sur un support donné de la conversation privée, il suffit que le moyen technique d'enregistrement audio soit placé sans droit dans le but d'enregistrer une conversation privée.*

À cet égard, le tribunal de première instance[1677] a établi que l'acte commis par le prévenu[1678] constitue l'infraction d'atteinte à la vie privée prévue à l'article 226 alinéas (1er) et (5) du Code pénal, remplissant certainement les conditions de typicité objective prévues par la loi, dans le sens où cette infraction n'est pas subordonnée à l'obtention d'un résultat, c'est-à-dire au stockage effectif d'une conversation privée sur un support particulier, tel qu'un support magnétique ou optique, mais il suffit que l'appareil d'enregistrement audio soit placé, sans droit, dans la maison, la pièce ou la dépendance de la personne concernée afin d'enregistrer une conversation privée.

655. Écouter un enregistrement antérieur, simple indiscrétion ? À la lumière de la littérature de spécialité, le texte de loi visé à l'alinéa (1er) de l'article 226 du Code pénal criminalise l'écoute d'une personne qui se trouve dans un logement / pièce / dépendance y liée ou d'une conversation avec une autre personne en temps réel, et l'écoute / l'enregistrement devant être effectué par des moyens techniques.[1679] Ainsi, l'écoute avec des moyens techniques d'un enregistrement antérieur d'une conversation ou l'écoute n'est naturellement pas constitutive de délit, puisqu'il n'y a dans ces cas aucune interception active de la conversation en temps réel. Dans ces situations, on ne peut parler que de l'indiscrétion d'une personne, qui ne répond pas aux éléments nécessaires pour constituer le délit d'atteinte à la vie privée.

656. L'enregistrement implique implicitement le stockage. En ce qui concerne « l'enregistrement audio d'une personne dans un logement / pièce / dépendance ou d'une conversation qu'elle porte, il est considéré que cet acte implique le stockage du contenu de la conversation sur un support magnétique ou optique, tel qu'une bande magnétique ou un fichier numérique. »[1680] La doctrine souligne également que les enregistrements audio ne concernent que des conversations privées, c'est-à-dire des discussions tenues dans un cadre privé qui sont censées demeurer confidentielles. Cela exclut, par exemple, « l'enregistrement d'une

---

https://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=202438#highlight=%23%23

[1677] Par la sentence pénale no. 97/F du 29 juillet 2022, prononcée par la Cour d'appel de Galati – Section pénale et pour les affaires impliquant des mineurs, dans *l'affaire no. x/44/2020*, sur la base de l'art. 396 alinéa (6) C. proc. pén. rapporté à l'article 16 alinéa (1er) lettre f) C. proc. pén. et art. 154 alinéa (1er) lettre d) C. pénal avec l'application de la Décision de la Cour constitutionnelle de Roumanie *no. 358 du 26.05.2022*, a été ordonné, entre autres, de mettre fin au procès pénal engagé contre la prévenue A pour avoir commis le délit d'atteinte à la vie privée, prévu par l'article 226 alinéas (1) et (5) du Code pénal, étant donné que la prescription de la responsabilité pénale était intervenue.

[1678] Dans l'acte de notification, il a été noté, entre autres, que le matin du 16 mars 2017, la prévenue A, directrice de la Chambre des comptes, a placé un dispositif d'enregistrement de type magnétophone, décrit et photographié par les personnes lésées concernées, dans le bureau de la personne lésée B, auditeur public externe de la Chambre des comptes, afin d'enregistrer les discussions privées qui avaient lieu à l'intérieur de ce bureau.

[1679] A. Mureşan - *Violarea vieţii private în noul Cod penal*, Caiete de drept penal, nr. 3, 2012. p.78.

[1680] Ibidem.

conversation dans un lieu public où les personnes concernées n'ont pas les mêmes attentes en matière de confidentialité. »[1681]

657. Définition de la conversation privée. De plus, pour que l'acte soit considéré comme un délit, celui-ci doit être commis sans droit. « La conversation désigne une conversation, un dialogue, une discussion entre deux personnes ou plus, pouvant être menée directement entre les auteurs, ou par l'intermédiaire de moyens techniques. La conversation privée a été définie comme une conversation orale à laquelle l'auteur s'attend à ne pas être interceptée par des personnes autres que celle à qui elle est destinée. »[1682]

Dans le même sens, en ce qui concerne l'article 226 alinéa (5) du Code pénal, il est à noter que cet alinéa est important non seulement parce qu'il sanctionne les actes réels d'atteinte à la vie privée (tels que l'écoute ou l'enregistrement de conversations privées), mais aussi parce qu'il concerne les actes de préparation, agissant ainsi comme une intervention proactive du droit pénal.

658. Prémeditation du délit. Ainsi, l'installation a été définie comme étant « la pose, l'installation de moyens techniques d'enregistrement dans le but de photographier, filmer, enregistrer une personne ou capturer ou écouter une conversation privée. »[1683] Ces appareils peuvent comprendre des microphones, des caméras vidéo ou tout autre équipement technique capable de capturer des sons ou des images dans un endroit où la personne pourrait s'attendre à avoir une conversation privée (comme dans la maison, ses dépendances ou tout autre lieu privé). La littérature de spécialité a considéré qu'il est nécessaire que « ces équipements soient fonctionnels, capables de capter des sons ou des images, mais il importe peu qu'ils fonctionnent ou non dans le cas concret ».[1684]

Par conséquent, les dispositions de l'article 226 alinéa (5) du Code pénal n'exigent pas que le but de l'infraction soit effectivement atteint, mais seulement que la mise en place des moyens d'enregistrement ait été faite avec l'intention de commettre une infraction d'atteinte à la vie privée. En d'autres termes, il n'est pas nécessaire que, concrètement, le dispositif technique ait effectivement enregistré une conversation privée ou ait acquis des images ou des sons. Il suffit que « l'appareil ait été placé dans le but d'enregistrer une conversation privée, de sorte que l'acte soit considéré comme objectivement typique. »[1685]

[1681] V. Cioclei*, Drept penal*. *Partea specială I, Infracţiuni contra persoanei şi infracţiuni contra patrimoniului*, Ed. C.H. Beck, Bucureşti, 219, p.228.
[1682] A. Mureşan - *Violarea vieţii private în noul Cod penal*, Caiete de drept penal, nr. 3,2012. p.78.
[1683] N. Neagu, V. Dobrinoiu, I. Pascu, *Noul Cod penal comentat*, ed. a II-a, Ed. Universul Juridic, p.204.
[1684] R. Slăvoiu, *Infracţiunea de violarea vieţii private – O noutate în legislaţia penală din România*, Dreptul, nr. 10, 2013 p.97.
[1685] *Ibidem*.

En question, « le dispositif mis en place par la prévenue était un magnétophone, aspect résultant de la photo prise par les personnes lésées de ce dispositif immédiatement après sa découverte et qui révèle un appareil d'enregistrement audio de type W, corroboré par la déclaration du témoin D. qui a montré qu'il avait vu à deux autres occasions cet appareil utilisé avec la même destination, celle d'enregistrer des conversations dans l'environnement ambiant. »[1686] Le tribunal a conclu que la nature de l'appareil et le but de son emplacement sont prouvés.

659. Clarification des notions de logement, dépendance, pièce par la Cour constitutionnelle. Contre la sentence pénale no. 97/F du 29 juillet 2022 prononcée par la Cour d'appel de Galati – section pénale, la prévenue a exercé son droit de recours et a relevé l'existence d'erreurs graves dans l'établissement de l'état des choses et l'interprétation des dispositions légales, qui a conduit à la formulation des conclusions erronées sur la réalisation des conditions objectives typiques du délit d'atteinte à la vie privée, prévu à l'article 226 alinéas (1er) et (5) du Code pénal. L'appelante soutient que la poursuite pénale et le tribunal ont prolongé indûment l'applicabilité de cet article, ce qui est contraire à la doctrine et à la pratique en la matière. Dans ce contexte, l'appelante renvoie à la décision no. 33/2017 de la Cour constitutionnelle de Roumanie, qui clarifie la portée des notions de « logement », « pièce » et « dépendance », les termes visés à l'article 226 alinéa (1er) du Code pénal.

L'appelante considère que « l'extension artificielle de l'applicabilité des dispositions de l'art. 226 du Code pénal par le procureur n'a pas respecté les limites de la protection prévue par la loi, et le fait de placer un appareil d'enregistrement audio ou vidéo dans le but d'intercepter une conversation privée ne répond pas aux conditions de typicité objective du délit prévues par cet article. L'appelante souligne que, conformément à la décision de la Cour constitutionnelle, la protection de la vie privée ne s'étend pas automatiquement aux lieux publics ou aux lieux qui ne relèvent pas de la définition du « logement » ou de la « pièce privée ».[1687]

660. La Haute Cour confirme la typicité. La Haute Cour rejette les critiques formulées par l'appelante et confirme le bien-fondé de la décision du tribunal compétent. Il est rappelé que le premier tribunal a correctement identifié les éléments typiques du délit d'atteinte à la vie privée, prévu à l'article 226 alinéas (1) et (5) du Code pénal, sur la base de l'opinion dans la doctrine et l'interprétation du texte de loi concernant l'enregistrement audio d'une conversation privée.

661. L'enregistrement n'est pas obligatoire. À cet égard, l'article 226 du Code pénal protège la vie privée d'une personne en garantissant le droit de mener des activités privées sans

[1686] Cour suprême de justice, section pénale, décision n° 92/A du 1er mars 2023. https://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=202438#highlight=%23%23

[1687] *Ibidem*.

être exposée ou interceptée sans son consentement par d'autres personnes. L'art. 226 alinéa (5) réglemente le placement, sans droit, des moyens techniques d'enregistrement audio ou vidéo, afin d'intercepter des conversations privées. La Haute Cour rappelle que l'exigence essentielle de la partie objective est de placer les moyens techniques d'enregistrement audio sans droit aux fins de l'enregistrement d'une conversation privée sans qu'il soit nécessaire que l'enregistrement soit effectivement stocké sur un support.

662. Installation de dispositifs d'enregistrement dans les institutions publiques. En l'espèce, la Haute Cour constate que la prévenue a placé un magnétophone dans le bureau de la personne lésée avec l'intention d'enregistrer une conversation privée entre celle-ci et d'autres personnes. Même si l'activité a été effectuée dans un bureau d'une institution publique, la Cour estime que ce lieu pourrait être considéré comme un lieu où les personnes lésées avaient le droit de protéger la confidentialité de leurs discussions. La conversation était privée parce que les personnes concernées avaient le droit exclusif de décider qui pouvait entendre ou participer à cette discussion.

663. Activités professionnelles protégées par le droit à la vie privée. La Haute Cour rejette également l'idée que les activités professionnelles ne peuvent être protégées par le droit à la vie privée, expliquant qu'il est souvent difficile de faire la distinction entre la vie professionnelle et la vie personnelle. La Cour renvoie à la jurisprudence de la Cour européenne des droits de l'homme, qui souligne que la protection de la vie privée s'applique également aux activités professionnelles (affaire Niemietz c. Allemagne).

Ainsi, il est considéré que « la typicité objective du délit d'atteinte à la vie privée prévue par l'article 226 alinéas (1er) et (5) du Code pénal n'est pas conditionnée par l'obtention d'un résultat aux fins de stockage sur un certain support de la conversation privée, il suffit que les moyens techniques d'enregistrement audio soient placés, sans droit, dans le but d'enregistrer une conversation privée. »[1688]

664. Incrimination de l'acte, quelle que soit sa finalité. Cet aspect souligne un principe important du droit pénal : la protection de la vie privée ne dépend pas de l'achèvement d'un processus technique ou matériel (tel que l'enregistrement réel du son sur un périphérique de stockage), mais sur l'intention et l'action originelles d'intervenir dans une conversation privée par l'utilisation non autorisée d'un moyen technique d'écoute.

Par conséquent, même en « l'absence d'un résultat concret (par exemple sans que l'enregistrement soit sauvegardé ou diffusé), le simple fait de placer un appareil dans l'intention d'enregistrer une conversation privée constitue une violation des règles sur la vie privée, et cela

[1688] *Ibidem*.

constitue un délit en vertu de la législation en vigueur. Ainsi, il est souligné que « la typicité de l'infraction est atteinte au moment de l'action de placer le dispositif d'enregistrement, sans qu'il soit nécessaire que le résultat (l'enregistrement réel de la conversation) soit effectivement obtenu »[1689].

b). Peines en régime de détention uniquement pour les récidivistes et les délits concurrents

665. Situations imposant des peines privatives de liberté. Les décisions de condamnation ordonnées par les tribunaux nationaux ont été appliquées dans des affaires spécifiques où la gravité de l'infraction et les circonstances liées du comportement de la personne qui a commis une infraction pénale ont imposé au tribunal une analyse beaucoup plus sévère. Compte tenu de ces aspects, dans le contexte de la jurisprudence nationale, une peine d'exécution en régime de détention a été prononcée si l'inculpé avait commis une atteinte à la vie privée en concurrence avec une autre infraction portant atteinte aux droits protégés par le droit pénal.

De plus, les tribunaux ont prononcé des peines privatives de liberté lorsque l'accusé a commis le délit d'atteinte à la vie privée dans un état de récidive, en commettant ce délit après une condamnation définitive préexistante. En l'espèce, les juridictions nationales ont considéré que l'imposition d'une peine privative de liberté est nécessaire non seulement pour sanctionner un comportement infractionnel, mais aussi pour décourager la perpétration répétée d'actes.

666. Infractions multiples, durcissement des sanctions. Dans l'analyse des solutions de condamnation avec exécution, un exemple pertinent est la sentence civile no. 662/2021 du 1er octobre 2021 prononcée par le tribunal civil du 3ème arrondissement de Bucarest[1690], qui est demeurée définitive par la décision civile no. 304/2022 du 24 mars 2022 rendue par la Cour d'appel de Bucarest.[1691] La présente affaire porte sur un certain nombre de délits graves, y compris des atteintes à la vie privée, l'agression physique et des violations des mesures de protection imposées par le tribunal. Ainsi, à compter du 22 avril 2021, le prévenu a agi de façon systématique, dans l'intention de surveiller et de contrôler la victime par diverses méthodes illégales, notamment en installant un enregistreur audio et une surveillance GPS dans le sac de la victime et dans son logement.

[1689] *Ibidem*.

[1690] Décision n° 662/2021 du 01.10.2021 rendue par le tribunal du secteur 3 de Bucarest, https://www.rejust.ro/juris/824g6d66e.

[1691] Décision n° 304/2022 du 24 mars 2022, rendue par la Cour d'appel de Bucarest, https://www.rejust.ro/juris/4e9e5g43e.

En parallèle, le prévenu a continué à manifester un comportement violent envers la personne lésée, agressant physiquement la victime, tant à son domicile qu'à sa voiture personnelle, ce qui a entraîné des souffrances physiques. Ce type de comportement s'accompagnait de menaces et d'intimidations constantes, manifestées par des messages agressifs et des photos qui créaient un état de peur à la victime. En outre, le prévenu a violé l'ordonnance de protection émise par le tribunal civil, continuant à contacter la victime via l'application WhatsApp et à la harceler avec des messages, alors que la mesure préventive du contrôle judiciaire dans une autre affaire pénale lui était imposée.

667. Gravité accrue du comportement inapproprié. Compte tenu de ces aspects, le tribunal a noté que « bien que formellement les actes commis par le prévenu ne soient pas graves, les limites de peine prévues par la loi ne sont pas élevées, la façon dont le prévenu a agi leur confère une sévérité accrue. Ainsi, le tribunal tiendra compte du fait que tous les actes du prévenu qui sont circonscrits aux éléments constitutifs des délits pour lesquels il a été envoyé en justice ont été commis dans un délai de 2 mois, avec une fréquence étonnante - le nombre de messages envoyés étant très élevé, le prévenu ne contrôlant pas ses réactions, choisissant de commettre des délits plutôt que de régler de manière légale les différends entre lui et sa concubine, quelle qu'en soit la raison. »[1692]

À cet égard, le tribunal a souligné la gravité du comportement du prévenu qui, malgré les mesures juridiques imposées, a continué d'exercer une pression agressive sur la victime par des messages répétés, des menaces et du harcèlement. Les messages transmis, qui prouvent une obsession dangereuse et un mépris total de toute règle, ont mis en évidence un danger accru, ce comportement ayant un impact considérable sur le psychisme de la victime, générant un risque élevé de récidive.

668. Prouver l'intention et la dangerosité accrue. Par conséquent, le tribunal a conclu que le prévenu avait agi intentionnellement et à plusieurs reprises en violation de la loi, ce qui démontrait un danger accru. Cela s'est traduit non seulement par le grand nombre de délits commis, mais aussi par leur nature, qui impliquent des actes de violence et une violation flagrante de l'intimité de la vie privée de la personne lésée.

Plus précisément, il y a eu atteinte à la vie privée de la personne lésée dans le cas de l'acte du 22 avril 2021, lorsque le prévenu s'est présenté au lieu de travail de la personne lésée situé à Bucarest, et a placé, sans droit, dans son sac, un mini-appareil avec la carte Vodafone, utilisé pour l'enregistrement audio ambiant ainsi que pour le suivi et la localisation du type GPS afin d'écouter les appels émis par celle-ci »[1693] et dans le cas de l'acte du 10 mai 2021 lorsque

[1692] *Ibidem*.
[1693] *Ibidem*.

« en profitant du fait que les personnes lésées n'étaient pas à l'adresse de domicile, il est entré à l'intérieur de l'appartement mentionné et placé sans droit à l'intérieur de la maison, plus précisément dans la chambre de la personne un mini-appareil avec carte Vodafone, qui est utilisé pour l'enregistrement audio ambiant, l'installant dans la prise derrière l'armoire, afin d'écouter les conversations tenues à l'intérieur de l'appartement par les deux personnes lésées. »[1694] Ainsi, le tribunal a considéré que ces actes sont particulièrement graves, la solution consistant à condamner le prévenu à une peine, en régime de détention, assurant une protection correspondant à l'ordre social et au droit à la vie privée de la personne lésée.

Dans toutes ces situations, les condamnations pour l'exécution de la peine privative de liberté reflètent le besoin de répondre de manière claire à la violation du droit à la vie privée, en tenant compte à la fois de son impact sur les victimes et du risque de récidive du prévenu. Ainsi, les tribunaux ont estimé que seule l'application d'une peine privative de liberté peut assurer une protection suffisante du droit à la vie privée de la personne lésée et prévenir des comportements infractionnels répétés.

c). En général, la jurisprudence établit un régime de sanction clément

669. Situations permettant l'exécution de la peine sous surveillance. Cependant, dans certaines affaires, les tribunaux ont considéré qu'une solution de condamnation peut être ordonnée avec sursis de l'exécution de la peine sous surveillance, selon les circonstances spécifiques de chaque affaire, mais aussi certains critères prévus par la loi. La sentence pénale no. 563/2024 du 26 juin 2024 prononcée par le tribunal civil du 1er arrondissement de Bucarest[1695] est un exemple pertinent d'application d'une solution de condamnation avec sursis de l'exécution de la peine sous surveillance, le tribunal considérant que certaines circonstances particulières de l'affaire justifient une mesure plus douce par rapport à la gravité de l'infraction commise par le prévenu. Selon l'acte de renvoi du tribunal, « le 7 novembre 2023, entre 21:00 et 23:00, le prévenu, tandis qu'il se trouvait à l'intérieur de l'appartement no. 7 a photographié la personne sans droit, pendant cette dernière était allongée sur le lit, sans qu'elle donne son consentement, portant atteinte à sa vie privée. Par la suite, entre le 07 novembre 2023, 23:15 - le 08 novembre 2023, 01:38, le prévenu a forcé la personne lésée, en la menaçant par des messages audio-vidéo, mais aussi texte, qu'il enverra la photo prise précédemment sans son

[1694] *Ibidem*.
[1695] Décision n° 563/2024 du 26 juin 2024 rendue par le tribunal de première instance du secteur 1 de Bucarest. https://www.rejust.ro/juris/729gg2557.

consentement à l'ami de la victime, dans le but clair et précis de déterminer qu'elle a des relations sexuelles avec lui. »[1696]

670. L'infraction d'atteinte à la vie privée, aggravée par l'infraction de chantage. Le tribunal a constaté que les faits décrits ci-dessus répondent à tous les éléments constitutifs du délit « d'atteinte à la vie privée » prévu par l'art. 226 alinéa (1er) du Code pénal et de l'infraction de « chantage » prévue et punie par l'art. 207 alinéas (1er) et (2) du Code pénal. Cependant, même si l'auteur a porté atteinte au droit à la liberté de la personne, ainsi qu'à sa vie privée, le tribunal a appliqué une solution de condamnation avec sursis de l'exécution de la peine sous surveillance. En ordonnant cette solution, il a tenu compte du contenu constitutif des infractions imputées au prévenu, considérant que les faits sont de gravité moyenne, dans le contexte de la nécessité de protéger des valeurs sociales particulièrement importantes telles que la liberté psychique et la vie privée de la personne. En faveur du prévenu, il doit retenir son âge, seulement 24 ans, le fait qu'il a un emploi, mais aussi le fait qu'il est bien intégré dans la communauté. »[1697]

Cette solution est un exemple d'application plus souple du droit pénal, auquel cas les tribunaux tiennent compte non seulement de la gravité des délits commis, mais aussi de la situation personnelle du défendeur et des risques liés à un régime de détention.

d). Motivation des jugements d'acquittement prononcés au cours des dix dernières années

671. Décisions d'acquittement. Cependant, dans certains cas, lorsqu'il n'y a pas suffisamment de preuves pour prouver la culpabilité du prévenu ou lorsque l'acte ne répond pas aux éléments constitutifs d'un délit, les tribunaux disposent des solutions d'acquittement. Dans l'analyse des trois jugements dans lesquels les juridictions nationales ont prononcé des solutions d'acquittement en cas d'atteinte à la vie privée, il est essentiel de mettre en évidence les raisons qui ont conduit les juges à émettre ces solutions. Dans la plupart des affaires, les décisions d'acquittement ont été prononcées lorsque les juridictions nationales ont estimé que les actes commis ne relèvent pas de la catégorie des infractions régies par le droit pénal ou dans des situations où elles ont constaté que l'acte n'est pas commis avec la forme de culpabilité prévue par le droit pénal.

672. Analyse minutieuse des éléments constitutifs de l'infraction. À cet égard, dans l'analyse des décisions d'acquittement prononcées dans les affaires d'atteinte à la vie privée, il

[1696] *Ibidem*.
[1697] *Ibidem*.

est important de mentionner la sentence civile no. 1904/2024 prononcée le 19 août 2024 par le Tribunal civil de Iasi[1698]. Dans l'affaire susmentionnée, le tribunal qui a examiné la nature objective du délit, a conclu que l'action du prévenu, « qui avait placé une caméra vidéo dans un bureau de l'Institut de psychiatrie, bureau utilisé par certains des professionnels de la santé pour changer de vêtements, afin de capturer et d'enregistrer des images de ceux-ci »[1699] ne répond pas aux éléments constitutifs du délit d'atteinte à la vie privée, et régis par l'article 226 alinéa (5) du Code pénal, l'acte n'étant pas prévu par le droit pénal.

Afin de parvenir à cette conclusion, le tribunal a pris en compte la décision no. 18 du 22 avril 2024 rendue par la Haute Cour de cassation et de justice dans une décision préalable pour le règlement d'une question de droit établissant « qu'en application des dispositions de l'article 226 alinéa (1er) du Code pénal, les notions de logement, de pièce ou de dépendance au contenu du délit d'atteinte à la vie privée, ont le même sens que les notions de logement, de pièce ou de dépendance au contenu du délit d'atteinte à la vie privée, prévues par l'article 224 alinéa (1er) du Code pénal, étant subsumées à la notion de domicile au sens du droit pénal. »

673. Rappel de la nécessité de clarifier la notion de logement. En prononçant cette solution, la Cour suprême a examiné plusieurs arguments essentiels pour clarifier l'interprétation des notions de « logement », « pièce » et « dépendance » dans le contexte du délit d'atteinte à la vie privée, régi par l'article 226 alinéa (1er) du Code pénal. Un argument solide en faveur de l'interprétation des notions susmentionnées dans le contexte du délit d'atteinte à la vie privée est étayé par l'analyse systématique du Code pénal. Ainsi, la mise en place des infractions réglementées par l'art. 224 du Code pénal, Violation de domicile et art. 226 du Code pénal, Atteinte à la vie privée, au sein du même chapitre du Code pénal conduit à l'assurance unitaire et l'application des mêmes notions, qui ont le sens habituel, dans le contenu constitutif des incriminations alléguées.

L'argument selon lequel les notions de « pièce » et de « logement » doivent être interprétées dans le sens consacré par les règlements du Code pénal, à savoir conformément au délit de violation de domicile prévu à l'article 224 alinéa (1er) du Code pénal, s'appuie sur le principe de la clarté et de la prévisibilité de la loi »[1700]. Selon ce principe, seul le législateur a le pouvoir de définir explicitement les notions et concepts utilisés dans les réglementations pénales, notamment lorsqu'elles peuvent avoir plusieurs significations dans le langage commun.

[1698] Décision n° 1904/2024 du 19 août 2024 rendue par le tribunal de première instance de Iași. https://www.rejust.ro/juris/3983677d7

[1699] *Ibidem*.

[1700] O. Loghin, T. Toader, *Drept penal român. Partea specială*, Ed. Șansa, București, 2001. p.166.

674. Exigences en matière de technique législative. La loi no. 24/2000 sur les normes techniques législatives pour l'élaboration des actes normatifs, à l'article 25, stipule qu'il incombe au législateur de donner une définition précise des concepts lorsqu'il vise à établir un sens différent des termes usuels ou habituels. Ainsi, « en l'absence d'une réglementation claire qui donne un sens distinct aux termes « logement », « pièce » ou « dépendance », ils doivent être compris selon le sens traditionnel, consacré dans le droit pénal, au sein du délit de violation du domicile. »[1701]

Ainsi, selon les dispositions de l'article 16 alinéa (1er) lettre b) de la thèse I du Code de procédure pénale, l'action pénale ne peut être engagée et, une fois qu'elle a été engagée, elle ne peut plus être exercée si l'acte n'est pas prévu par le droit pénal.[1702] Étant donné que les conditions de typicité objective n'étaient pas réunies dans l'affaire pour que l'acte du prévenu constitue une infraction, le tribunal a retenu l'impossibilité de poursuivre à exercer l'action pénale contre le prévenu. À cet égard, « (…) sur la base de l'art. 396 alinéa (5) rapporté à l'art. 16 alinéa (1er) lettre b) thèse I du Code de procédure pénale, le tribunal ordonne l'acquittement du prévenu pour avoir commis le délit d'atteinte à la vie privée prévu par l'art. 226 alinéa (5) du Code pénal, puisque l'acte n'est pas prévu par le droit pénal. »[1703]

675. Analyses jurisprudentielles. À la suite de l'analyse des solutions d'acquittement, une autre affaire d'intérêt dans laquelle le tribunal a constaté que les conditions prévues par la loi pour la rétention du délit d'atteinte à la vie privée ne sont pas remplies est la Sentence civile no. 19/2023 du 31 janvier 2023 prononcée par le Tribunal civil de Pogoanele[1704], qui est demeurée définitive par la Décision civile no. 58/2024 du 16 janvier 2024 émise par la Cour d'appel de Ploieşti.[1705] En l'espèce, sur la base des mêmes résolutions infractionnelles, aux dates des 09 avril 2021, 14 avril 2021 et 1er juillet 2021, le prévenu a envoyé à des tiers des vidéos représentant la victime dans des situations indécentes et tout en maintenant des relations

---

[1701] On retrouve la même interprétation dans les considérants de la Décision de la Cour constitutionnelle de Roumanie *no. 33 du 19 janvier 2017,* publiée au Journal officiel de Roumanie, partie I, no 320 du 4 mai 2017. La Cour constitutionnelle a rejeté l'exception d'inconstitutionnalité dans laquelle l'auteur de l'exception critiquait les dispositions de l'article 226 alinéa (1er) du Code pénal, car elle n'assurerait pas la même protection du droit fondamental et lorsque la violation de la vie intime, familiale et privée se déroule dans des espaces extérieurs à la notion de logement, de pièce ou de dépendance, selon le cas dans des espaces appartenant respectivement au domaine public ou dans lesquels opèrent les institutions ou autorités publiques. En étayant la solution de rejet, la Cour constitutionnelle a constaté que par le règlement contesté l'État ne nie pas le droit de la personne à la vie intime, familiale et privée, mais offre une protection accrue aux faits antisociaux qui affectent ce droit, lorsqu'ils sont commis dans un logement ou une pièce ou une dépendance, c'est-à-dire domicile au sens pénal, dans les autres situations la partie lésée ayant ouvert la voie à une action civile dans le système judiciaire.

[1702] *Ibidem*.

[1703] Décision n° 1904/2024 du 19 août 2024 rendue par le tribunal de première instance de Iași. https://www.rejust.ro/juris/3983677d7

[1704] Décision n° 19/2023 du 31 janvier 2023 rendue par le tribunal de première instance de Pogoanele, https://www.rejust.ro/juris/39g75e34d.

[1705] Décision n° 58/2024 du 16 janvier 2024 rendue par la Cour d'appel de Ploiești, https://www.rejust.ro/juris/ded5g265d.

sexuelles orales et normales, sans son consentement, affectant ainsi la vie privée de la victime, puisque les images sont entrées en possession de plusieurs de ses collègues. Selon les éléments de preuve présentés au cours de l'enquête pénale, le motif de commettre cet acte est la vengeance du prévenu parce que l'appelée ci-dessus a refusé de poursuivre la relation de concubinage avec lui, mais aussi parce que le prévenu est jugé pour avoir commis l'infraction de tentative de meurtre au préjudice du père de la personne lésée. »[1706]

Après l'analyse de toutes les données et preuves administrées au cours du procès, le Tribunal civil de Pogoane a conclu que le prévenu n'avait pas agi avec la forme de culpabilité requise par la loi (avec intention), au moment de la commission des deux actes matériels des 09 avril 2021 et 14 avril 2021, étant remplies les conditions prévues par la loi pour le délit d'atteinte à la vie privée seulement pour l'acte commis par le prévenu en date de 1er juillet 2024.

En ordonnant la solution de l'acquittement pour les deux actes matériels soulignés ci-dessus, le tribunal a pris en compte plusieurs aspects essentiels liés au contenu des vidéos présentées par le prévenu et à la façon dont elles affectaient le droit à la vie privée de la personne lésée.

676. Absence d'identification claire dans les vidéos. Ainsi, le tribunal a conclu que les deux vidéos ne saisissaient pas clairement la physionomie des deux personnes impliquées dans un rapport sexuel. De plus, le tribunal a souligné qu'il n'y avait aucune preuve établissant que le prévenu était celui qui avait filmé ou créé ces vidéos. Ces questions sont contraires à la version de la personne lésée - selon laquelle les deux vidéos ont été faites par le prévenu dans la maison de ses grands-parents, avant le moment où la victime est tombée enceinte. En outre, la version du prévenu (selon laquelle il a téléchargé les vidéos à partir de l'application Telegram) est partiellement étayée par les conclusions de l'informaticien spécialiste, qui a établi un lien entre les vidéos et ladite application. »[1707]

677. Divulgation non autorisée par des personnes autres que l'auteur. À cet égard, afin de répondre aux exigences de l'élément matériel du côté objectif du délit d'atteinte à la vie privée, l'art. 226 alinéa (2) du Code pénal, la loi ne prévoit pas que les enregistrements audio-vidéo doivent être divulgués par la personne qui les a réalisés, ces enregistrements étant accessibles par l'auteur à partir d'autres applications ou reçus par d'autres personnes. Toutefois, pour que le délit d'atteinte à la vie privée ait un caractère subjectif, il est nécessaire que l'auteur prévoie et poursuive ou prévoie et accepte qu'en divulguant les dossiers, il porte atteinte à vie privée de la personne concernée.

[1706] *Ibidem*.
[1707] *Ibidem*.

Ou, dans la présente affaire, le tribunal a conclu que des éléments de preuve administrés ne sortait pas certainement que le prévenu savait au moment de la remise des deux vidéos auprès de la collègue d'emploi de la personne lésée que la personne de sexe féminin enregistrée était la personne lésée, de sorte que « le prévenu n'ait pas prévu que cela nuirait à la vie privée de la personne lésée. » Compte tenu de l'ensemble des aspects exposés ci-dessus, conformément aux dispositions de l'article 396 alinéa 5 CPP, rap. à l'article 16, alinéa 1er, lettre b, thèse II du CPP, le tribunal ordonnera l'acquittement du prévenu pour avoir commis le délit d'atteinte à la vie privée sous une forme continue, prévu à l'article 226 alinéa 3 du CP, avec application de l'art. 35 alinéa 1er du CP (2 actes matériels, des dates du 09 avril 2021 et 14 avril 2021, respectivement la divulgation d'une vidéo au témoin) parce que l'acte n'a pas été commis avec la culpabilité prévue par la loi (avec intention).[1708]

678. La complexité de l'interprétation juridique, des décisions différentes. Au contraire, le tribunal a ordonné la condamnation du prévenu pour le délit d'atteinte à la vie privée, sous forme simple pour l'acte du 1er juillet 2021 dans lequel il a transmis à la collègue d'emploi de la personne lésée un nombre de trois vidéos « l'une dans laquelle la victime était complètement nue et deux dans lesquelles la victime touchait dans la zone intime. » Ainsi, « au moyen de messages téléphoniques portés avec le témoin mentionné, le prévenu lui a fait comprendre que la personne de sexe féminin des enregistrements est son ancienne concubine - la personne lésée et, sachant que le témoin est une collègue avec la personne lésée, le prévenu lui a envoyé pour distribuer les vidéos à d'autres personnes. »

Dans cette situation, le tribunal a jugé que l'acte du prévenu de divulguer au témoin les trois vidéos mentionnées répond à tous les éléments constitutifs du délit d'atteinte à la vie privée, la forme simple, prévue par l'article 226 alinéa (2) du Code pénal.

Toutefois, par la Décision civile no. 58/2024 du 16 janvier 2024 prononcée par la Cour d'appel de Ploiești, l'appel soumis par le bureau du procureur attaché au Tribunal civil de Pogoanele a été admis et a partiellement dissout la sentence civile no. 19/2023 du 31 janvier 2023 prononcée par le Tribunal civil de Pogoanele. À cet égard, de « l'examen du jugement de la première instance, la Cour constate qu'il est dépourvu de fondement en ce qui concerne l'acquittement du prévenu pour le délit d'atteinte à la vie privée (actes matériels des 09 avril 2021 et 14 avril 2021), de la probation administrée résultant la commission d'actes matériels sous forme de culpabilité d'intention directe. »[1709]

[1708] *Ibidem*.
[1709] Décision n° 58/2024 du 16 janvier 2024 rendue par la Cour d'appel de Ploiești. https://www.rejust.ro/juris/ded5g265d.

Dans la motivation de cette décision, la Cour d'appel de Ploiești constate que selon les preuves administrées au cours de l'enquête pénale et pendant la phase d'enquête, le prévenu a transmis à des tiers des images de la victime, sur la base de la même résolution infractionnelle, ayant des relations sexuelles orales et normales, sans avoir le consentement de cette dernière et afin de se venger sur elle. Ainsi, « la culpabilité du prévenu est prouvée, y compris par les procès-verbaux de la fouille informatique et les captures d'écran des conversations Messenger tenues par le prévenu avec des témoins. Sur l'ensemble des éléments de preuve administrés, y compris devant la Cour d'appel, la Cour estime que la culpabilité du prévenu est pleinement établie pour tous les actes matériels de l'infraction prévue à l'article 224 alinéa 1er du Code pénal, en suivant à ordonner la condamnation du prévenu à une peine d'emprisonnement de 1 (un) an pour avoir commis l'infraction prévue par l'art. 226, alinéa 2 du Code pénal, avec l'application de l'article 35, alinéa 1er du Code pénal. »[1710]

À cet égard, on peut noter la complexité de l'interprétation juridique en matière d'atteinte à la vie privée, notamment dans le contexte des preuves numériques et de la motivation infractionnelle. Le jugement de la Cour d'appel de Ploiești souligne l'importance d'une analyse rigoureuse de la probation administrée en question, ainsi que l'application stricte des dispositions légales dans l'évaluation de tous les éléments constitutifs du délit d'atteinte à la vie privée.

679. Clarification de l'interprétation des normes juridiques. Ainsi, les solutions d'acquittement ordonnées par les juridictions nationales en matière d'atteinte à la vie privée sont pertinentes non seulement pour l'application correcte du droit pénal, mais aussi pour mettre en évidence les défis rencontrés dans le domaine de la protection de la vie privée. Dans ce contexte, les décisions de la Haute Cour de cassation et de justice jouent un rôle fondamental pour clarifier l'interprétation des règles juridiques applicables et en même temps pour normaliser la pratique judiciaire. Comme on pouvait facilement le constater, ces décisions ont directement influencé les solutions d'acquittement ordonnées par les juridictions nationales, offrant des repères juridiques importants pour ordonner une solution correcte et légale.

En outre, une interprétation plus détaillée des éléments de preuve recueillis et leur évaluation aussi approfondie que possible peuvent être essentielles pour démontrer la forme de culpabilité avec laquelle le prévenu avait agi. Ainsi, dans les cas où la preuve n'était pas suffisamment concluante pour démontrer l'intention directe du prévenu ou dans les cas où il y a incertitude quant à la finalité des actions du prévenu, les tribunaux ont ordonné une solution d'acquittement.

[1710] *Ibidem*.

Par conséquent, l'analyse de tous ces aspects soulignés ci-dessus est cruciale pour que les tribunaux aient des solutions justes et équitables qui contribuent à la consolidation d'un cadre juridique cohérent et uniforme applicable dans le domaine de la protection de la vie privée. La complexité des cas d'atteinte à la vie privée, surtout dans le contexte dynamique du numérique, exige une approche nuancée, dans laquelle les éléments de preuve sont évalués en détail et les circonstances de chaque affaire sont analysées avec la plus grande rigueur.

e). Sept jugements reportant l'application de la peine en dix ans

680. Les solutions de report, justifiées par l'impact sur les victimes`. Ensuite, pour les sept solutions qui reportent l'application de la peine et d'une solution de renonciation à l'application de la peine, les juridictions nationales ont estimé que les délits d'atteinte à la vie privée commis par les prévenus n'avaient pas d'impact significatif sur les victimes ou sur l'ensemble de la société, et leur gravité a été jugée faible.

Étant donné qu'il n'existe qu'une seule solution au niveau des juridictions nationales pour déroger à l'application de la sanction en cas d'atteinte à la vie privée, le caractère exceptionnel de cette solution est mis en évidence. À cet égard, la Solution civile no. 17/2020 du 24 juin 2020, prononcée par le tribunal d'Intorsura Buzaului[1711], qui est demeurée définitive par la décision civile no. 680/2020 du 23 novembre 2020, prononcée par la Cour d'appel de Brasov[1712], présente un intérêt. Selon l'acte de saisine du tribunal, « le 26 mai 2018 alors qu'elle était à la maison, la prévenue a eu une discussion contradictoire avec son mari, la personne lésée. La prévenue a filmé cette discussion, en étant vue par son mari lorsqu'elle a fait cela, puis l'a publiée sur sa page du site www.facebook.com, cette vidéo étant diffusée publiquement, il était possible d'être visionnée par quiconque y accédait et elle avait le 24 juillet 2018, 103 commentaires, 4 distributions et 2,1 milliers de visualisations ».

681. Éléments constitutifs réunis, mais existence de circonstances atténuantes. En analysant les éléments de preuve présentés dans l'affaire, le Tribunal dans le cadre du Tribunal Civil d'Intorsura Buzaului conclut que l'infraction déduite du jugement a une gravité réduite, compte tenu de la nature et de l'étendue des conséquences, des moyens utilisés, de la manière et des circonstances dans lesquelles elle a été commise, la raison et le but poursuivis et considère que, eu égard à la personne de la prévenue, au comportement antérieurement à la commission

[1711] Décision n° 17/2020 du 24 juin 2020 rendue par le tribunal d'Inţorsura Buzăului https://www.rejust.ro/juris/72ede7726

[1712] Décision n° 680/2020 du 23 novembre 2020 rendue par la Cour d'appel de Braşov https://www.rejust.ro/juris/74gg566e.

du délit, ainsi qu'à ses possibilités de correction, l'application d'une sanction serait inappropriée en raison des conséquences qu'elle aurait sur la personne.

Même si l'acte analysé en l'espèce répond aux éléments constitutifs d'atteinte à la vie privée, prévue et punie par l'art. 226 al. (2) du Code pénal, le tribunal « tiendra compte des circonstances liées à l'acte commis, en ce sens qu'entre la prévenue et la personne lésée - des conjoints - à compter du 26 avril 2018 lorsqu'ils se séparent de corps, il y a eu des désaccords au sujet de la cohabitation et d'autres circonstances liées à la vie familiale que le tribunal considère comme diminuant la gravité de l'infraction et le danger de la prévenue. En ce qui concerne les circonstances personnelles, le tribunal rendra effectif le fait que la prévenue a manifesté de l'intérêt pour sa situation en se présentant devant le tribunal, en substance n'a pas nié l'acte pour lequel elle a été envoyée au tribunal, mais seulement qu'elle a construit devant le tribunal une défense fondée sur l'existence d'un intérêt légitime dans son action pour diffuser l'enregistrement du 26 mai 2018. »[1713]

Ainsi, dans la présente affaire, le tribunal a appliqué une solution de renonciation à l'application de la peine, en tenant compte des circonstances atténuantes et du comportement post-infractionnel de la prévenue. Cette analyse reflète une application proportionnée d'une sanction, tenant compte de la gravité de l'acte mais aussi des possibilités de réhabilitation de la prévenue.

682. Analyse des circonstances atténuantes et du comportement post-infractionnel. Dans les cas où les tribunaux ont ordonné le report de l'application de la peine, une approche similaire peut être observée sur la base de l'analyse des circonstances atténuantes et du comportement post-infractionnel des prévenus. Dans l'analyse des solutions de différenciation de l'application de la peine en cas d'atteinte à la vie privée, il est important de mentionner la Sentence civile no. 1380/2022 du 05 décembre 2022 prononcée par le tribunal de Braila dans laquelle le tribunal a ordonné une solution de différenciation de l'application de la peine.

Selon l'acte de renvoi devant le tribunal, il a été constaté « qu'en juin – juillet 2019, le prévenu a diffusé par l'application informatique facebook messenger tandis qu'il entretenait un acte sexuel oral au cours de février 2019, dans son domicile, une action qui a conduit à la rediffusion de ce matériel pornographique sur le réseau social, devenant public. »

En analysant l'ensemble des éléments de preuve présentés, le Tribunal a conclu que l'acte susmentionné répondait à toutes les caractéristiques essentielles d'un délit. Cela est prévu par le droit pénal comme un délit, est commis avec culpabilité, est injustifié et est imputable au

[1713] *Ibidem*.

prévenu, car il n'y a pas d'incidents dans le cas de l'une des causes limitatives prévues par l'art. 18-31 du Code pénal.

À cet égard, le Tribunal a conclu que l'élément matériel est constitué par la « transmission de messages par le biais de l'application informatique facebook messenger, sans le consentement de la personne lésée, du matériel pornographique dans lequel la personne lésée était présentée pendant un rapport sexuel oral avec le prévenu. »[1714] En outre, afin de motiver cet aspect, le Tribunal retient la Décision no. 51/24.06.2021 prononcée par la Haute Cour de cassation et de justice[1715], dans la formation de jugement pour la suppression des questions juridiques en matière pénale, qui a établi sur une base obligatoire que la typicité d'atteinte à la vie privée, prévue par l'article 226 alinéa (2) du Code pénal, n'est pas conditionnée par l'obtention illégale de matériels (sons, images ou conversations) avant leur divulgation, soulignant que l'élément matériel de l'infraction se rapporte aux actes de divulgation, diffusion, présentation ou transmission sans droit.

683. Approche au cas par cas en fonction des circonstances. Ainsi, le tribunal constate que l'acte déduit au jugement a été prouvé et que la culpabilité du prévenu de l'avoir commis a été prouvée, concluant, au-delà de tout doute raisonnable, que l'acte existe, constitue une infraction et a été commis par le prévenu. Toutefois, compte tenu des circonstances réelles et personnelles du prévenu, le tribunal estime que l'application d'une sanction n'est pas nécessaire, mais il est nécessaire de superviser son comportement pendant une certaine période dans le cadre d'une solution de report d'application de la sanction.

Ces solutions reflètent une approche proportionnée des tribunaux qui, selon les circonstances de chaque cas, ont jugé que des mesures plus atténuées, telles que le report de l'exécution d'une sanction ou la dispense de l'exécution d'une sanction, sont appropriées pour répondre à des délits graves sans compromettre le but préventif du droit pénal.

684. Cessation de la procédure pénale. Ensuite, on peut noter que même des solutions pour la clôture du procès pénal ont été prononcées, celles-ci étant présentes dans les cas où il a été constaté que la personne lésée avait retiré sa plainte préalable formée contre le prévenu.[1716] Ainsi, dans les 5 cas spécifiques où une solution pour la clôture de la procédure pénale a été ordonnée, le retrait de la plainte préalable a conduit à la conclusion de la procédure pénale, soulignant que dans de telles situations, la procédure pénale peut être suspendue lorsqu'il n'y a

---

[1714] *Ibidem*.

[1715] ICCJ, Décision n° 51 du 24 juin 2021, Journal officiel, partie I, n° 1050, 03.11.2021. https://www.iccj.ro/2021/11/04/decizia-nr-51-din-24-iunie-2021/.

[1716] Le délit d'atteinte à la vie privée prévu et puni par l'art. 226 du Code pénal appartient à la catégorie des infractions pour lesquelles le retrait de la plainte préalable de la personne lésée élimine la responsabilité pénale. À cet égard, selon l'art. 226 alinéa (3) du Code de procédure pénale « *L'action pénale est engagée sur plainte préalable de la personne lésée.* »

pas de volonté de la victime de poursuivre la procédure, cette dernière ayant le droit de renoncer à la procédure pénale devant les autorités judiciaires.

f). Retrait de la plainte enlève la nature pénale de l'acte

685. Retrait préalable de la plainte. Un exemple pertinent dans lequel le tribunal a ordonné une solution de clôture de la procédure pénale est la Sentence civile no. 1849/2024 du 31 octobre 2024 prononcée par le Tribunal civil de Deva[1717]. À cet égard, tous les éléments de preuve ont montré que le prévenu avait commis l'infraction d'atteinte à la vie privée prévue à l'article 226 alinéa (2) du Code pénal, puisqu'il a distribué des photographies compromettantes de la personne lésée sans son consentement, en violant ainsi son droit au respect de la vie privée.

Toutefois, au cours de la procédure pénale, il a été constaté que la personne lésée avait exprimé son désir de retirer la plainte antérieure, ce qui élimine la responsabilité pénale de la personne à l'égard de laquelle la plainte a été retirée. Conformément aux dispositions légales, le retrait de la plainte préalable dans ces cas a pour effet de mettre fin à la procédure pénale, étant donné qu'il s'agit d'une condition essentielle pour la poursuite de la procédure pénale. Par conséquent, « compte tenu de la manifestation de la volonté de la personne lésée, au sens du retrait de la plainte pénale soumise dans cette affaire, le tribunal constate l'intervention d'une cause qui empêche l'exercice d'une action pénale pour l'infraction d'atteinte à la vie privée, raison pour laquelle, conformément à l'article 396 alinéa 6 rapporté à l'art. 16 alinéa 1er lettre g) thèse du I C.p.p., le tribunal ordonne la clôture du procès pénal contre le prévenu pour la commission du délit d'atteinte à la vie privée. »[1718]

g). Équilibre entre les intérêts de la victime et le but de la peine

686. Décision proportionnelle aux circonstances de l'infraction. Par conséquent, les solutions ordonnées par les tribunaux nationaux dans les affaires d'atteinte à la vie privée reflètent une application uniforme des dispositions de l'article 226 du Code pénal régissant le délit d'atteinte à la vie privée. Ces solutions reflètent non seulement l'application correcte du droit pénal, mais aussi une évaluation minutieuse des éléments de preuve recueillis au cours de l'enquête judiciaire afin d'aboutir à une décision proportionnée et équitable.

[1717] Décision n° 1849/2024 du 31 octobre 2024 rendue par le tribunal de première instance de Deva. https://www.rejust.ro/juris/98g5738e8.
[1718] *Ibidem*.

D'abord, les tribunaux ont appliqué des peines exécutoires, en régime de détention, dans les cas où ils avaient été prouvés avec certitude et avaient eu un impact significatif sur la victime ou sur la société dans son ensemble. Dans ces cas, les tribunaux ont évalué la façon dont les faits ont été commis et l'impact qu'ils ont eu sur la victime, protégeant essentiellement le droit à la vie privée des individus.

D'autre part, dans les cas de gravité moindre, les tribunaux ont adopté des solutions plus favorables pour le prévenu, telles qu'un report de la sanction ou une solution de dispense de la sanction. Ces solutions ont été ordonnées à la suite d'une analyse détaillée de la situation personnelle des prévenus, qui dans la plupart des cas n'avaient pas de casier judiciaire et présentaient des comportements de réadaptation favorables. Dans ces situations, les tribunaux ont estimé que l'application d'une peine de détention serait disproportionnée à la gravité de l'acte, mais ont plutôt opté pour des mesures moins punitives, mais qui assurerait la surveillance du comportement des prévenus pour une période déterminée.

Un autre aspect important qui a influencé les solutions des tribunaux était l'évaluation minutieuse de la preuve et du côté subjectif du délit d'atteinte à la vie privée. Dans plusieurs cas, les tribunaux ont ordonné des solutions d'acquittement lorsque l'acte n'a pas été commis avec la forme de culpabilité prévue par le droit pénal ou si les délits commis ne remplissaient pas les conditions prévues par la loi, l'acte n'étant pas prévu par le droit pénal. Dans d'autres affaires, cependant, les tribunaux ont appliqué des solutions pour mettre fin à la procédure pénale, en particulier lorsque la victime a retiré sa plainte antérieure.

687. Cadre juridique équilibré. Ainsi, les solutions rendues par les juridictions nationales répondent à la nécessité de protéger le droit à la vie privée de la victime tout en respectant le principe de proportionnalité dans l'application des sanctions. Dans l'ensemble, en ce qui concerne les solutions apportées, les juridictions nationales ont réussi à assurer un cadre judiciaire équilibré reflétant l'application correcte de la législation en matière d'atteinte à la vie privée.

Section 3. VUE COMPARATIVE DE LA RÉGLEMENTATION DU DÉLIT D'ATTEINTE À LA VIE PRIVÉE DANS LE DROIT PÉNAL FRANÇAIS ET ROUMAIN

Le législateur roumain a choisi de criminaliser certains faits qui peuvent sérieusement mettre en danger la vie publique d'une personne en exposant à d'autres personnes certains éléments de la vie privée. La nécessité de criminaliser ces faits découle également de l'existence

d'une curiosité inhérente à toute personne dans des questions qui concernent la vie privée des autres.

688. Soif d'information et exposition publique. Bien que la citation suivante soit de 1996, nous considérons qu'elle est encore aussi actuelle que possible : « La société moderne compte parmi ses caractéristiques, l'immense développement des activités d'information. Je fais un objet de cette soif d'information et de certains aspects de la vie des personnes avec lesquelles le public entre en contact plus souvent (hommes politiques, célébrités, athlètes, etc.), publiant même des détails de la vie privée de ces personnes qui ont réussi à sortir, d'une certaine façon, de la sphère de l'anonymat. Il n'y a pas d'objet inintéressant ou négligeable pour la curiosité humaine, et il n'y a pas d'objet de moralité douteuse auquel la curiosité des hommes puisse résister »[1719].

689. Les limites de l'ancien Code pénal roumain. L'infraction d`atteinte à la vie privée, prévue par les dispositions de l'art. 226 du Code pénal roumain n'a pas de correspondant dans les anciens règlements (Code pénal de 1969). Le législateur roumain n'a pas accordé de protection pénale au droit à la vie privée dans les anciens règlements ou dans des lois spéciales[1720]. Pour cette raison, il n'est pas question d'une application plus favorable de la loi pénale[1721].

690. Augmentation du nouveau Code pénal roumain dans le contexte de la législation européenne. De l`exposition des raisons du nouveau Code pénal[1722], le législateur roumain a établi sur l'infraction visée par cette thèse que « une autre nouvelle incrimination est la violation du secret de la vie privée » (art. 225), « la réglementation nécessaire pour compléter le cadre de la protection pénale des valeurs garanties par l'article 8 de la Convention européenne des droits de l'homme. La réglementation a été conçue de manière à ne pas mettre d'obstacles à l'exercice du rôle de la presse dans une société démocratique et se retrouve correspondant dans la plupart des codes pénaux européens actuels » (art. 226-1 Code pénal français, art. 197 du Code pénal espagnol, art. 192 du Code pénal portugais, art. 615bis du Code pénal italien, art. 179bis-179 quinuis du Code pénal suisse, chapitre 24. section 5-8 du Code pénal finnois, etc.) ».

Il est clair que le législateur a pris en considération la protection des valeurs établies par l'article 8 de la CEDH, qui prévoit le droit au respect de la vie privée et familiale. Dans le même temps, on souhaitait que la façon de réglementer mette des obstacles en place pour les médias.

[1719] D. Pavel, C. Turianu*, Calomnia prin presă*, Casa de editură şi presă Şansa, Bucureşti, 1996. p.10-11

[1720] T. Toader, M.I. Michinici, A. Crișu-Ciocîntă, M. Dunea, R. Răducanu, S. Răduleţu, *Noul Cod penal, Comentarii pe articole,* ed. Hamangiu, București, 2014, p. 387.

[1721] *Idem*, p.388.

[1722] *Exposé des motifs concernant l'élaboration et l'adoption d'un nouveau code pénal, ministère de la Justice*. https://www.avocatnet.ro/articles/download/27594dd98162e6a0f16f508136c53140

Nous croyons que la réglementation de l`infraction est bienvenue et que la vie privée de chaque personne doit être protégée adéquatement, quelles que soient les circonstances.

En ce qui concerne le Code pénal roumain, le législateur a criminalisé cette infraction dans des termes un peu similaires[1723], art. 226 al. (1er) montrant que l'atteinte à la vie privée peut être obtenue « en photographiant, capturant ou enregistrant des images, en écoutant ou en enregistrant le son d'une personne dans un logement ou une pièce ou une dépendance, en ayant une conversation privée. »

691. Clarifications concernant les modalités de violation de la vie privée. Bien qu'ils aient un contenu similaire, il semble à première vue que le texte du législateur roumain est moins synthétique, ayant plusieurs composantes qui couvrent à la fois des éléments juridiques substantiels et des éléments de droit pénal procédural. Pour l'atteinte à la vie privée trois façons sont prévues, selon lesquelles elle est présentée, à savoir : 1) « l`atteinte à la vie privée, sans droit, en photographiant, en capturant ou en enregistrant des images, l'écoute par des moyens techniques ou l'enregistrement audio d'une personne dans un logement ou une pièce ou la dépendance de celle-ci ou d`une conversation privée »; 2) « la divulgation, la diffusion, la présentation ou la transmission, sans droit, des sons, conversations ou images prévus à l`alinéa (1er), à une autre personne ou au public »; 3) « la mise en place, sans droit, des moyens techniques d'enregistrement audio ou vidéo, aux fins de commettre les actes prévus à l`alinéa (1er) et l`alinéa (2) ». Tous ces actes doivent être accomplis sans que l'auteur en ait le droit. Selon l`art. 226 alinéa (2), le Code pénal roumain sanctionne plus sévèrement la divulgation, la présentation ou la transmission, sans droit, à une autre personne ou au public des sons, conversations ou images contenus dans l`alinéa 1er, la peine étant plus lourde lorsque l'acte exercé consiste à placer des moyens techniques d'enregistrement vidéo ou audio, dans le but de commettre l'acte dans les deux premières versions incriminées »[1724].

692. Différences entre le Code pénal français et le Code pénal roumain. Le Code pénal français réglemente l`atteinte à la vie privée à l'art. 226 et stipule qu'il est puni d'un an de prison et d'une amende de 45 000 euros pour atteinte volontaire, par toute procédure, à la vie privée d'une autre personne ». Contrairement au législateur roumain, le législateur français a fusionné les dispositions relatives à l`atteinte à la vie privée avec d'autres dispositions de nature similaire. Ainsi, par exemple, toujours dans le même article, le législateur français a également introduit la violation de domicile ou la falsification d'identité. Pour des raisons de synthèse,

[1723] Il est compréhensible que les délits aient un contenu constitutif similaire, étant donné que le législateur roumain s'est inspiré des codes et de la doctrine française pour rédiger le nouveau Code pénal. Toutefois, nous demandons de façon rhétorique s'il ne s'agissait pas d'une coïncidence lorsque les délits ont été numérotés de la même manière dans les deux codes.

[1724] G. Antoniu, T. Toader, *Explicațiile Noului Cod penal*, Academia Română – Institutul de Cercetări Juridice, Editura Universul Juridic, 2016. p.261.

nous n'entrerons pas dans les détails et nous nous concentrerons sur le délit d'atteinte à la vie privée, tel que réglementé par le Code pénal roumain.

Une différence qu'il vaut la peine de présenter est celle qui concerne la réglementation de la tentative concernant ces délits. Ainsi, si le législateur roumain stipule en général que la tentative est punissable selon l'art. 32 du Code pénal et que les limites des peines sont réduites de moitié, le législateur français a choisi de traiter plus sévèrement l`atteinte à la vie privée et stipule à l'article 226 - 5 que la tentative est sanctionnée par la même peine pour l'acte consommé[1725].

Bien sûr, c'est le choix du législateur de prévoir les limites de la peine en cas de commission de l'acte restant sous la forme de la tentative, mais en lisant tout le Code pénal français, il s'ensuit que ce dernier contient des sanctions plus sévères que celui roumain, parce que, pour la plupart des délits, la même peine est prévue pour la tentative. Toutefois, nous notons que le droit pénal français a une structure différente et établit plusieurs motifs de réduction de peine ou de non-sanction[1726].

693. Sanctions appliquées aux personnes morales. Dans les législations française et roumaine, le sujet actif de l'infraction peut être toute personne qui est pénalement responsable de ses actes et qui met en œuvre le comportement décrit dans le contenu constitutif de l'infraction. Étant donné que le sujet actif est un sujet non circonstancié, il s'ensuit qu'une personne morale peut aussi être un sujet actif du délit d`atteinte à la vie privée, qui est également régi par le droit français[1727].

La participation pénale est possible sous toutes ses formes[1728], l'infraction peut être commise en co-auteurs, instigation et complicité, ce qui est également valable dans le cas de la législation française.

694. Sujet passif : la personne physique dont les intérêts sont lésés. Le contenu du délit dans les deux législations montre que le sujet passif peut être toute personne dont la vie privée a été lésée de la manière décrite par la norme, en termes génériques par l'espionnage visuel et

---

[1725] La tentative des infractions prévues par la présente section est punie des mêmes peines.

[1726] Par exemple, l'art. 222-43 du Code pénal français prévoit que la peine privative de liberté prononcée à l'encontre du délinquant ou du complice des infractions prévues aux articles 222-35 à 222-39 est réduite de moitié si, en avertissant les autorités administratives ou judiciaires, elle a permis de mettre fin à la conduite répréhensible et d'identifier, le cas échéant, les autres coupables. Dans le cas visé à l'article 222-34, la peine de réclusion à perpétuité est réduite à vingt ans.

[1727] Art. 226-7 Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section encourent, outre l'amende suivant les modalités prévues par l'article 131-38 :

- (Abrogé);
- L'interdiction, à titre définitif ou pour une durée de cinq ans au plus, d'exercer directement ou indirectement l'activité professionnelle ou sociale dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise ;

L'affichage ou la diffusion de la décision prononcée, dans les conditions prévues par l'article 131-35.

[1728] T. Toader*, op. cit.,* p.387.

l'espionnage auditif. Afin d'être un sujet passif du délit d`atteinte à la vie privée, la victime ne doit pas connaître les intentions du sujet actif, et si elle les connaît, celle-ci devrait exprimer sa désapprobation que celui-ci continue son activité.

La plupart des controverses concernant le statut de sujet passif dans le délit d'atteinte à la vie privée sont étroitement liées aux éléments constitutifs du délit. Par exemple, une personne qui est espionnée auditivement ou visuellement dans un espace privé, par une personne qui n'a pas le droit de le faire, ne saurait être un sujet passif de l'infraction si la personne qui fait l'objet d'espionnage commet une infraction lorsque l'atteinte à la vie privée est commise par les moyens décrits ci-dessus.

695. Controverse autour de la personne décédée. Un aspect intéressant, apparemment controversé dans la doctrine, est donné par le fait de considérer la personne décédée comme un sujet passif des délits d'atteinte à la vie privée. Aujourd'hui, en France, les choses sont beaucoup plus claires[1729] qu'en Roumanie sur cette question parce que les opinions doctrinales ont déjà été complétées par une jurisprudence claire montrant que la protection de la vie privée doit être accordée de manière similaire à la personne vivante et à la personne décédée[1730]. Dans un autre avis juridique[1731] quelque peu similaire, il est démontré que « la loi vise avant tout à assurer le respect dû à la personne humaine et que la protection qui en découle doit être comprise même au-delà de la mort ». Dans certains aspects de la vie privée, cependant, la conception globale de l'Europe semble légèrement différente. Par exemple, le règlement général sur la protection des données protège strictement les personnes vivantes et non les données privées des personnes décédées.

Étant donné qu'il n'existe pas en Roumanie de bonne pratique judiciaire dans laquelle l'infraction prévue à l'article 226 doit être examinée, les tribunaux ne se prononcent pas concrètement sur la question de savoir si le défunt est considéré comme un sujet passif de l'infraction. De plus, les opinions exprimées dans la doctrine sont lapidaires. Nous considérons que le délit d`atteinte à la vie privée peut concerner la situation dans laquelle un espionnage visuel de la personne décédée est exercé, non seulement en nous référant à la jurisprudence et à la doctrine françaises, mais en analysant le contenu de l'article 74 lettre g du Code civil, texte normatif protégeant la personne décédée en montrant que les images d'une personne sous traitement médical qui décède ultérieurement ou les résultats de son autopsie ne peuvent être diffusées qu'avec l'accord des membres de la famille.

[1729] Chambre criminelle de la Cour de cassation, *20 oct. 1998, bulletin des arrêts nr. 264.*
[1730] V. Malabat, *Droit Pénal spécial*, Dalloz, 7-e édition, 2015. p.336
[1731] M.Véron, *Droit Pénal spécial*, Dalloz, 16-e édition, 2017. p.224. „*La loi entend surtout assurer le respect dû à la personne humaine et la protection qui en découle doit s'entendre au-delà même de la mort*".

Toutefois, nous n'excluons pas la possibilité que le délit d`atteinte à la vie privée ne puisse être commise à l'égard d'une personne décédée, étant donné le contenu du délit d`atteinte à la vie privée, qui est formulée de manière à assurer la vie privée.

696. Inaptitude de la personne morale en matière de vie privée. En ce qui concerne la personne morale, elle ne peut être le sujet passif du délit d`atteinte à la vie privée. Étant donné que cette infraction protège notamment le droit à la vie privée, consacré tant par le droit international que national, « l'objet juridique le constitue les relations sociales dont l'existence et le développement normaux sont conditionnés au respect de la vie privée »[1732].

Dans une autre définition un peu semblable, on a montré que l'objet juridique du délit est « représenté par la vie privée de l'individu et les relations sociales qui naissent et se développent autour de cette valeur »[1733].

697. L'élément matériel du délit d'atteinte à la vie privée. Comme indiqué dans la doctrine spécialisée[1734], le délit d'atteinte à la vie privée n'a pas d'objet matériel parce qu'en réalité les images ou conversations obtenues à la suite de l'intrusion sans droit dans la vie privée sont le résultat de la commission de l`infraction, et les caméras de photographie, de captage ou d'enregistrement sont des biens avec lesquels le délit est commis. La solution est naturelle, parce que l'objet matériel représente cette partie de la réalité physique dans laquelle la valeur sociale protégée par les normes pénales est enchâssée. Toutefois, dans le cas du délit analysé, la vie privée ne peut être incorporée, étant une valeur intrinsèque de l'être humain.

L'élément matériel diffère selon la manière de commettre l'acte, mais aussi selon la forme de l'infraction, principale, dérivée ou connexe. Ainsi, la forme principale de l'infraction prévue par le 226-1 du Code pénal français consiste à capturer, enregistrer ou transmettre, sans le consentement de la personne concernée, les paroles prononcées lors d'une discussion privée ou confidentielle. Au contraire, l'espionnage visuel est réalisé en fixant, enregistrant ou transmettant, sans le consentement de la personne concernée, l'image d'une personne qui se trouve dans un lieu privé[1735].

[1732] *Idem*, p. 261

[1733] M. Udroiu, „*Drept penal. Partea specială. Sinteze și grile*" Ed. C. H. Beck, București, 2014. p.183.

[1734] M. Udroiu, op. cit., p. 185

[1735] Une idée intéressante est exprimée par M. Veron, *Droit pénal spécial*, 14e édition, Sirey, 2012. p.208, qui affirme que les photographies de la princesse Diana, prises à la sortie de l'hôtel ou après l'accident dont elle a été victime, constituent une atteinte à sa vie privée. Cependant, nous nous demandons dans quelle mesure il peut y avoir une atteinte à la vie privée d'une personne décédée, étant donné qu'elle était une personne publique et réputée, et surtout si le sujet passif de l`atteinte à la vie privée peut aussi être une personne autre que la personne concernée. Ainsi, nous croyons que de l'idée mise en question par la doctrine française pourrait conduire à une conclusion novatrice et que l`atteinte à la vie privée pourrait avoir des sujets plus passifs, les conséquences négatives de la divulgation et d'autres formes de commettre le délit se répercutent sur un plus grand nombre de personnes. Par ailleurs, le même auteur rappelle que le législateur français entend avant tout assurer le respect de la personne et la protection doit s'étendre au-delà du décès.

698. Exigences essentielles de typicité. Le Code pénal roumain stipule que « le délit d`atteinte à la vie privée est commise en touchant, sans droit, la vie privée d'une personne physique qui se trouve dans un logement ou une pièce ou une dépendance en tenant compte de celle-ci effectuée par photographie ». La photographie est l'immortalisation d'un moment, et cela doit être préjudiciable à la vie privée. L'infraction subsiste même dans la supposition que la personne prend la photo pour elle-même, ne pas la partageant avec quelqu'un d'autre.

La photographie doit viser exclusivement la personne concernée et cette dernière soit le sujet central de la photographie. Nous croyons que le délit ne subsiste pas si elle est capturée de façon adjacente ou seulement partielle et que l'intention de la personne était de capturer un autre élément[1736]. La même opinion est exprimée dans la doctrine française[1737] où il a été démontré qu'il ne constitue pas le délit d`atteinte à la vie privée si on capture l'image d'un bien tel qu'une maison ou un jardin, le texte du législateur français se référant à l'image d'une personne. Bien sûr, cette hypothèse ne doit pas être considérée comme absolue, chaque cas devant être interprété selon les spécificités de la situation factuelle.

699. Capture, enregistrement, diffusion : actions distinctes. Bien qu'il semble qu'entre ces deux éléments matériels de la capture, respectivement de l'enregistrement, il n'y ait pas de différences, nous montrons que, d'un point de vue technique, la capture équivaut à la collecte d'images mais sans être enregistrées. Ainsi, les deux se différencient par le fait que l'enregistrement des images implique également de les stocker pour pouvoir être offertes plus tard. Une question intéressante concernant la capture d'images est que la doctrine spécialisée a décidé qu'elle ne constitue pas le délit d`atteinte à la vie privée commise par cette voie si l'acte est commis en espionnant une personne à l'aide de jumelles ou par le trou de la serrure.

700. Modification de la responsabilité pénale en fonction du consentement. Il est établi par la pratique judiciaire[1738] que si la personne a d'abord donné son consentement, et ensuite, jusqu'à ce que l'inscription soit terminée, elle demande que l'inscription soit supprimée, l'acte constituera un délit si le sujet actif refuse de se conformer à la demande. L'acte de l`inculpé CNB, qui, au cours du mois de février 2017, a transmis sans le consentement de la personne lésée GSI par l'intermédiaire de l`application WHATSAPP, à l`inculpé DI, un enregistrement audio-vidéo dans lequel il entretenait des relations sexuelles orales et normales avec la personne lésée, répond aux éléments constitutifs du délit « d`atteinte à la vie privée », prévu et puni par l'art. 226 alinéa 2 du Code pénal. L'élément matériel consiste en la transmission sans le

[1736] Par exemple, un immeuble avec de nombreux étages est photographié, l'élément central étant l'immeuble lui-même, et à l'une des fenêtres on constate plus tard qu'une personne a été prise dans une hypostase indécente et préjudiciable à son image.
[1737] P. Conte, *Droit Penal Special*, 6e Edition, Ed. LexisNexis SA, 2019. p.241
[1738] Tribunal Civil de Brasov, Jugement pénal *no. 701 du 18 avril 2018*, définitive.

consentement de la personne lésée GSI, par l'intermédiaire de l`application WHATSAPP, à l`inculpé DI, un enregistrement audio-vidéo dans lequel l`inculpé C entretenait des relations sexuelles orales et normales avec la personne lésée.

Il est évident que l'enregistrement a été effectué avec le consentement de la personne lésée, mais à des fins autres que la présentation publique ou la diffusion à des tiers, ce qui résulte sans aucun doute de l'attitude de la personne lésée après l'enregistrement, consistant dans le fait qu'elle a demandé la suppression de l'enregistrement. La transmission de l'enregistrement était donc sans droit, dans le contexte où il n'y avait pas de consentement de la personne lésée à cet égard, par la façon dont l'inculpé a agi, affectant la vie privée de la personne lésée.

La conséquence immédiate est l'apparition d'un état de danger dû à la violation du droit à l'inviolabilité de la vie privée de la personne lésée, le lien de causalité résultant ex re. L'inculpé a agi avec une intention directe, conformément à l'article 16 alinéa 3 lettre a) du Code pénal.

701. Causes justificatives. Il est démontré dans la littérature française de spécialité qu'il existe également des causes justifiant l'enregistrement d'images avec une personne, ce qui pourrait constituer une ingérence dans la vie privée. Par exemple, il est permis d'enregistrer les contrevenants avec des caméras pour prouver qu'ils ont une vitesse au-dessus de la limite permise ou des personnes qui sont soumises à un processus d'audition par les organes judiciaires[1739].

702. Nuances jurisprudentielles dans l'admissibilité des enregistrements clandestins. En interprétant certaines décisions de la Cour de justice française, il a été conclu que les preuves obtenues illégalement ne devaient pas être exclues par plano des procédures pénales et pourraient être utilisées à condition qu'elles soient sujettes au débat. La raison de cette interprétation de la Cour était qu'il y a parfois des situations (opinion à laquelle on acquiert) où une personne, afin de construire sa propre défense, utilise des images ou des enregistrements qui sont essentiellement une interférence dans la vie privée d'une autre personne[1740].

703. Interpretabilité de la notion d'écoute. L'écoute par des moyens techniques est nécessaire pour examiner les discussions privées ou qui, par leur nature, ne sont pas destinées

[1739] P. Conte, *op. cit*., p.243

[1740] Voir par exemple Cass. crim., 11 fevr. 1992, prec. -Cass. crim., 11 juin 2002: Bull. aim. 2002, n' 131 ; Rev. sc. crim. 2002, p. 879, obs. Renucci. -Cass. crim., 31 janv. 2012, prec. - Les autres chambres de la Cour de cassation jugent irrecevables les preuves obtenues dans de telles conditions : V. par ex., pour un employeur, Cass. soc., 20 nov. 1991: D. 1992, p. 73, cone\. Chauvy. -Cass. soc, 1S mai 2007: D. 2001, somm. p. 3015, obs. Aubert-Monpeyssen. -Comp. Cass. soc., 14 mars 2000: Bull. civ. 2000, V. no 101; JCP G 2001, 10472, note Puigelier (preuve recevable car les salaries etaient informes). -V. aussi, considérant comme une preuve irrecevable, car obtenue de façon déloyale, un enregistrement effectue à l'insu d'une des parties à la conversation, Cass 1. civ, 7 occ. 2004 : Bull. civ. 2004, II, no 447

au grand public. Un exemple de ceci est le placement des microphones pour capturer le son ambiant dans une pièce.

Cette forme de commission du délit donne lieu à une discussion au moins intéressante sur le suivi immédiat du délit. Bien sûr, la plupart du temps, le suivi immédiat, en tant que constituant de l'infraction, ne diffère pas selon les façons de commettre l'acte. La question se pose toutefois de savoir si la notion « d'écoute » doit être interprétée en ce sens que l'information fournie par l'action est intelligible, ou, au contraire, la responsabilité pénale sera engagée indépendamment du fait que l'auteur de l'infraction ne puisse pas percevoir correctement le message qu'il essayait d'obtenir. La différence entre les deux hypothèses est inextricablement liée à la façon dont le sujet particulier de l'infraction est interprété et comment il est atteint ou non par l'infraction. Ou, comme nous l'avons vu, la Cour européenne des droits de l'homme elle-même a montré que la notion de « vie privée » est large et ne comporte pas une définition exacte, donc on peut dire la même chose, sans possibilité d'avoir tort, à propos de la notion « d'atteinte à la vie privée ».

Ainsi, dans une première hypothèse, si nous parlons de l'écoute d'une personne et de la perception totale ou même partielle du message par l'auteur, nous sommes dans une situation claire de commission d'un délit d'atteinte à la vie privée sous forme d'écoute par des moyens techniques. Dans la seconde hypothèse, si l'auteur ne perçoit pas le message sous quelque forme que ce soit pour diverses raisons (affections propres de l'appareil auditif, problèmes techniques liés à l'équipement utilisé, etc.), nous considérons alors que nous sommes en présence d'une tentative parfaite, qui est claire, impunie par le législateur roumain. L'opinion se fonde précisément sur le fait que « l'écoute » est une action active, réalisée dans le but de la perception consciente de l'information qu'elle peut procurer. Étant donné qu'il a été brouillé pour diverses raisons, bien que l'élément matériel du délit subsiste (l'action de l'auteur a été menée jusqu'au bout), il n'y a pas de suivi immédiat, la vie privée de la personne concernée ne subit aucun préjudice réel.

Bien sûr, la discussion reste ouverte, on peut présenter une autre opinion contradictoire possible dans le sens que la simple tentative d'écoute, même en l'absence d'information sur la vie privée de la personne lésée, est susceptible de porter atteinte à ce droit fondamental. Il reste à la jurisprudence de fournir des perspectives claires sur l'interprétation de cette situation juridique.

704. Enregistrement audio, protection de l'image. L'enregistrement audio consiste à capturer uniquement le son dans les conversations ou ce qu'une autre personne dit, sans capturer l'image qui déterminera son identité. Cependant, l'identité de la personne doit émerger de la nature, de l'objet et du message de l'enregistrement. Si plus d'une personne apparaît dans

l'enregistrement et que l'intention de l'auteur était de porter atteinte à la vie privée de plusieurs personnes, il sera alors possible de retenir l'existence d'un concours d'infractions.

705. Situation des enregistrements environnementaux. Étant donné l'ère de la technologie dans laquelle nous vivons, de plus en plus d'employeurs installent des caméras de surveillance à côté des microphones pour enregistrer les actions et ce dont les employés discutent au travail. Ainsi, nous montrons que le droit à la vie privée est également défendu au travail, et si l'employeur monte des caméras ou des microphones sans porter cela à l'attention des employés et qui veut évidemment capturer les actions et ce dont les employés parlent au travail, alors l'acte sera typique. D'autre part, l'acte ne sera pas typique si ceux-ci sont exposés et que les employés sont informés de leur existence.

706. Divulgation des interceptions : circonstance aggravante. Ensuite, nous nous concentrerons sur la divulgation, la diffusion, la présentation ou la transmission, sans droit, des sons, conversations ou images obtenus par l'atteinte de la vie privée dans les formes décrites ci-dessus, à une autre personne ou au public.

Il s'agit de la forme aggravée de l'acte typique et exige qu'en plus des éléments indiqués dans l'explication de l'alinéa (1er), ils soient divulgués, diffusés ou transmis à une autre personne ou au public. Dans toutes les hypothèses mentionnées ci-dessus, l'acte n'est pas typique s'il est autorisé ou permis par la loi, par exemple, le juge des droits et libertés permet d'écouter les conversations d'une personne à la suite d'une supervision technique. Ainsi, pour que l'hypothèse de l'alinéa (2) de l'article 226 puisse s'appliquer, il est nécessaire que les faits visés à l'alinéa (1er) de l'infraction affectent la vie privée de la personne, sans droit.

707. Définition de la divulgation. La divulgation implique une révélation, une divulgation à une autre personne qui n'avait pas connaissance de l'élément présenté. On se demande si le délit existe si la personne à qui l'acte susceptible de porter atteinte à la vie privée était déjà au courant de cet élément.

Nous considérons que si l'atteinte à la vie privée a déjà eu lieu à l'égard d'un événement particulier, la divulgation subséquente du même événement par une autre personne peut ne plus constituer un délit étant donné que le fait divulgué n'est plus nouveau. Nous considérons en ce sens que le caractère de nouveauté de la divulgation entraîne l'atteinte à la vie privée précisément parce que, en son absence, on ne peut plus parler de vie privée, mais de vie publique. En d'autres termes, les tiers connaissent déjà ces aspects qui sont sortis de la sphère privée. Cependant, dans cette hypothèse nous considérons que l'acte ne peut plus être typique, puisque la divulgation, avec les autres modalités de l'élément matériel, par leur essence doit présenter des éléments nouveaux et inconnus. Les circonstances, les situations ou tout fait qui

devient de notoriété publique ne peuvent affecter la vie privée qu'une seule fois, la reprise subséquente de ces éléments n'ayant pas plus la même intensité et la capacité de nuire à la vie privée.

708. De la divulgation à la diffusion. La diffusion consiste à vendre ou à diffuser des images ou des sons, et la présentation fait référence à leur exposition sur des appareils capables à les offrir (via un moniteur ou un panneau par vidéoprojection). La transmission consiste en la mise à disposition effective des images ou sons respectifs sur tout support (CD, DVD, stick, etc.). Toutes ces modalités doivent être remplies en respectant la condition que le sujet actif agisse sans droit dans la transmission ultérieure à une personne physique ou morale des images ou sons concernés.

La réunion de plusieurs modalités du délit ne constituera pas un concours, mais une seule infraction commise en plusieurs façons. De plus, si le sujet actif commet une atteinte à la vie privée conformément à l'alinéa (1er) et à l'alinéa (2), il y aura un concours d'infractions.

En ce qui concerne les modalités du délit, nous considérons que le législateur roumain a tenté de les définir de manière extensive. Cependant, nous considérons que les limites entre les modalités sont quelque peu difficiles à tracer. Par exemple, nous considérons que la différence entre la diffusion, qui consiste à mettre en circulation pour la vente ces images ou sons; et la transmission, qui est la transmission d'images ou de sons, c'est que le premier se fait à titre onéreux et l'autre à titre gratuit. Nous déduisons cet aspect de la définition donnée par le dictionnaire explicatif de la langue roumaine, qui explique la diffusion par « la mise en vente d'une publication ou diffusion (par mot, presse, etc.) d'idées, nouvelles, etc. » D'autre part, la transmission, à partir de la même source, est définie comme « envoyer ou communiquer quelque chose par l'intermédiaire d'une personne, d'une lettre, etc. »; « porter à l'attention de quelqu'un une chose, un fait »; « communiquer quelque chose à quelqu'un avec l'aide d'un émetteur radio, d'une télévision, d'un télégraphe »; « émettre »; faire en sorte qu'il arrive à un autre, passer d'homme à homme ».

709. Distinctions pénales entre espionnage auditif et visuel : France vs Roumanie. Comme on peut le constater, dans le Code pénal français, le législateur a fait une distinction entre les points 1 et 2. Ainsi, le point 1 se réfère à l'espionnage auditif et le point 2 à l'espionnage visuel, les termes étant séparés et la distinction ne se trouvant qu'aux termes capture et réalisation. De ce point de vue, le législateur français a criminalisé le délit d'une manière plus compréhensible, choisissant de ne pas alourdir le texte avec des hypothèses difficiles à distinguer. Contrairement au législateur français, le législateur roumain a introduit la photographie, la capture, l'enregistrement d'images, l'écoute avec des moyens techniques ou

l'enregistrement audio, la divulgation, la diffusion, la présentation ou la transmission, le placement sans droit de moyens techniques d'enregistrement audio ou vidéo.

En outre, nous ne trouvons pas dans l'ensemble du délit un terme plus approprié et qui est utilisé dans la pratique des tribunaux. Nous y faisons référence à la distribution. La pratique judiciaire est pertinente, car elle montre que le tribunal lui-même n'a pas rigoureusement encadré la manière dont l'inculpé a commis l'infraction : en droit, tout d'abord, le premier tribunal a tenu compte du fait que l'inculpé a commis les deux actes, du 12 janvier 2016 et du 13 au 14 mars 2016, à des intervalles relativement rapprochés, sur la base de la même résolution pénale, chaque acte, en partie, en remplissant le contenu de la même infraction (ayant le même mode d'opération, à savoir la divulgation, sans droit, à d'autres personnes ou au public des mêmes documents relatifs à la vie privée de la personne lésée, des documents qui ont été capturés dans un logement/une pièce).

710. Le tribunal a conclu de l'acte d'accusation que l'acte de l'inculpé avait été commis par divulgation, mais nous croyons qu'en plus de la divulgation, l'hypothèse de transmission doit être retenue, étant donné que l'inculpé a créé plusieurs CD avec des images de nature sexuelle qui affectent la vie privée de la personne lésée et ont été diffusées à travers sa ville, un acte qui s'encadre à la de transmission : « Dans le même temps, il a été pris en compte que le certificat délivré par RATB Titan (soumis par l'inculpé au terme du 26 septembre 2017) montre que le 13 mars 2016 l'inculpé était libre, et le 14 mars 2016 dans l'intervalle de temps 15.00 à 18.00 il a travaillé, aspects qui, corroboré avec les autres moyens de preuve administrés (déclaration des témoins, la personne lésée), confirment, au-dessus de tout doute raisonnable, que l'activité infractionnelle consistant à distribuer des CD contenant des images compromettantes de la personne blessée, dans la zone de I., dép. de B., a été faite dans cette période »[1741].

711. Initiatives législatives visant à interdire la divulgation et la diffusion d'images intimes. Nous signalons qu'au moment de la rédaction de cette thèse, il y a une initiative d'un membre du Sénat qui tend à modifier cet article dans la Commission juridique de la Chambre des députés du Parlement de Roumanie. L'initiative législative vise à combler un vide juridique lié à la pornographie de vengeance, à savoir l'affichage de photos ou de vidéos, à la suite d'une séparation, avec l'ancien partenaire dans des positions indécentes. Nous pensons que l'initiative[1742] est de bon augure, étant donné que chacun a le droit à la vie privée et à vivre chez soi comme il le souhaite et ce droit doit être défendu par le législateur.

[1741] La Décision Pénale *no. 303/A* de l'audience publique du 6 mars 2018 pendant à la Cour d'appel de Bucarest, 2ème Section pénale.

[1742] L'initiative prévoit l'introduction de quatre nouveaux paragraphes avec le contenu suivant :

1. « *Divulgation, diffusion, présentation ou transmission d'une image intime d'une personne identifiée ou identifiable par les renseignements fournis, sans le consentement de la personne représentée, susceptible de lui*

712. Installation de dispositifs d'enregistrement : forme autonome, plus grave encore que la transmission d'images. L'alinéa (5) du délit d'atteinte à la vie privée[1743] criminalise les actes préparatoires à l'infraction visée à l'article 226 alinéas (1) et (2). De la rédaction du dernier alinéa, il s'ensuit que le législateur voulait punir les actes qui peuvent être considérés antérieurs la commission de l'infraction, n'étant pas nécessaire que l'infraction soit effectuée selon l'article 226 alinéas (1) et (2), étant donc une infraction en soi. Nous attirons l'attention sur le fait que le législateur a choisi de criminaliser la mise en place (qui représenterait en réalité l'installation) de moyens techniques d'enregistrement audio ou vidéo, plus grave que la violation même de la vie privée par la divulgation ou la transmission d'images.

Nous ne comprenons pas la raison d'opter pour une telle formulation, compte tenu que l'alinéa (5) de l'art. 226 du Code pénal roumain prévoit un délit en soi et il n'est plus nécessaire de remplir les conditions des alinéas (1) et (2). Cependant, la finalité, en réalité, est bien pire dans les alinéas (1) et (2) que le simple placement des moyens de supervision technique, parce qu'aux alinéas (1) et (2) le sujet passif subit une atteinte majeure à sa vie privée.

Ainsi, dans cette perspective, l`alinéa (5) prévoit la peine la plus sévère, et l'acte peut être commis même sans porter atteinte à la vie privée parce qu'il est incriminé comme un délit en soi et ne se rapporte pas aux alinéas (1) et (2) sauf dans la mesure où le but de commettre l'élément important décrit dans ces alinéas est commis.

713. Dans ces circonstances, il ne ressort pas du libellé du texte que l'objectif de la commission doit être atteint, mais nous considérons que seul le libellé était équivoque et que la volonté du législateur était en réalité d'incriminer une forme aggravée des alinéas (1) et (2) que lorsque l`atteinte à la vie privée est commise en mettant, sans droit, des moyens d'enregistrement audio ou vidéo, alors elle doit être punie plus sévèrement[1744]. En outre, le placement de tels moyens représente un degré de danger plus grand que l'élément matériel décrit dans les alinéas mentionnés ci-dessus.

---

causer de la détresse mentale ou le préjudice de son image, est puni d'un emprisonnement de trois mois à deux ans ou d'une amende »

2. « L'action pénale est engagée sur plainte préalable de la personne lésée »;

3. « Image intime désigne toute reproduction, sur quelque support que ce soit, de l'image d'une personne nue qui expose totalement ou partiellement ses parties génitales, son anus ou sa zone pubienne ou, dans le cas des femmes, ses seins, ou qui est impliquée dans une relation sexuelle ou un acte sexuel »;

4. « *L'acte commis ne constitue pas une infraction :*

a) s'il était nécessaire de prévenir, de capturer ou de prouver la commission d'une infraction ;

b) si elle a été autorisée, dans des cas dûment justifiés, par un organe judiciaire au cours d'une procédure judiciaire »

[1743] Le placement, sans droit, des moyens techniques d'enregistrement audio ou vidéo, afin de commettre l'atteinte à la vie privée en conditions de l'art. 226 alinéas (1) et (2).

[1744] La même opinion sur l`alinéa (5) du délit d`atteinte à la vie privée peut être trouvée à M. Udroiu, *Drept penal. Partea specială*, 3e édition, révisée et ajoutée, Editura C.H. Bech, București, 2016. p.205.

714. Espionnage via le système GPS. Il est intéressant de noter que même si nous avons un règlement relativement nouveau qui est censé avoir pris en compte la technologie actuelle, le délit d`atteinte à la vie privée ne comprend pas le moyen controversé mais fréquemment utilisé de suivre les personnes par le système GPS.

Si un système de surveillance GPS est installé sur la voiture de la personne lésée, bien qu'il représente une interférence dans sa vie privée, ayant à sa disposition des informations sur les lieux qu'elle fréquente et où elle se trouve à tout moment, le délit d`atteinte à la vie privée n'existe pas parce qu'il n'y a pas de moyens prévus par la loi sur l'image ou le son. Toutefois, la surveillance GPS d'une personne répond aux conditions de l'infraction prévue à l'article 26 alinéa (1er) rapporté à l'article 14 alinéa (2) lettre e) de la loi no. 51/1991 sur la sécurité nationale de la Roumanie[1745].

715. Facilité d'acquisition des dispositifs d'espionnage. Nous considérons que, par rapport aux moyens technologiques actuels, le délit lié à la sécurité nationale de la Roumanie n'est plus justifié, étant donné que cette loi date de 1991 et qu'actuellement des dispositifs de suivi de ce type peuvent être achetés par toute personne à des prix abordables. Nous pensons qu'un tel acte constitue également une ingérence dans la vie privée de la personne et que les dispositions de la règle qui fait l'objet de cette thèse devraient être complétées par une telle modalité de commettre l'acte.

716. Irrélevance de l'atteinte au résultat pour la retenue de l'infraction. D'après le libellé du texte, il n'est pas nécessaire que l'objectif visé (des images ou des conversations soient capturées et divulguées, présentées, transmises, etc.) soit atteint aux fins de la retenue du délit. Cependant, si le placement et l'objectif pour lesquels les moyens techniques ont été placés sont remplis, il y aura une concurrence d'infractions entre l'acte prévue à l'art. 226, alinéas (1) ou (2), et l`acte prévu à l'art. 226, alinéa (5).

717. Cas particuliers justifiés où la captation/diffusion ne constitue pas une infraction. Comme pour les autres moyens présentés, l'acte manquera de typicité si le placement de

[1745] En 2017, un tel cas a été rapporté dans la presse, dans lequel l`inculpé, en colère contre le fait que sa petite amie l'ait quitté, a monté sur sa voiture un dispositif de suivi GPS acheté sur des sites publics à vendre au prix de 150 lei. Pour cet acte, il a été mis en justice par les procureurs de la DIICOT au regard des dispositions de l'article 14 alinéa (2) lettre e) de la loi 51/1991 qui prévoient (2) les activités spécifiques prévues à l'alinéa (1) peuvent consister en : e) la localisation, le suivi et l'obtention d'informations au moyen du GPS ou d'autres moyens techniques de surveillance; et les dispositions de l'article 26 alinéa (1) qui prévoient que l'exercice, sans autorisation, des activités propres à la collecte de renseignements soumis à autorisation en vertu de la présente loi ou au dépassement de l'autorisation accordée est punissable d'une peine d'emprisonnement de 2 à 7 ans, si l'acte ne constitue pas une infraction plus grave. La personne en question a été condamnée à un an avec sursis à l'exécution de la peine par la Cour d'appel de Ploieşti, mais acquittée par la Haute Cour de cassation et de justice. Voir sentence pénale *no. 128/2017* sur le rôle de la Cour d'appel de Ploiesti et la décision de la Haute Cour de cassation et de justice *no. 18/2018* dans l'affaire *no. 363/42/2017*.

moyens techniques audio ou vidéo est autorisé par la loi. Par exemple, si le juge des droits et libertés autorise, conformément à la loi, le placement de tels moyens.

L`alinéa 4 de l'article 226 du Code pénal roumain prévoit trois cas dans lesquels le sujet actif n'est pas puni.

Le législateur roumain a prévu le cas de non-punition dans l'hypothèse où le sujet actif du délit aurait participé à la rencontre avec la personne lésée au cours de laquelle les éléments susceptibles d'entraîner l`atteinte à la vie privée auraient été saisis, mais seulement s'il justifie un intérêt légitime[1746]. Ainsi, « ne constitue pas un délit l'acte commis par la personne qui a participé à la rencontre avec la personne blessée au cours de laquelle les sons, conversations ou images ont été capturés, s'il justifie un intérêt légitime ».

Nous croyons qu'il peut y avoir un intérêt légitime lorsque des faits sont discutés dans le cadre de discussions privées ou lorsqu'on fait des déclarations qui pourraient être pertinentes dans un procès civil ou pénal et qui pourraient être utilisées comme éléments de preuve. Par exemple, on pourrait enregistrer une personne qui ne fait que des déclarations à moitié vraies, et plus tard les autres déclarations soient révélées par un interrogatoire corroboré avec l'enregistrement de l`origine.

718. La notion de consentement présumé. Le législateur français n'a pas prévu une telle hypothèse pour conduire à la suppression de l'infraction[1747], mais il a prévu à la fin de l'article 226 que si les actes visés dans cet article ont été accomplis en pleine vue et avec la connaissance des intéressés sans qu'ils s'y opposent, lorsqu'ils étaient en mesure de le faire, leur consentement est présumé »[1748].En d'autres termes, si une personne opère publiquement en France, le législateur a institué une présomption absolue concernant le consentement de la personne lésée.

Par exemple, si une personne fait des divulgations intimes qui la concernent, dans un train plein de voyageurs, il est présumé qu'elle a donné son consentement pour que ces questions deviennent publiques. Aussi, une fois que ces divulgations acquièrent le caractère public, dépassant la limite du privé et de l'intime, alors il est permis par le législateur que ces

[1746] Nous mentionnons que même dans le règlement actuel, l'intérêt légitime n'a pas été défini avec précision et il est nécessaire de se référer à la loi 554/2004 du contentieux administratif, où, dans l'art. 2 lettres p) et r) il est stipulé que p) l'intérêt légitime privé - la possibilité de revendiquer une certaine conduite, en considérant la réalisation d'un droit subjectif futur et prévisible; r) l'intérêt légitime public - l'intérêt de la primauté du droit et de la démocratie constitutionnelle, la garantie des droits fondamentaux, des libertés et des devoirs des citoyens, la satisfaction des besoins de la communauté, la réalisation de la compétence des pouvoirs publics;

[1747] Il doit montrer que le législateur français a adopté un style différent concernant la politique pénale et n`a prévu qu`à certains chapitres des dispositions comme Toute personne qui a tenté de commettre l'une des infractions prévues par les articles 411-2, 411-3, 411-6, 411-9 et 412-1 sera exempte de peine si, ayant averti l'autorité administrative ou judiciaire, elle a permis d'éviter que l'infraction ne se réalise et d'identifier, le cas échéant, les autres coupables.

[1748] Art. 226-1 „*Lorsque les actes mentionnés au présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en meure de le faire, le consentement de ceux-ci est présumé*"

questions puissent être enregistrées et transmises ultérieurement, toutes fondées sur le consentement présumé de la personne qui fait les divulgations[1749].

719. La rétention du délit, donnée par l'intention de la personne lésée d'être entendue/vue. On peut dire que le législateur roumain s'est inspiré du Code pénal français et a institué un cas de suppression de la typicité de l'acte dans le cas où la victime aurait agi (en transmettant des informations relatives à sa vie privée) avec l'intention d'être vue ou entendue. En tant que tel, l'hypothèse de la législation française a été établie, un exemple de consentement présumé[1750] existant également dans la législation roumaine - il ne constitue pas un délit si la personne lésée a agi explicitement avec l'intention d'être vue ou entendue par l'auteur.

Nous pensons qu'il doit y avoir une intention sans équivoque de la personne lésée de ne pas être entendue ou vue par l'auteur[1751]. Il peut être prouvé qu'en réalité la personne lésée a été surprise par le sujet actif, mais elle ne voulait pas clairement cela, mais seul l'auteur a interprété les actes de la personne lésée de manière à considérer que celle-ci agit dans l'intention d'être vue. Par exemple, la personne lésée est complètement nue dans sa propre maison, avec des rideaux tirés, mais ils sont légèrement transparents. Le sujet actif du délit l'enregistre en croyant qu'elle aime être regardée par d'autres personnes. En réalité, la personne lésée se considérait défendue par les rideaux et ne savait pas qu'on pouvait voir à travers eux, donc il n'y avait pas de consentement présumé qu'elle aimerait ou permettrait à une autre personne de l'enregistrer dans des situations intimes.

720. Surprise ou preuve d'une infraction. Pour des raisons de prévention, le législateur roumain a prévu qu'il ne constitue pas une violation de l'hypothèse de la vie privée dans laquelle la commission d'un délit est prise ou contribue à prouver la commission d'un délit. Ainsi, la première thèse est pleinement applicable, en ce sens qu'il n'y a pas de situation où la surprise de commettre un délit représente la commission du délit d'atteinte à la vie privée.

Cependant, nous croyons que cela pourrait soulever des problèmes en utilisant le terme d`infraction. Ainsi, d'autres éléments extrinsèques qui n'appartiennent pas à la personne effectuant l'inscription entreront dans l'équation. Par exemple, le législateur a introduit la notion d'infraction, ce qui signifie que la personne prise en train de commettre un acte prévu par le droit pénal doit être définitivement reconnue coupable d'avoir commis l'infraction, c'est-

[1749] Nous attirons l'attention sur le fait qu'il s'agit de questions qui concernent la vie privée de la personne concernée et non celle d'une autre personne.
[1750] Nous envoyons également à *l`art. 22 du Code pénal roumain* qui nomme une cause justificative.
[1751] Il est intéressant de noter que le législateur roumain a préservé certains archaïsmes de l'ancienne procédure pénale. À l'heure actuelle, le terme auteur est rarement utilisé dans le Code et nous pensons qu'il ne s'agit que d'une échappatoire du législateur roumain. Dans le nouveau Code de procédure pénale, la peine de l'auteur ne s'applique pas parce que la poursuite commence in rem et plus tard in personam lorsque l'auteur devient un suspect. Cependant, nous n'avons pas vraiment un auteur, même si nous capturons la personne en flagrant délit, il sera entendu en tant que témoin et non en tant qu'auteur.

à-dire d'avoir accompli tous les éléments de l`infraction. On sait que l'établissement de la circonstance qu'une personne a commis ou non une infraction est le privilège du juge, qui décide par une décision qui doit être définitive. Cependant, il est très probable que la personne qui fait l'enregistrement n'a pas de connaissances spécialisées dans le domaine juridique et ne soupçonne que ce qu'elle enregistre est un délit possible. Cela peut conduire à une situation dans laquelle l'affaire se finira par une solution de classification, la renonciation à des poursuites pénales, un acquittement ou même la clôture d'une procédure pénale, et pour la personne qui a fait l'enregistrement commencer l'enquête pénale pour avoir commis le délit d`atteinte à la vie privée.

Bien sûr, la situation est une hypothèse rare, mais un seul cas suffit pour qu'une telle situation injuste se produise et que la liberté d'une personne soit restreinte.

721. Justification de la divulgation. Ce n'est pas un délit le fait de saisir des questions d'intérêt public qui sont importantes pour la vie de la collectivité et dont la divulgation a plus d'avantages publics que le préjudice causé à la personne lésée. Cette cause de non-punition est une nouveauté apportée par le législateur roumain. Nous sommes toutefois conscients que le libellé est générique et qu'il doit être interprété avec prudence par les instances judiciaires. Par exemple, le législateur a choisi d'introduire l'expression de faits qui ont une signification pour la vie de la communauté, ce qui est nouveau et un peu difficile à interpréter. Cette situation doit donc être analysée concrètement au cas par cas.

722. Interprétation correcte du terme « avantage communautaire ». D'abord, on peut se demander quel degré de signification l'acte d'intérêt public doit présenter, en continuant à déterminer le point de vue de quelle personne il faut faire l'appréciation et qui est le système de référence en termes d'intérêt public et de vie communautaire. Nous considérons que l'acte doit susciter l'intérêt d'une communauté élargie et d'un nombre considérable de personnes. Ainsi, moins la communauté est nombreuse, plus l'incidence de la cause de non-punition est faible. Nous croyons aussi qu'à la lumière de l'intérêt public, il faut examiner une loi qui est d'une grande importance pour la communauté et qui susciterait l'intérêt de toute personne qui fait partie de cette communauté.

Par exemple, nous croyons qu'un tel acte pourrait exister dans l'hypothèse où le maire d'une ville, lors d'une fête privée avec ses amis proches, révèle qu'il a utilisé une partie des fonds alloués au développement de la localité pour son propre intérêt. D'autre part, nous considérons qu'il n'est pas important et qu'il ne constitue pas un acte d'intérêt public la divulgation par le même maire au cours du même événement privé qu'il avait des relations extraconjugales. Cet aspect est étroitement lié à la vie privée, peu importe sa qualité de maire ou autre personne publique.

723. Introduction dans la législation du terme « avantage public ». Le législateur a également introduit la notion d'avantage public. Il est difficile de quantifier et d'apprécier. L'avantage public pourrait être défini comme le gain que la communauté a en relation avec l'intrusion dans la vie privée de la personne lésée. Il s'agit d'une situation délicate dans laquelle un organe judiciaire devra trouver un équilibre entre l'intérêt de la collectivité et l'avantage que procurent l'intrusion et la vie privée de la personne.

Cependant, si nous ne regardons que cette dernière cause de non-punition, il y a des termes qui présentent une nouveauté dans le texte pénal roumain, tels que : signification – vie communautaire – avantage public.

§1. RÉGLEMENTATION DU DÉLIT D'ATTEINTE À LA VIE PRIVÉE EN CONTEXTE EUROPÉEN

724. Préoccupations européennes concernant la protection de la vie privée. À l'heure actuelle, la plupart des États européens sont très préoccupés par la nécessité de trouver les instruments législatifs appropriés pour protéger le plus efficacement possible la vie privée. D'après l'analyse réalisée jusqu'à présent, c'est en Allemagne que l'innovation semble la plus importante dans ce domaine. La manière dont sont protégées les données intimes des citoyens, l'intrusion agressive des réseaux sociaux dans la vie privée des utilisateurs, ont suscité des réactions législatives assez controversées au niveau européen[1752]. Le Code pénal allemand réglemente notamment « l'espionnage informatique » (section 202b) ainsi que d'autres atteintes à la vie privée (section 202a). Les délits « de violation de l`intimité des conversations » (article 201), « l`atteinte à la vie privée en prenant des photos » (article 201a) et « le délit de violation du secret des écrits » (section 202) sont également criminalisées. Le législateur allemand a accordé une attention particulière à l'amélioration de la protection de la vie privée lors de la prise de photos précisément dans le contexte de la numérisation et de l'évolution technologique, dernière modification du Code pénal concernant l'infraction même qui fait l'objet de cette recherche, entrée en vigueur le 1er janvier 2021[1753].

[1752] A. Toor, *Germany passes controversial law to fine Facebook over hate speech*, The Verge, 2017. https://www.theverge.com/2017/6/30/15898386/germany-facebook-hate-speech-law-passed

[1753] Code pénal allemand, 201a StGB – Violation de l'espace intime extrêmement personnel et des droits de la personnalité par la réalisation d'enregistrements, 2004. StGB est le code pénal allemand. Le paragraphe 201a protège l'intimité et la dignité des personnes contre la photographie ou le tournage non autorisés. Il a été introduit en 2004 afin de lutter contre la surveillance et la prise de photos à l'insu des personnes concernées. En 2015, à la suite du scandale Edathy, la diffusion de contenus dégradants ou mettant en scène des mineurs a également été incluse dans la liste des infractions. Actuellement, la norme englobe également la protection des personnes décédées. https://dejure.org/gesetze/StGB/201a.html

Le législateur italien a criminalisé l'acte d`atteinte à la vie privée par les dispositions de l'article 615 bis, dans une formule similaire à celle du Code pénal roumain[1754]. Par rapport à l'infraction type prévue par l'article 226 de la législation roumaine, le Code pénal italien prévoyait une peine allant de six mois à quatre mois d'emprisonnement, étant punie jusqu'à cinq ans d'emprisonnement pour l'acte de l`agent public qui commet un tel délit[1755].

Dans le système juridique anglo-saxon, la protection de la vie privée bénéficie d'une réglementation développée. Dans ce cas, nous parlons du Royaume-Uni, qui à son tour a connu une augmentation de la criminalité dans ce domaine. Le principal outil normatif est le Code de pratiques dans le domaine de la réglementation des faits affectant la vie intime de la personne (2000, révisé et mis à jour en 2008)[1756].

Le droit pénal espagnol a institué les premières mesures de protection de la vie privée depuis 1995, après que l'article 18 de la constitution espagnole[1757] ait reconnu le droit à la vie privée comme un droit fondamental. L`Art. 197.1 du Code pénal espagnol punit quiconque confisque des lettres, des messages ou d'autres documents ou intercepte des communications afin de découvrir des secrets ou de violer l`intimité de la victime sans son consentement[1758]. La législation et les opinions doctrinales en Espagne parlent de l'interdiction de révéler les secrets d'une autre personne[1759]. Évidemment, le simple recours à des moyens techniques pour l'espionnage audiovisuel est puni. La peine maximale est de quatre ans d'emprisonnement. En même temps, la situation dans laquelle l`auteur de l`infraction est responsable de l'enregistrement ou du support informatique est aggravante, lorsque les secrets découverts affectent des données sur la religion, la santé, l'origine raciale ou la vie sexuelle, lorsque les secrets concernent des mineurs ou des personnes handicapées ou lorsque le but infractionnel est d'obtenir un profit financier.

[1754] I. Vasiliu, G. Antoniu, T. Toader, *Explicațiile Noului Cod penal*, Universul Juridic, Bucarest, 2015, p.267.
[1755] *Le code pénal italien, art. 615-bis, sanctionne toute intrusion non autorisée dans la vie privée, telle que la capture ou l'utilisation d'images ou de sons*. https://officeadvice.it/codice-penale/articolo-615-bis/
[1756] *Ibidem*
[1757] *Constitution espagnole de 1978, dernière mise à jour en 2024*. https://www.boe.es/buscar/act.php?id=BOE-A-1978-31229
[1758] Constitution espagnole de 1978, dernière mise à jour en 2024 Version consolidée de la Constitution espagnole, par la « Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal », loi adoptant le Code pénal espagnol. Le Code pénal de 1995 a remplacé l'ancien Code pénal de 1973, adaptant la législation aux exigences de l'État de droit démocratique. En Espagne, les lois organiques sont des actes normatifs de rang supérieur, nécessaires à la réglementation des droits fondamentaux et des libertés publiques. https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444
[1759] Code pénal espagnol, chapitre I, titre X, livre II, Délits contre l'intimité, art. 197-201.https://www.conceptosjuridicos.com/delito-contra-la-intimidad/

Conclusions du chapitre 2

Le chapitre 2 présente les notions essentielles relatives à la configuration de l'infraction d'atteinte à la vie privée/violation de la vie privée, en examinant le droit pénal français et roumain sous l'angle des modalités concrètes de réalisation de l'infraction et des mécanismes normatifs associés. Tant en droit pénal français qu'en droit pénal roumain, l'architecture des infractions faisant l'objet de la présente étude est analysée et commentée : une distinction claire est établie entre les formes d'« espionnage auditif » et d'« espionnage visuel », en fonction du caractère privé ou confidentiel de la situation, de la capture, de l'enregistrement et de la transmission non autorisés, de l'existence ou non de causes justificatives, ainsi que de la nécessité du consentement. Il en ressort ainsi une typologie fondée sur des critères de contexte (espace privé/public), de finalité et de moyens techniques, auxquels s'ajoutent la géolocalisation, le droit à l'image, les formes aggravées et, de manière significative, le rapport de tension et d'équilibre entre le droit à la vie privée et la liberté d'expression. Les règles spéciales relatives à la fabrication et à l'utilisation des dispositifs de surveillance et la référence au *deepfake* indiquent une extension explicite de la protection aux nouvelles techniques de manipulation de la réalité.

Conclusions Titre II

725. Protection de la vie privée, sujet d'actualité, responsabilité délicate. Comme on peut le voir, le domaine de la protection de la vie privée humaine n'est pas seulement un sujet d'actualité, mais une responsabilité délicate du législateur français et du législateur roumain, qui ont compris le besoin vital d'adapter et de mettre à jour leurs normes en fonction des défis générés par l'évolution de la technologie numérique.

Bien que dans certaines situations, strictement liées à des raisons politiques internes d'un État, les règles puissent créer une occasion de sacrifier l'intérêt individuel en faveur de l'intérêt public[1760], cependant, dans leur forme actuelle, elles sont susceptibles de créer à l'avenir un cadre juridique suffisamment solide et efficace pour la protection de la vie privée de la personne.

726. Analyse de la législation française par rapport à la législation roumaine. Cette recherche nous convainc que le législateur français fait preuve d'un sens beaucoup plus

[1760] Par exemple, le législateur roumain autorise l'ingérence dans la vie privée d'une personne soupçonnée d'avoir commis un délit si, sur la base d'un enregistrement, on peut prouver la commission d'un acte prévu par le droit pénal.

inovateur que le législateur roumain, en ce sens qu'il met davantage l'accent sur la nécessité d'éliminer les menaces qui se sont produites avec l'évolution de la technologie numérique. Cette plus grande préoccupation de sa part peut être analysée notamment par la sévérité avec laquelle il entendait rendre responsable l'acte d`atteinte à la vie privée d'une personne. D'un autre côté, le législateur roumain semble plus tolérable et moins axé sur la prévention et la lutte contre les acquis possibles dans le contexte du numérique.

Après cette synthèse concernant les modifications législatives intervenues dans les deux pays, nous constatons que le législateur français est orienté vers une réglementation plus détaillée, liée à plusieurs hypothèses de mise en œuvre, contrairement au législateur roumain qui préfère une approche plus simpliste, en réglementant les façons de commission d`une infraction plus générale. La réglementation complexe formulée par le législateur français peut avoir un apport significatif à la protection des individus, puisque les différentes façons de commettre l'infraction conduisent automatiquement à une protection élevée de la vie privée.

Dans le même sens et avec le même intérêt, le législateur français sanctionne l'acte infractionnel d'exécution interrompue, à la lumière de la tentative, sur tous les délits repris dans l'article qui réglemente l'atteinte à la vie privée, tandis que le législateur roumain manifeste une position plus passive-agressive, réglementant la tentative comme une possibilité de contrainte, mais pas punissable.

727. Analyse des modifications apportées à la doctrine. En ce qui concerne les modifications apportées à la législation pénale française, nous sommes ralliés à la conclusion de la doctrine[1761] de considérer la forme en vigueur du droit français comme représentant, en réalité, la réglementation de nouveaux types de délits, spécifiques non seulement aux actes commis traditionnellement, mais aussi à ceux commis dans le contexte de la technologie numérique 2.0.

À ce titre, nous appuyons l'application et la poursuite de la réforme pénale sous toutes ses formes dans tous les aspects du droit privé ou public de la vie de la personne, dans le contexte de la prise de conscience et de l'hypothèse de cette évolution spectaculaire de la technologie que nous ne sommes pas seulement témoins de l'extérieur, mais participons activement, de l'intérieur. De ce point de vue, nous saluons non seulement le souci français d'une justice pénale plus juste et plus réaliste, mais aussi le courage français de sortir de la zone de confort et sa capacité à renouveler ses principes en fonction de la personnalité de l'individu, et pas seulement les caractéristiques du système juridique dans son ensemble.

[1761] Pour des détails, consulter l`opinion de J. Bossan, „*La protection de la représentation à l'ère du numérique et du deepfake : le délit de montage version 2.0*", Légipresse 2024. p.380

728. Nous pensons que, y compris le législateur roumain, devrait accorder plus d'attention à l'importance de légiférer un cadre juridique plus spécifique et plus actuel, en signalant strictement les délits déjà commis dans le domaine des technologies numériques, et dont la réglementation traditionnelle ne peut actuellement assurer une protection suffisamment efficace des droits et libertés privés. En tant que telle, une réforme législative visant à adapter les mesures de prévention et de lutte contre les atteintes à la vie privée de la personne est non seulement pertinente mais impérative en Roumanie.

729. L'importance de l'éducation publique. Comme suggestion, excluant l'existence[1762] ou non d'une réforme dans ce domaine, nous considérons qu'il est essentiel de mettre l'accent sur la valeur réelle de l'éducation publique, sur l'augmentation des investissements en matière de sécurité et sur l'importance de la formation professionnelle des organismes officiels, afin que nous puissions profiter pleinement des effets d'une réforme législative éventuelle ou existante.

Précisément pour ces arguments, même la réforme législative de la France ne doit pas être considérée comme une réponse isolée et partielle aux défis de l'évolution technologique, mais plutôt comme une partie intégrante d'un long et vaste processus d'adaptation et de transformation.

Conclusions Première partie

La première partie de la thèse fixe les repères essentiels de la protection juridique de la vie privée dans le contexte des transformations numériques, en suivant un parcours cohérent depuis les fondements jusqu'à l'application. D'une part, elle clarifie la signification contemporaine de la vie privée, comprise comme un droit subjectif qui inclut la dimension informationnelle, les médias numériques, l'identité projetée en ligne, la circulation et l'exploitation des données, les conditions valables du consentement et les exigences techniques minimales imposées aux opérateurs. D'autre part, la configuration de l'infraction d'atteinte à la vie privée et ses formes concrètes de réalisation sont analysées dans le droit français et roumain

[1762] Pour un point de vue qui appelle à l'inefficacité d'une réforme législative, en l'absence d'autres mesures, voir l'opinion de l'auteur historique israélien Y. N. Harari, « *21 Lessons for the 21st Century* », Penguin Books, 2018. p.30-31. Nous donnons, en bref, un petit fragment : « *Les révolutions dans la technologie de l'information et la biotechnologie sont encore à leurs débuts (...). La plupart des habitants de Birmingham, d'Istanbul, de Saint-Pétersbourg et de Mumbai ne sont que vaguement conscients - ou pas du tout - du développement de l'intelligence artificielle et de son impact potentiel sur leur vie. Mais il ne fait aucun doute que les révolutions technologiques vont décoller dans les prochaines décennies et soumettre l'humanité aux épreuves les plus difficiles qu'on ait jamais connues. Toute histoire qui essaiera d'attirer la loyauté de l'humanité sera testée tout d'abord par la capacité à faire face aux deux révolutions (...) devra non seulement comprendre l'intelligence artificielle, les algorithmes de Big Data et la bioingénierie, mais aussi les intégrer dans une nouvelle histoire qui a du sens* ».

: la capture et la diffusion d'images et de conversations, la surveillance par des moyens techniques, la géolocalisation, les manipulations numériques de l'image et de l'identité, ainsi que les premières réponses normatives aux nouvelles pratiques en ligne et au contenu intime divulgué.

L'ensemble de ces éléments montre que la protection de la vie privée ne peut plus être réduite à l'espace domestique ou au secret classique de la correspondance, mais suppose une délimitation juridique précise des informations, des contextes et des technologies impliqués, ainsi qu'une réévaluation du rôle de la sanction pénale par rapport à d'autres formes de réglementation. La première partie fournit ainsi le cadre nécessaire à l'analyse ultérieure de l'efficacité et des limites du droit pénal face aux intrusions spécifiques à l'ère algorithmique.

Seconde partie

LE DROIT PÉNAL FACE À L'ÉVOLUTION TECHNOLOGIQUE : INTRUSION, DÉFIS, ADAPTATION

T.S. Eliot : «La plupart du mal dans ce monde est fait par des gens ayant de bonnes intentions. »

Titre I

LE DROIT PÉNAL FACE AUX ALGORITHMES: UNE NOUVELLE RÉALITÉ JURIDIQUE

730. La technologie numérique, par rapport à la vie privée. L'article 1er de la loi de 1978 sur la protection des données dispose : « L'informatique doit être au service de chaque citoyen. Son développement doit se faire dans le cadre de la coopération internationale. Elle ne doit pas porter atteinte à l'identité humaine, aux droits de l'homme ou à la confidentialité, ni aux libertés individuelles ou publiques. Chacun a le droit de décider et de contrôler les modalités d'utilisation des données personnelles, dans les conditions prévues par cette loi[1763].

Chapitre 1

LE DROIT PÉNAL FACE À L'INTELLIGENCE ARTIFICIELLE, L'APPRENTISSAGE AUTOMATIQUE ET LE PROFILAGE DE MASSE

„Le temps du monde fini commence"

Paul Valéry, 1945

731. L'intelligence artificielle, le « cerveau » des machines[1764]. Le terme « intelligence artificielle » a été inventé en 1956 par John McCarthy, considéré comme le père de l'IA[1765]. Dans la même décennie Alan Turing pose la fameuse question : « les machines peuvent-elles penser ? »[1766].

L'intelligence artificielle (IA)[1767] est essentiellement un sous-domaine de l'informatique, visant à créer des programmes capables d'effectuer des tâches similaires à celles

[1763] LOI n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. https ://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000886460

[1764] C. Castets-Renard, J. Eynard (dir.), *Quel futur droit de l'< intelligence > < artificielle >* ?, Dalloz IP/IT, 2022.

[1765] S.L. Andresen, *John McCarthy : father of AI. Intelligent Systems*, IEEE. 17, 2002. p.84-85. 10.1109/MIS.2002.1039837.

[1766] A.M. Turing, *Computing machinery and intelligence*, Mind, Volume LIX, Issue 236, 1950. p.433-460, https ://doi.org/10.1093/mind/LIX.236.433

[1767] J.H. Fetzer, *What is Artificial Intelligence?* in: *Artificial Intelligence: Its Scope and Limits. Studies in Cognitive Systems*, vol. 4. Springer, 1990. https ://doi.org/10.1007/978-94-009-1900-6_1

des humains[1768]. Les humains restent les organismes les plus intelligents connus, possédant « l'intelligence naturelle ».[1769] Les tâches qui définissent l'intelligence sont la perception visuelle et auditive, l'apprentissage et l'adaptation, le raisonnement, la reconnaissance des formes et la prise de décision. Le terme « IA » est utilisé comme terme générique pour décrire une gamme de techniques et de technologies connexes, y compris l'apprentissage automatique, l'analyse prédictive, le traitement du langage naturel et la robotique, des tâches qui sont considérées comme intelligentes[1770].

732. IA, de l'exception à la routine. Bien que la philosophie derrière l'intelligence artificielle ait été discutée dès le XVIIIe siècle[1771], avec Leibnitz, le concept d'IA tel que nous l'utilisons aujourd'hui existe depuis 1940 et s'est fait connaître avec le développement du test de Turing en 1950[1772]. Ces dernières années, nous assistons à un développement accéléré dans le domaine de l'IA en raison de trois facteurs : l'amélioration des algorithmes, l'augmentation de la puissance de calcul et la capacité accrue à capturer et stocker des quantités colossales de données[1773]. Outre les développements technologiques, le rôle de plus en plus important de l'IA dans la vie contemporaine influence la dynamique entre les relations humaines et organisationnelles, apporte de nombreux avantages mais aussi de nombreux défis en matière de vie privée[1774]. La voix automatique qui répond[1775] au téléphone ou les recommandations adaptées aux préférences individuelles et aux besoins des utilisateurs[1776] sont des exemples de

---

[1768] F. Rosenblatt, *Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms*, éd. Spartan Books, 1962

[1769]*Difference Between Artifical Intelligence and Human Intelligence*, Geeks for Geeks, 2024. https ://www.geeksforgeeks.org/difference-between-artificial-intelligence-and-human-intelligence/

[1770]B, Coppin, *Artifical Intelligence Illuminated,* ResearchGate, 2004. /https ://www.researchgate.net/publication/31754500_Artificial_Intelligence_Illuminated_B_Coppin

[1771] V. Celso, *The Relevance of Artificial Intelligence in Realizing Leibniz's Dream of Justice*, Reasearch Gate, 2021.https ://www.researchgate.net/publication/352865386_The_Relevance_of_Artificial_Intelligence_in_Realizing_Leibnizs_Dream_of_Justice

[1772] O. Graham, D. Doe, "*The Turing test*", The Stanford Encyclopedia of Philosophy*,* 2021. <https ://plato.stanford.edu/archives/win2021/entries/turing-test/>.

[1773] S. J. Russell, P. Norvig, *Artificial Intelligence A Modern Approach,* Pearson Education Limited, 2022, p. 7 https ://api.pageplace.de/preview/DT0400.9781292401171_A41586057/preview-9781292401171_A41586057.pdf

[1774] Al Abdwani, *The Rise of Thinking Machines: A review of Artificial Intelligence in Contemporary Communication,* Journal of Business Communication & Technology, 2024.https ://www.researchgate.net/publication/380374802_The_Rise_of_Thinking_Machines_A_review_of_Artificial_Intelligence_in_Contemporary_Communication

[1775] S. Singh, S.S. Panwar, H. Dahiya, Khushboo, *Artificial intelligence voice assistant and home automation*, International Journal of Science and Research Archive, 2024.https ://www.researchgate.net/publication/381115227_Artificial_intelligence_voice_assistant_and_home_automation

[1776] D. Hirolikar, A. Satuse, O. Bhalerao, P. Pawar, H. Thorat, Hrithik, *Intelligent Movie Recommendation System Using AI and ML*, International Journal for Research in Applied Science and Engineering Technology, 2022,p.611-622.
https ://www.researchgate.net/publication/360974600_Intelligent_Movie_Recommendation_System_Using_AI_and_ML

l'omniprésence de l'IA dans la vie quotidienne[1777]. Aujourd'hui, des techniques telles que la reconnaissance vocale, le traitement du langage naturel ou l'analyse prédictive sont couramment utilisées et l'intelligence artificielle est également incluse[1778].

733. Aujourd'hui, l'IA est considérée comme la « technologie déterminante du futur »[1779]. En 2017, l'Eurobaromètre a montré que 61% des Européens ont une bonne opinion sur l'utilisation de l'IA, mais 88% estiment qu'il est nécessaire de la gérer avec prudence[1780]. Accroître l'efficacité, réduire les coûts, améliorer considérablement la santé et la recherche, accroître la sécurité des véhicules et le confort général ne sont que quelques-unes des promesses de l'IA. Cependant, comme toute nouvelle technologie, l'IA pose également des défis à la société et à la législation[1781].

Section 1. L'INTELLIGENCE ARTIFICIELLE ET LE MACHINE LEARNING: ENJEUX ET RÉGULATION JURIDIQUES

734. Types d'intelligence artificielle. Les principaux types d'IA[1782] sont l'intelligence étroite, l'intelligence générale et la super intelligence artificielle.

735. Intelligence artificielle étroite : également connue sous le nom d'intelligence augmentée, elle est délibérément programmée pour être compétente dans un domaine spécifique, avec la capacité d'améliorer l'intelligence. Par exemple, un ordinateur développé par IBM en 1980, appelé Deep Blue[1783], peut jouer aux échecs à un niveau plus élevé, étant le premier ordinateur

---

[1777] D. Spooner, *Mainstream AI: Redefining Business and Daily Life in 2024,* Scrums, 2024. https ://www.sovtech.com/blog/mainstream-ai-redefining-business-and-daily-life

[1778] F. Rosenblatt, *Principles of Neurodynamics: Perceptrons and the Theory of Brain Mechanisms*, éd. Spartan Books, 1962.

[1779] F. Meuris-Guerrero, *Quelques illustrations contemporaines de l' intelligence artificielle,* Comm. com. électr., alerte 96, n° 12, 2018: L'intelligence artificielle est considérée comme la technologie déterminante de l'avenir, notamment en raison de ambivalence, puisqu'elle promet des progrès scientifiques et une efficacité acccrue dans divers domaines :
l'algorithme « Google Inception v3 » peut identifier avec une précision de plus de 95 % plusieurs types de cancer du poumon ;
une œuvre générée par l'IA a été vendue aux enchères pour plus de 350 000 euros ;
dans le domaine de la sécurité, l'IA a contribuit au développement de détecteurs de mensonge fondés sur l'analyse des mouvements oculaires, de la voix et de la posture.

[1780] European Parliament Topics, *Artificial intelligence (AI) is set to be a "defining future technology", but what exactly is AI and how does it already affect our lives*?, 2020. https ://www.europarl.europa.eu/topics/en/article/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used

[1781] P. Boucher, *Artificial intelligence : How does it work, why does it matter, and what can we do about it?,* Scientific Foresight Unit (STOA), European Union, 2020. https ://www.europarl.europa.eu/RegData/etudes/STUD/2020/641547/EPRS_STU(2020)641547_EN.pdf

[1782]Coursera Staff, *4 Types of AI : Getting to Know Artificial Intelligence*, 2024 https ://www.coursera.org/articles/types-of-ai

[1783]Britannica, The Editors of Encyclopaedia. *"Deep Blue",* Encyclopaedia Britannica. https ://www.britannica.com/topic/Deep-Blue. Consulté le 5 octobre 2024.

de l'histoire à gagner une partie contre un champion du monde[1784]. Cependant, alors que Deep Blue démontre une extraordinaire puissance de traitement et de fabrication d'algorithmes optimisés pour le jeu d'échecs, son intelligence s'arrête à ce jeu[1785].

736. Intelligence générale artificielle – IGA (IA générale ou forte/puissante) : elle a la capacité d'apprendre, de comprendre et d'appliquer des connaissances dans de multiples domaines[1786]. IGA représente certainement la technologie du futur, apportant avec elle de nombreux défis et risques pour l'humanité, en particulier en ce qui concerne la protection de la vie privée[1787].

737. La super intelligence artificielle (SIA) est un type d'IA hypothétique avec une capacité intellectuelle supérieure à l'intellect humain. Un auteur notable sur le sujet, Nick Bostrom, définit la super intelligence comme « un intellect beaucoup plus intelligent que les meilleurs cerveaux humains dans presque tous les domaines, y compris la créativité scientifique, la sagesse générale et les compétences sociales[1788]. À l'heure actuelle, l'ASI n'existe pas, étant seulement un concept hypothétique, mais ses implications dans la société, dans la sécurité de la vie privée, dans les aspects éthiques, sont déjà discutées dans les publications de profil[1789]. Ray Kurzweil[1790] prédit dans son dernier livre qu'en 2029 nous aurons une voiture aussi intelligente qu'un homme, et que 2045 sera l'année où « l'homme deviendra immortel ». [1791]À l'heure actuelle, ce genre d'intelligence peut être découvert dans le domaine du cinéma, avec des films de science-fiction comme *ex Machina* ou *Her* fournissant une image fascinante et en même temps effrayante de l'IA et, tout en mettant en évidence son évolution rapide dans le monde quotidien. Bien que toujours au niveau SF, la super intelligence artificielle suscite des inquiétudes quant à l'intérêt humain et au respect des valeurs humaines, les experts en la matière soulignent la nécessité de l'aborder de manière éthique et responsable[1792].

[1784] G. Kasparov*, Deep Thinking : Where Machine Intelligence Ends and Human Creativity Begins,* PublicAffairs, 2017.https ://books.google.ro/books/about/Deep_Thinking.html?id=0Ub6DAAAQBAJ&redir_esc=y

[1785] R. E. Korf, *Does Deep-Blue use AI?,* Computer Science Department Unversity of California, 1997. https ://cdn.aaai.org/Workshops/1997/WS-97-04/WS97-04-001.pdf

[1786] B. Goertzel, Ben, *Artificial General Intelligence: Concept, State of the Art, and Future Prospects,* Journal of Artificial General Intelligence, 2014. https ://www.researchgate.net/publication/271390398_Artificial_General_Intelligence_Concept_State_of_the_Art_and_Future_Prospects

[1787] R. Macey-Dare, *How Soon is Now? Predicting the Expected Arrival Date of AGI-Artificial, General Intelligence*, 2023. Available at SSRN : https ://ssrn.com/abstract=4496418

[1788] N. Bostrom, E. Yudkowsky,"*The Ethics of Artificial Intelligence",* Artificial Intelligence Safety and Security, 2014.https ://www.semanticscholar.org/paper/The-Ethics-of-Artificial-Intelligence-Bostrom-Yudkowsky/787996496a300356188ba921f02f926331f80a63

[1789] R., Swajan. (2023). *AI Superintelligence and Human Existence: A Comprehensive Analysis of Ethical, Societal, and Security Implications*, Research Gate, 2023.

[1790] Ray Kuzweil est le directeur de l'ingénierie de Google, l'un des visionnaires les plus importants de l'Intelligence Artificielle et de sa place dans le futur. https ://time.com/7012871/ray-kurzweil/

[1791] R. Kurzweil, *The Singularity in Nearer*, Hardcover, 2024. https ://www.thesingularityisnearer.com/

[1792]M. Brundage, *Taking superintelligence seriously : Superintelligence : Paths, dangers, strategies by Nick Bostrom*, Elsevier, 2014.p.32-35

738. Les formes les plus connues d'IA. Parmi les exemples les plus connus de l'IA utilisée aujourd'hui, nous pouvons citer : ChatGPT, Google Translate, Netflix, Tesla[1793]. ChatGPT, une plateforme d'IA très populaire et très avancée, offre de nombreux avantages aux utilisateurs, aidant à générer du texte, des traductions ou des résumés[1794]. Un exemple promu est le cas du plombier, qui, souffrant de dyslexie[1795], communique avec ses clients avec l'aide de ChatGPT, parvenant ainsi à doubler ou même tripler ses revenus[1796].

§1. L'ADAPTATION DYNAMIQUE DES TECHNOLOGIES NUMÉRIQUES FACE AUX EXIGENCES DU DROIT

A. Machine Learning et Deep Learning

739. L'apprentissage automatique, une section de l'intelligence artificielle[1797], est une technique informatique qui permet aux ordinateurs d'« apprendre » par eux-mêmes. Ce qui différencie l'apprentissage automatique des autres formes d'IA, c'est sa capacité à s'adapter dynamiquement aux données reçues, sans ou avec de mineures interférences humaines, en développant sa propre logique[1798].

Il existe deux principaux types d'apprentissage automatique : supervisé et non supervisé.[1799] L'apprentissage supervisé nécessite des conseils externes qui étiquettent les données et décrivent comment elles doivent être interprétées. L'apprentissage non supervisé implique un algorithme qui, en traitant une grande quantité de données, apprend librement en

---

https ://doi.org/10.1016/j.futures.2015.07.009.(https ://www.sciencedirect.com/science/article/pii/S0016328715000932)

[1793] Coursera Staff. *What Is Artificial Intelligence? Definition, Uses, and Types*, 2024. https ://www.coursera.org/articles/what-is-artificial-intelligence

[1794] O. Oviedo-Trespalacios, A. E Peden, Thomas Cole-Hunter, et all, *The risks of using ChatGPT to obtain common safety-related information and advice*, Safety Science, Volume 167, 2023. https ://doi.org/10.1016/j.ssci.2023.106244.(https://www.sciencedirect.com/science/article/pii/S0925753523001868)

[1795] La dyslexie est un type de trouble de reconnaissance des lettres et des nombres qui affecte la capacité de lire, comprendre ou écrire du texte.

[1796] H., Drew, N. Tiku, W. Oremus, "*Stumbling with their words, some people let AI do the talking*", Washington Post, 10, 2022. https ://www.washingtonpost.com/technology/2022/12/10/chatgpt-ai-helps-written-communication/?mc_cid=59d8f27a92&mc_eid=3129ad1f80

[1797] I. Sarker, M.D. Furhad, R. Nowrozy, *AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions,* SN Computer Science, 2021. https ://www.researchgate.net/publication/350421584_AI-Driven_Cybersecurity_An_Overview_Security_Intelligence_Modeling_and_Research_Directions

[1798] I.H Sarker, *Machine Learning: Algorithms, Real-World Applications and Research Directions*, SN Comput Sci. 2021.

[1799] J. Han, J. Pei J, M. Kamber *Data mining: concepts and techniques,* Elsevier, 2011. [Google Scholar] [Ref list]

trouvant des schémas et des informations pertinentes par lui-même[1800]. Le succès de ces algorithmes dépend en grande partie de la qualité et de la quantité des données disponibles. Pour cette raison, le big data joue un rôle crucial dans le développement de l'apprentissage automatique.[1801]

Par exemple, pour prédire le prix d'une maison, l'algorithme analyse un certain nombre d'informations, telles que la zone où il se trouve, l'année de construction, le nombre de pièces, leur confort, l'existence d'un jardin, etc. Dans une approche d'apprentissage supervisé, des informations supplémentaires sont fournies, par exemple, les prix historiques de maisons comparables, de sorte que l'algorithme construit un modèle qui comprend la relation entre les caractéristiques et le prix, et est ensuite capable de prédire raisonnablement le prix de la maison sur la base de ces caractéristiques. Dans le contexte de l'apprentissage non supervisé, la machine ne reçoit aucun prix ou caractéristiques importantes, et doit identifier des modèles par elle-même.

740. Capacités de prédiction et de classification. Ces techniques sont utilisées dans divers contextes et à des fins[1802] diverses. Des exemples de « machine learning/apprentisage automatique » largement connus incluent les services de référence[1803] tels que Spotify, Netflix, Amazon, ou des services permettant de prédire la valeur d'un produit en fonction du marché existant[1804]. L'apprentissage automatique supervisé est généralement utilisé à des fins de prédiction et de classification, tandis que l'apprentissage automatique non supervisé est utilisé par les domaines de recherche. Aucun d'entre eux ne nécessite une programmation explicite, ce qui leur donne une certaine autonomie dans la génération de sa logique et dans l'identification des tendances qui pourraient être omises par les humains[1805].

741. Système d'apprentissage profond, synapse artificielle. L'apprentissage profond[1806] est une sous-gamme de l'apprentissage automatique, le plus souvent utilisé pour désigner les

---

[1800] A. McCallum, *Information extraction: distilling structured data from unstructured text*. Queue, 2005. [CrossRef] [Google Scholar] [Ref list]

[1801] X.W. Chen, X. Lin, « *Big Data Deep Learning : Challenges and Perspectives* », IEEE Access, vol. 2, 2014. p.514-525. https ://ieeexplore.ieee.org/document/6817512

[1802] D. Hain, R. Jurowetzki, S. Lee, et al, *Machine learning and artificial intelligence for science, technology, innovation mapping and forecasting: Review, synthesis, and applications*, Scientometrics, 2023. *p.*1465–1472. https ://doi.org/10.1007/s11192-022-04628-8

[1803] A. Marchand, P. Marx, *Automated product recommendations with preference-based explanations,* J Retail, 2020. [CrossRef] [Google Scholar] [Ref list]

[1804] M.S. Mahdavinejad, M. Rezvan, M Barekatain, P. Adibi, P. Barnaghi, A.P. Sheth, *Machine learning for internet of things data analysis: a survey*, Digit Commun Netw*,* 2018. [CrossRef] [Google Scholar] [Ref list]

[1805] C. Candrian, A. Scherer, *Rise of the machines: Delegating decisions to autonomous AI*, Computers in Human Behavior, vol 134, 2022. https ://doi.org/10.1016/j.chb.2022.107308. (https ://www.sciencedirect.com/science/article/pii/S0747563222001303)

[1806] Y. LeCun, Y., Y. Bengio, G. Hinton, *Deep Learning,* Nature*, 2015. p.*436-444 https ://doi.org/10.1038/nature14539

réseaux neuronaux profonds[1807]. En termes généraux, un réseau neuronal récurrent (RNN) traite les données en couches, chaque nouvelle couche prenant les données de sortie de la couche antérieure[1808], et le cerveau humain peut être utilisé comme analogie pour expliquer les réseaux neuronaux[1809]. Le terme « profond » fait référence au nombre de couches dans le réseau neuronal. Certains décrivent les RNN comme ayant une sorte de « mémoire » qui, comme pour la pensée humaine, peut influencer les résultats[1810]. Un exemple très utilisé et efficace de logiciel qui utilise l'apprentissage profond est le système de traduction automatique, qui parvient à obtenir une qualité, une précision et un naturel de traduction similaires à ceux atteints par des traducteurs humains[1811].

742. Problèmes de confidentialité. Plus le réseau est profond, plus les schémas deviennent complexes, plus la logique devient difficile à suivre et il est de plus en plus difficile de comprendre comment ils atteignent certaines décisions ou prédictions, car ils ne sont pas facilement expliqués et vérifiés. Les difficultés d'interprétation des modèles d'apprentissage profond forment ce que l'on appelle « l'effet boîte noire »[1812]. Cela soulève des questions dans le contexte de la protection de la vie privée, de la transparence, de l'éthique et de la sécurité, de la diminution de la confiance dans les systèmes fondés sur l'IA et de la nécessité d'un équilibre entre performance et interprétabilité[1813]. À mesure que les technologies d'IA s'intègrent de plus en plus dans nos vies, il devient crucial qu'il existe des mesures robustes pour rendre les systèmes d'IA plus transparents et conviviaux, garantissant ainsi la confidentialité et la protection des données personnelles[1814].

[1807] P. Baldi, K. Hornik, *Neural networks and principal component analysis: Learning from examples without local minima*, Neural Networks, vol. 2, issue 1, 1989. https ://doi.org/10.1016/0893-6080(89)90014-2. (https ://www.sciencedirect.com/science/article/pii/0893608089900142)

[1808] J. Schmidhuber, *Deep learning in neural networks: An overview,* Neural Networks, vol. 61, 2015. https ://doi.org/10.1016/j.neunet.2014.09.003.
(https ://www.sciencedirect.com/science/article/pii/S0893608014002135)

[1809] G. Marcus, *Deep Learning: A Critical Appraisal. Marcus propose une critique des limites de l'apprentissage profond, y compris la difficulté à expliquer les inférences dans les réseaux neuronaux complexes*, arXiv, 2018. https ://doi.org/10.48550/arXiv.1801.00631

[1810] S. Mortezapour, T. Perumal, R. Mohamed, *A Comprehensive Overview and Comparative Analysis on Deep Learning Models,* Journal on Artificial Intelligence, 2024.

[1811] M. Popel, M. Tomkova, J. Tomek, *et al. Transforming machine translation: a deep learning system reaches news translation quality comparable to human professionals*. Nat Commun, 2020. https ://doi.org/10.1038/s41467-020-18073-9

[1812] I. U. Ekanayake, D.P.P. Meddage, Upaka Rathnayake*, A novel approach to explain the black-box nature of machine learning in compressive strengh predictions of concrete using Shapley additive explanations (SHAP*), Case Studies in Construction Materials, vol. 16, 2022. https ://doi.org/10.1016/j.cscm.2022.e01059. (https ://www.sciencedirect.com/science/article/pii/S2214509522001917)

[1813] V. Hassija, V. Chamola, A. Mahapatra, *et al. Interpreting Black-Box Models: A Review on Explainable Artifical Intelligence,* Cogn Comput, 2024. p.45–74 https ://doi.org/10.1007/s12559-023-10179-8

[1814] C. Zednik, *Solving the black box problem: A normative framework for explainable artifical intelligence*, Philosophy & Technology, 2024, p.265-288. https ://doi.org/10.1007/s13347-019-00382-7

Un autre problème est lié au risque de biais auquel les modèles d'apprentissage profond sont exposés[1815]. Un autre effet indésirable est l'effet papillon, qui fait référence à la façon dont de petites variations apparemment insignifiantes des données d'entrée peuvent produire des effets importants et disproportionnés sur les résultats[1816].

743. Le mimétisme neurocognitif dans le logiciel Tray. Comme exemple des difficultés énumérées ci-dessus, nous pouvons rappeler, le logiciel Tay, développé en 2016 par Microsoft[1817]. Avec l'IA, il analyse et apprend des conversations des utilisateurs de Twitter, puis communique avec eux. Il a été fermé après seulement une journée en raison de réactions obscènes et agressives[1818].

En conclusion, la totalité des algorithmes dits « deep learning » révolutionne le domaine de l'IA avec des implications importantes en sciences cognitives et en philosophie, domaines à ce jour spécifiques à l'homme[1819].

a). Contexte de la vie privée et confidentialité (privacy)

744. Accès à des quantités colossales de données[1820]. Le machine learning et le deep learning sont basés sur l'analyse de grands volumes de données[1821], dont beaucoup sont privées.

[1815] M. Shah, N. Sureja, *A Comprehensive Review of Bias in Deep Learning Models: Methods, Impacts, and Future Directions*, Arch Computat Methods Eng, 2024. https ://doi.org/10.1007/s11831-024-10134-2

[1816] E. Ferrara, *The Butterfly Effect in artificial intelligence systems: Implications for AI bias and fairness*, Machine Learning with Applications, vol. 15, 2024. https ://doi.org/10.1016/j.mlwa.2024.100525. (https ://www.sciencedirect.com/science/article/pii/S266682702400001X)

[1817] G. Neff, P. Nagy, *Talking to Bots: Symbiotic Agency and the Case of Tay*, International Journal of Communication, 2016. p4915-4931. https ://www.researchgate.net/publication/309101946_Talking_to_Bots_Symbiotic_Agency_and_the_Case_of_Tay

[1818] S. Nistor, M. Moca, D. Moldovan, D. Oprean, R. Nistor, Răzvan, *Building a Twitter Sentiment Analysis System with Recurrent Neural Networks*, Sensors, 2021. https ://www.researchgate.net/publication/350378725_Building_a_Twitter_Sentiment_Analysis_System_with_Recurrent_Neural_Networks

[1819] P/ Perconti, P. Alessio, *Deep learning and cognitive science,* Cognition, vol.203, 2020. https ://www.sciencedirect.com/science/article/abs/pii/S0010027720301840

[1820] H. Haas, S. Astier, *Les biais de l'intelligence artificielle : quels enjeux juridiques ?*, Répertoire IP/IT, Dalloz, 2019. En ayant accès à une quantité aussi importante de données et en les analysant, les systèmes d'intelligence artificielle exercent un impact significatif sur l'égalité, la transparence et la responsabilité. Il est question de la nécessité d'une responsabilité partagée entre les concepteurs, les utilisateurs et les autorités de régulation, ainsi que de l'importance des principes de transparence, d'explicabilité et d'audit algorithmique pour la protection des droits fondamentaux.

[1821] S. Hend, M.Hoda, M. Walaa, *Big Data Analytics deep learning techniques and applications: A survey,* Information Systems, vol.120, 2024. https ://doi.org/10.1016/j.is.2023.102318. (https ://www.sciencedirect.com/science/article/pii/S0306437923001540)

Les logiciels utilisés pour la publicité personnalisée ou la reconnaissance vocale[1822] impliquent le traitement de données privées, et il existe un risque réel de mauvaise utilisation[1823].

745. Confidentialité de conception[1824]. Par conséquent, un aspect essentiel du développement de l'IA est l'impact sur la vie privée et la vie privée[1825]. L'IA est basée sur des quantités massives de données, dont beaucoup sont des données personnelles, telles que l'historique de navigation, les préférences des consommateurs ou même des données biométriques[1826]. Cela a conduit les régulateurs de la vie privée à analyser et comprendre le phénomène et également à vérifier que ce mode de traitement des données est conforme à la législation en vigueur[1827]. En mars 2023, l'Autorité italienne de protection des données (garante) a bloqué l'accès des utilisateurs à ChatGPT[1828] après avoir découvert qu'elle collectait des données sur les utilisateurs afin d'affiner son modèle d'IA, mais en violation du RGPD[1829]. Un nouveau terme « Privacy by design » est né, ce qui signifie que les principes de confidentialité[1830] sont respectés tout au long du traitement des données personnelles. Des exemples d'algorithmes d'IA qui analysent les informations personnelles sont les systèmes d'apprentissage en ligne qui détectent les états émotionnels par l'analyse de l'expression faciale[1831] ou les systèmes d'analyse et de détermination du comportement[1832].

b). ONU : La gouvernance de l'IA et son impact sur l'humanité

[1822] N. Bostrom, *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press, 2014. https ://psycnet.apa.org/record/2014-48585-000.

[1823] M. Taddeo, L. Floridi, *The case for e-trust*, Ethics and Information Technology*, 2011.* p.1–3. https ://doi.org/10.1007/s10676-010-9263-1

[1824] B. Cassar, *L'importance de la gouvernance des données dans l'usage de systèmes d'IA générative*, Dalloz IP/IT, 2023

[1825] M. van Rijmenam, CSP. *Privacy in the Age of AI: Risks, Challenges and Solutions*, The Digital Speaker, 2023. https ://www.thedigitalspeaker.com/privacy-age-ai-risks-challenges-solutions/

[1826] Y. Poullet, *Le RGPD face aux défis de l' intelligence artificielle* : Larcier, coll. CRIDS, 2020.

[1827] J. King, C. Meinhardt, *Rethinking Privacy in the AI Era Policy Provocations for a Data-Centric World,* White Paper, 2024. https ://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf

[1828] L. Bertuzzi, "*Italian data protection authority bans ChatGPT citing privacy violations*", Euractiv, 2023. https ://www.euractiv.com/section/artificialintelligence/news/italian-data-protection-authority-bans-chatgpt-citing-privacy-violations/

[1829] Garante per la protezione dei dati personali [hereafter Garante], "*Artificial intelligence: stop to ChatGPT by the Italians SA, Personal data is collected unlawfully, no age verification system is in place for children*", 2023. https ://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english.

[1830] Office of the Privacy Commissioner of Canada, "*Statement on Generative AI",* 2023, https ://www.priv.gc.ca/en/opc-news/speeches/2023/s-d_20230621_g7/

[1831] U. Ayvaz, H. Gürüler, M. Osman Devrim, *Use of facial emotion recognition in e-learning systems*, Information Technologies and Learning Tools, vol.60, no4, 2017.https ://acikerisim.mu.edu.tr/xmlui/bitstream/handle/20.500.12809/2100/G%C3%BCr%C3%BCler.pdf?sequence=1

[1832] A. Bucher, E. S. Blazek, C. T. Symons, *How are Machine Learning and Artificial Intelligence Used in Digital Behavior Change Interventions? A Scoping Review*, Mayo Clinic Proceedings: Digital Health, vol.2, issue 3, 2024. https ://doi.org/10.1016/j.mcpdig.2024.05.007.

746. L'importance du renforcement de la gouvernance internationale. Il n'y a pas de panacée pour gérer l'expansion de l'IA, c'est pourquoi l'Organisation des Nations Unies (ONU), qui comprennent officiellement 193 états membres, sur un total d'environ 195 états internationalement reconnus, publient en 2023 un rapport sur la gouvernance de l'IA et son impact sur l'humanité, renforcer la gouvernance internationale sur cette question[1833]. En septembre 2024, lors du Sommet sur l'avenir[1834], les puissances mondiales ont adopté un Pacte pour l'avenir[1835], dans lequel elles ont souligné l'importance de réglementer l'IA pour protéger les droits humains fondamentaux[1836].

Depuis 2021, le programme de recherche et d'innovation Horizon Europe est mis en œuvre au niveau européen[1837], ce qui témoigne de l'attention et de l'intérêt des autorités pour un développement responsable, tout en respectant les principes éthiques et démocratiques sur le droit à la vie privée.

747. Dans ce contexte, la Commission européenne[1838] a commencé à proposer et à développer un cadre juridique respectant les droits de la Charte des droits fondamentaux, en accordant une attention particulière au respect du droit à la vie privée, à la confidentialité, à la sécurité et à la protection des données[1839]. La résolution législative la plus récente sur le sujet a été adoptée le 13 mars 2024[1840], où les propositions du Parlement européen sur la loi sur l'intelligence artificielle [1841]et les modifications de la législation existante ont été discutées[1842]. La loi susmentionnée encourage l'innovation tout en garantissant le respect des droits

[1833]Governing AI for humanity: interim report/ Advisory Body on Artificial Intelligence, UN. Advisory Body on Artificial Intelligence, 2023. https ://digitallibrary.un.org/record/4042280?v=pdf

[1834] Summit of the Future https ://www.un.org/en/summit-of-the-future

[1835]A/RES/79/1. Resolution adopted by the General Assembly on 22 September 2024 https ://documents.un.org/doc/undoc/gen/n24/272/22/pdf/n2427222.pdf

[1836] A. Latil, *Droit de l'intelligence artificielle (droit international et droit européen),* JurisClasseur Communication, fasc. 988, LexisNexis, 2024. Le droit international de l'intelligence artificielle est encore dominé par des recommandations et des résolutions dépourvues de force obligatoire (ONU, OCDE, UNESCO, Conseil de l'Europe). En dépit des nombreuses déclarations éthiques, la régulation effective demeure partielle et inégale, confrontée à l'accélération de l'innovation technologique et à l'obsolescence rapide des normes.

[1837] Horizon Europe, un programme qui s'étend de 2021 à 2027, avec un financement important de l'Union Européenne. https ://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programs-and-open-calls/horizon-europe_en

[1838] Voir les communications de la Commission Européenne du 2018 (COM/2018/237 final), 2017 (2018/C 252/25) https ://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52017IP0051&from=IT
https ://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0237&qid=1728146549595

[1839] Résolution du Parlement Européen du 12 février 2019 sur une politique industrielle européenne globale en matière d'intelligence artificielle et de robotique https ://www.europarl.europa.eu/doceo/document/TA-8-2019-0081_EN.html

[1840] Résolution législative du Parlement Européen du 13 mars 2024 sur la proposition de règlement du Parlement Européen et du Conseil établissant des règles harmonisées en matière d'intelligence artificielle (Loi sur l'intelligence artificielle) et modifiant certaines dispositions législatives de l'Union (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD) https ://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html

[1841] AI Act enters into force. https ://commission.europa.eu/news/ai-act-enters-force-2024-08-01_en

[1842] Proposition de règlement du parlement européen et du conseil établissant des règles harmonisées en matière d'intelligence artificielle.https ://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

fondamentaux de l'homme[1843], faisant ainsi de l'UE une étape importante dans le maintien de l'équilibre entre la protection de la vie privée et le progrès technologique[1844].

B. Intelligence artificielle, apprentissage automatique et responsabilité pénale

748. IA, une menace pour la société. Il y a plus de 40 ans, en 1981, au Japon, un employé d'une usine de motos Kawasaki a été tué[1845] par un robot IA travaillant dans la même usine. Grâce à l'évolution majeure de la technologie, le pouvoir cognitif de l'IA a atteint un nouveau niveau et de plus en plus d'études dans le domaine examinent la responsabilité morale et juridique de ceux qui développent des logiciels dans l'utilisation des robots[1846]. L'IA peut devenir une menace pour la société, surtout si l'on considère que l'IA n'est pas encore soumise à des sanctions pénales[1847]. La question est de savoir qui devrait être tenu responsable des actes criminels commis par IA ? L'IA est déjà impliquée dans certaines activités qui, si elles étaient menées par des personnes, seraient considérées comme des crimes, telles que les faux avis, la manipulation des marchés financiers, les fausses nouvelles,[1848] et dans ce contexte est discutée la possibilité pour l'IA d'acquérir un statut juridique similaire à celui des personnes morales[1849].

Aujourd'hui, l'intelligence artificielle (IA) est de plus en plus utilisée dans des activités criminelles[1850] sur le dark web, dans des transactions de drogue ou dans la Commission de cybercriminalité[1851].

[1843] L. Grynbaum, C. Le Goffic, L. Pailler, *Droit des activités numériques*, 2e éd., Paris, Lefebvre Dalloz, 2023

[1844] The EU Artifical Intelligence(AI) Act: A Pioneering Framework for AI Governance, https ://www.womblebonddickinson.com/us/insights/alerts/eu-artificial-intelligence-al-act-pioneering-framework-ai-governance

[1845]*Robot kills man*, UPI archives, 1981. https ://www.upi.com/Archives/1981/12/08/Robot-kills-man/2127376635600/

[1846]R. Epstein, Richard, *The case of the killer robot.* IEEE Computer Society, 1997. https ://www.researchgate.net/publication/242362942_The_case_of_the_killer_robot

[1847] E. La Rosa, E., *Criminal Law and Artificial Intelligence: Which Spaces for a Criminal Liability of the Robot?*, in: D. Marino, M. Monaca(eds), *Artificial Intelligence and Economics : the Key to the Future. Lecture Notes in Networks and Systems*, vol 523. Springer, 2023. https ://doi.org/10.1007/978-3-031-14605-3_14

[1848]D. Leprence-Ringuet,r *Evil AI : These are the 20 most dangerous crimes that artificial intelligence will create*, Zdnet, 2020. https ://www.zdnet.com/article/evil-ai-these-are-the-20-most-dangerous-crimes-that-artificial-intelligence-will-create/

[1849] V.A. Kurki, *A theory of legal personhood*. Oxford University Press, 2019. https ://doi.org/10.1006/jevp.2001.0205

[1850]T. Blauth, O. Gstrein, et all., *Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI*, IEEE Access, 2022. https ://www.researchgate.net/publication/362096921_Artificial_Intelligence_Crime_An_Overview_of_Malicious_Use_and_Abuse_of_AI

[1851] M. Choraś, M. Woźniak, *The double-edged sword of AI: Ethical Adversarial Attacks to counter artifical intelligence for crime,* AI Ethics, 2022. p.631–634. https ://doi.org/10.1007/s43681-021-00113-9

De nombreux pays ont mis en place des véhicules autonomes, ce qui pose des problèmes techniques, éthiques et juridiques[1852]. En mars 2018, un véhicule autonome Uber a mortellement blessé un piéton en Arizona, aux États-Unis[1853]. Il s'agissait du premier cas de décès dans un accident de la route causé par un véhicule autonome[1854]. Les implications juridiques sont largement débattues, au cœur de la discussion étant l'absence de responsabilité pénale claire[1855], soulignant la nécessité d'adopter rapidement un cadre juridique[1856]. Les accusations criminelles sont allées au conducteur de secours de la voiture autonome, qui n'est pas intervenu à temps pour éviter l'accident, étant distrait en regardant une émission de télévision. Il a été accusé de meurtre coupable[1857]. Le sujet reste à l'attention des experts, puisque les véhicules autonomes sont l'avenir de la mobilité. Il traite d'une interaction complexe entre l'industrie des machines, le gouvernement (avec des réglementations et des politiques appropriées), la société civile et l'environnement[1858]. En 2016, la Déclaration d'Amsterdam sur la conduite automatisée a été adoptée[1859]. La France est le premier pays européen à adopter un cadre législatif complet en la matière, par la loi n° 2019-1428 de décembre 2019 relative à la mobilité (LOM-Loi d'orientation des mobilités)[1860]. Le décret fixe les conditions d'utilisation des véhicules autonomes, le niveau d'attention nécessaire du conducteur, ainsi que les conditions d'exemption du détenteur de la voiture en cas d'infraction[1861].

[1852] M. Martínez-Díaz, F. Soriguera, *Autonomous vehicles: theoretical and practical challenges*, Transportation Research Procedia, vol.33, 2018. https ://doi.org/10.1016/j.trpro.2018.10.103.(https ://www.sciencedirect.com/science/article/pii/S2352146518302606)

[1853] BBC,*Uber's self-driving operator charged over fatal crash*, 2020. https://www.bbc.com/news/technology-54175359

[1854] J.B. White, *Police identify first pedestrian killed by self-driving car*, Independent, 2018. https ://www.independent.co.uk/tech/selfdriving-car-death-autonomous-vehicle-crash-tempe-arizona-uber-elaine-herzberg-a8264311.html

[1855]M. L. Kubica, *Autonomous Vehicles and Liability Law*, The American Journal of Comparative Law, vol.70, Issue Supplement_1, 2022. p.i39–i69, https ://doi.org/10.1093/ajcl/avac015

[1856] Décr. nº 2021-873, 29 juin 2021, portant application de l'ordonnance nº 2021-443 du 14 avril 2021 relative au régime de responsabilité pénale applicable en cas de circulation d'un véhicule à délégation de conduite et à ses conditions d'utilisation : *JO* 1er juill. 2021, qui modifie le code de la route et le code des transports.

[1857] *The backup driver in the 1st death by a fully autonomous car pleads guilty to endanderment,* El Pais, 2023. https ://english.elpais.com/science-tech/2023-07-29/the-backup-driver-in-the-1st-death-by-a-fully-autonomous-car-pleads-guilty-to-endangerment.html

[1858] R. M. Gandia et al., *The Quintuple Helix Model and the Future of Mobility: The Case of Autonomous Vehicles,* 25th International Colloquium of Gerpisa-R/Evolutions: New Technologies and Services in the Automotive Industry, 2017.

[1859] Declaration of Amsterdam on cooperation in the field of connected and automated driving. https ://www.regjeringen.no/contentassets/ba7ab6e2a0e14e39baa77f5b76f59d14/2016-04-08-declaration-of-amsterdam---final1400661.pdf

[1860]LOI n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités, https ://www.legifrance.gouv.fr/loda/id/JORFTEXT000039666574/

[1861] G. Loiseau, *La responsabilité du conducteur d'un véhicule à délégation de conduite automatisée*, Communication Commerce électronique, 2022, comm. n° 3. L'impact des technologies de conduite automatisée sur la responsabilité du conducteur est analysé à la lumière de la loi Badinter du 5 juillet 1985 relative aux accidents de la circulation. L'auteur montre que, bien que de nouvelles notions apparaissent, telles que le « véhicule à délégation de conduite », le régime actuel d'indemnisation continue de s'appliquer aux véhicules autonomes, en

749. Système d'armes autonomes létales. Un autre défi est l'utilisation d'armes autonomes dans les forces militaires[1862]. Ces armes mortelles peuvent décider elles-mêmes de la cible, choisir le mode de fonctionnement et agir sans intervention humaine[1863]. À l'heure actuelle, le système de justice pénale présente des lacunes importantes dans ce domaine. En droit international humanitaire, branche du droit applicable dans les conflits armés, les systèmes d'armes autonomes ne sont pas spécifiquement réglementés[1864].

Le Groupe d'experts gouvernementaux[1865] sur les systèmes d'armes létales autonomes, instance internationale tenue en 2023, examine des propositions et s'est engagé à fournir un cadre réglementaire et opérationnel réglementant les systèmes d'armes létales autonomes conformément aux principes du droit humanitaire[1866].

En 2018, le Parlement Européen a adopté une résolution sur les systèmes d'armes autonomes[1867], dans laquelle il souligne la nécessité d'un contrôle humain de ces armes dans les décisions meurtrières, appelant à une position européenne commune sur le sujet.

En ce qui concerne la position des Nations Unies (ONU), le Secrétaire général a plaidé en 2018 pour l'interdiction des armes autonomes conformément au droit international. En 2023, il relance le sujet, soulignant la nécessité d'un cadre juridique interdisant le fonctionnement des armes sans supervision humaine.

750. Controverses dans la coopération internationale. En décembre 2018, les Nations Unies (ONU) ont adopté la résolution 27 intitulée « Favoriser le comportement réactif des États dans le cyberespace dans le contexte de la sécurité internationale »[1868], qui préconise l'utilisation du cyberespace à des fins pacifiques, appelant à la coopération internationale pour

---

assurant la protection des victimes par l'assurance obligatoire ou par le fonds de garantie, dans l'attente d'une éventuelle réforme spécifique adaptée à l'intelligence artificielle.

[1862] S. Abaimov, S., M. Martellini, *Artifical Intelligence in Autonomous Weapon Systems*, in M. Martellini, R. Trapp(eds), *21st Century Prometheus,* Springer, 2020. https ://doi.org/10.1007/978-3-030-28285-1_8

[1863] I. Cîrdei, *The Use of Artificial Intelligence and Autonomous Weapon Systems in Military Operations,* Reasearch Gate*,* 2024. https ://www.researchgate.net/publication/382005932_The_Use_of_Artificial_Intelligence_and_Autonomous_Weapon_Systems_in_Military_Operations

[1864] N. Davison, « *A legal perspective: Autonomous weapon systems under international humanitarian law* », în UNODA Occasional Papers *No. 30, Perspectives on Lethal Autonomous Weapon Systems*, United Nations Office for Disarmament Affairs, 2018, p. 5–18 https ://www.icrc.org/sites/default/files/document/file_list/autonomous_weapon_systems_under_international_humanitarian_law.pdf

[1865] Convention on Certain Conventional Weapons (CCW) https ://meetings.unoda.org/ccw-/convention-on-certain-conventional-weapons-group-of-governmental-experts-on-lethal-autonomous-weapons-systems-2024

[1866] Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System Geneva, 6-10 March, and 15-19 May 2023. https ://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.1_0.pdf

[1867] European Parliament resolution of 12 September 2018 on autonomous weapon systems (2018/2752(RSP))

[1868] Résolution adoptée par l'Assemblée générale le 22 décembre 2018 (sur la base du report de la Première Commission (A/73/505)) https ://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F73%2F27&Language=E&DeviceType=Desktop&LangRequested=False

prévenir toute utilisation préjudiciable. Les États-Unis et l'Union Européenne ont voté contre, affirmant qu'il restreigne le droit à la liberté et à l'expression dans le cyberespace[1869]. Une deuxième résolution sur le même sujet est intitulée : « Favoriser le comportement réactif des États dans le cyberespace dans le contexte de la sécurité internationale »[1870], et des pays comme la Russie et la Chine ont voté contre[1871].

a). Les délits générés par l'IA , créativité supérieure au délit classique

751. Les robots, un domaine réservé à la science-fiction ? À la fin des années 1980, le juge de Wendt v Host International[1872] a ouvert son opinion avec la phrase : « Robots Again = Robots de nouveau » (90). À cette époque, bien évidemment de manière ironique et anecdotique, le sujet étant plutôt un sujet de science-fiction.[1873] Il y a une discussion croissante sur la responsabilité juridique des robots, car il y a de plus en plus de délits dans lesquels ils sont impliqués[1874]. De plus en plus présente dans la vie quotidienne, l'IA est impliquée dans des activités qui ont causé des dommages aux personnes, aux animaux, aux biens et à l'environnement, qui seraient considérés comme des délits si elles étaient commises par des humains[1875]. Dans de tels cas, nous sommes confrontés à un vide législatif, la responsabilité pénale peut être attribuée dans certains cas aux opérateurs, propriétaires ou superviseurs, et non à l'entité PREND elle-même[1876]. Bien sûr, si une personne commet un délit en utilisant un objet (par exemple, une voiture ou un couteau)[1877], la responsabilité pénale incombe à la personne et non à l'objet.

[1869] G. Arvind, *A tale of two UN Resolutions on Ciber-security*, VIF 2019. https ://www.vifindia.org/2019/april/24/a-tale-of-two-un-resolutions-on-cyber-security

[1870] Résolution adoptée par l'Assemblée générale le 22 décembre 2018 [sur la base du report de la Première Commission (A/73/505)]. Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale https ://documents.un.org/doc/undoc/gen/n18/465/02/pdf/n1846502.pdf

[1871] G. Arvind, *A tale of two UN Resolutions on Ciber-security*, VIF 2019. https ://www.vifindia.org/2019/april/24/a-tale-of-two-un-resolutions-on-cyber-security

[1872] *Wendt v. Host Intern, Inc,* 197 F.3d 1284 (9th Cir. 1999) https ://casetext.com/case/wendt-v-host-intern-inc – en 1999, Bruce Wendt a intenté une action en justice contre Host International pour les dommages subis par les robots animaux utilisés pour interagir avec le public

[1873] R. Calo, *Robotics and the Lessons of Cyberlaw*, California Law Review, Vol. 103, No.3, 2014. pp.513-63 Available at SSRN : https ://ssrn.com/abstract=2402972 or http ://dx.doi.org/10.2139/ssrn.2402972

[1874] Malicious Uses and Abuses of Artificial Intelligence. https ://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

[1875] E. Nerantzi, G. Sartor, "*Hard AI crime": The Deterrence Turn,* Oxford Journal of Legal Studies, vol.44, Issue 3, 2024, p.673-701, https ://doi.org/10.1093/ojls/gqae018

[1876] R. Abbott, A. Sarch, *Punishing Artificial Intelligence: Legal Fiction or Science Fiction*, UC Davis Law Revie, 2019. Available at SSRN : https ://ssrn.com/abstract=3327485 or http ://dx.doi.org/10.2139/ssrn.3327485

[1877] T. Karagyozova, *Liability of the Indirect Perpetrator in the Absence of Identity Between What Was Done by "The Tool" and What It Was Intented to Do*, De jure, 2021. https ://www.researchgate.net/publication/356929243_Liability_of_the_Indirect_Perpetrator_in_the_Absence_of_Identity_Between_What_Was_Done_by_'The_Tool'_and_What_It_Was_Intented_to_Do

752. Types d'infractions générées par l'IA[1878]. Les délits liés à L'IA sont des actes illégaux commis par des systèmes IA/robotiques, de manière autonome ou semi-autonome[1879]. Les types de dommages que les systèmes d'IA peuvent causer sont :

- Les dommages inévitables sont les risques inhérents à tout produit ou service, puisqu'il n'y a pas un produit ou un service complètement sûr[1880]. L'exemple le plus connu est celui des accidents causés par des voitures autonomes[1881]. Aucun système, aussi sophistiqué soit-il, ne peut éviter toutes les collisions[1882].
- Les dommages délibérés de coût minimal sont prévisibles par les concepteurs, mais ne peuvent pas être évités complètement. Dans ce cas, les dommages, dont le résultat est le moins dommageable, sont pris en compte, sur la base de l'expérience psychologique « problème du chariot (trolley) »[1883].
- Dommages imprévisibles qui ne peuvent être prévus par les concepteurs. Ils apparaissent principalement à cause de la complexité des systèmes d'exploitation modernes et sont impossibles à éviter[1884].
- Dommages causés par des défauts, logiciels ou matériels généralement causés par l'inattention des designers[1885].
- Les dommages causés par une mauvaise utilisation, y compris les situations où les logiciels sont piratés ou manipulés pour être utilisés à des fins illégales[1886]. Un exemple est le logiciel équipé d'une caméra (drones) qui peut être utilisé pour espionner, ce qui implique des risques importants pour la vie privée et la sécurité des données[1887].
- Les dommages systémiques sont influencés par la nature et le type de données analysées par le système d'IA et sur la base duquel il fournit les résultats. En d'autres termes,

---

[1878] C. Coulon, *Du robot en droit de la responsabilité civile : à propos des dommages causés par les choses intelligentes*, Revue de droit de la responsabilité civile et des assurances (RCA), 2016, Étude 6.

[1879] M. Lemley, B. Casey, Bryan, *Remedies for Robots*, University of Chicago Law Review, 2019. available at SSRN : https ://ssrn.com/abstract=3223621 or http ://dx.doi.org/10.2139/ssrn.3223621

[1880] J.A. Page, "*Liability for Unreasonably and Unavoidably Unsafe Products: Does Negligence doctrine Have a Role to Play"*, Georgetown Law Faculty Publications and Other Works, 1996. https ://scholarship.law.georgetown.edu/facpub/1141

[1881] M. Monot-Fouletier, M. Clément, *Véhicule autonome : vers une autonomie du régime de la responsabilité civile* ?, Dalloz, 2018, p. 129

[1882] N.J. Goodall, *Ethical Decision Making during Automated Vehicle Crashes*, Transportation Research Record,2014. p.58-65. https ://doi.org/10.3141/2424-07

[1883] B. Duignan, "*Trolley problem*", Encyclopedia Britannica, 2024. https ://www.britannica.com/topic/trolley-problem. Consulté le 29 octobre 2024.

[1884]C. Shield, *Why do computers crash ?*, SCI. AMER., 2003. https ://www.scientificamerican.com/article/why-do-computers-crash/

[1885] D. Schreiner, *Building iRIS: A Robotic Immune System*, in R. Hähnle, J. Knoop,T. Margaria,D. Schreiner, B. Steffen(eds), *Leveraging Applications of Formal Methods, Verification, and Validation*, Communications in Computer and Information Science, vol 336. Springer, 2012. https ://doi.org/10.1007/978-3-642-34781-8_12

[1886] R. Calo, I.Evtimov, et all., *Is Tricking a Robot Hacking?,* University of Washington School of Law Research, 2018. available at SSRN : https ://ssrn.com/abstract=3150530 or http ://dx.doi.org/10.2139/ssrn.3150530

[1887] M.E. Kaminski, et all., *Averting Robot Eyes*, Maryland Law Review, Vol. 76, 2017. p. 983, Available at SSRN : https ://ssrn.com/abstract=3002576

l'impartialité et l'objectivité d'un système d'IA dépendent de l'impartialité et de l'objectivité des données à sa disposition[1888]. Approfondissant le sujet, avec le développement du Big Data, l'autonomie de l'IA augmente, et dans cette situation la responsabilité pénale en cas de délit est difficile à établir.[1889]

- Dommages collatéraux, y compris les risques de confidentialité et de sécurité découlant de l'omniprésence dans la vie quotidienne des systèmes d'intelligence artificielle, tout comme affirmait James Grimmelmann, « plus il y a d'opportunités d'innovation, plus il y a de cibles potentielles pour le piratage ».[1890]

753. Délit commis avec l'aide de l'IA. Ainsi, à mesure que la technologie progresse et que les bases de données s'agrandissent, l'IA sera de plus en plus autonome, ce qui nécessite une réglementation immédiate pour la contrôler et prévenir les activités criminelles[1891]. En outre, avec la technologie évolue les crimes, ceux faits avec l'aide de l'IA sont considérés comme des délits complexes[1892]. Les infractions LIÉES À L'IA se distinguent des infractions classiques, en particulier par la difficulté de les détecter et de les prouver, par la manière automatisée de collecter et de traiter les données, par la capacité d'étendre leurs conséquences au-delà des frontières physiques ou juridiques d'un État[1893]. En outre, contrairement à la criminalité traditionnelle, qui repose le plus souvent sur la force physique, la Commission d'une cybercriminalité nécessite un niveau plus élevé d'intelligence et de capacités mentales (créativité et manipulation, par exemple)[1894]. En examinant psychologiquement les cybercriminels, les experts soulignent qu'au-delà des gains matériels ils sont motivés à la fois par la provocation, le défi et l'idéologie, voulant démontrer leur supériorité et leur contrôle sur les autres[1895]. Par conséquent, tout cela nécessite un cadre juridique spécial[1896].

[1888] C. O'Neil, *Weapons of Math detruction: How Big Data increases inequality and threatens democracy*, Penguin Random House, 2016.

[1889] A.D.Selbst, *Disparate Impact in Big Data Policing*, Georgia Law Review, 2017. available at SSRN : https ://ssrn.com/abstract=2819182 or http ://dx.doi.org/10.2139/ssrn.2819182

[1890] J.Grimmelmann, *Regulation by Software*, Yale, 2005. available at SSRN : https ://ssrn.com/abstract=2358693

[1891] F. Lagioia, G. Sartor, *Ai Systems Under Criminal Law: a Legal Analysis and a Regulatory Perspective. Philosophy & Technology*, 2019.p.433-465. https ://doi.org/10.1007/s13347-019-00362-x.

[1892] I. al Qatawneh, A. Moussa, M. Haswa, Z. Jaffal, B. Jamal, *Artificial Intelligence Crimes,* Academic Journal of Interdisciplinary Studies, 2023. https ://www.researchgate.net/publication/366899260_Artificial_Intelligence_Crimes

[1893] T. King,et al, "*Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*", Science and engineering ethics vol. 26, 2020. https ://pmc.ncbi.nlm.nih.gov/articles/PMC6978427/

[1894] T. Fuentes-Camacho, *Les Dimensions Internationales Du Droit Du Cyberespace*, Éd. Unesco, 2000. https ://unesdoc.unesco.org/ark:/48223/pf0000219164

[1895] M. Bada, J. R. C. Nurse, "*Profiling the Cybercriminal: A Systematic Review of Research*", International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), 2021, pp. 1-8, https ://ieeexplore.ieee.org/document/9478246

[1896] A. Abd El-Latif, et.all., *Digital Forensics and Cyber Crime InvestigationRecent Advances and Future Directions*, CRC Press, 2024.

b). Europol: ChatGPT, aide pour commettre des délits (fraude, tromperie, manipulation)

754. Partant de la déclaration de T.S. Eliot selon laquelle « la plupart du mal dans ce monde est fait par des personnes avec de bonnes intentions » et reprenant la discussion sur ChatGPT[1897], en plus des avantages mentionnés ci-dessus, les chercheurs attirent l'attention sur le potentiel de manipulation et de tromperie que présente ce langage IA[1898]. En mars 2023, Europol a mis en garde contre les multiples façons dont ChatGPT peut être utilisé pour commettre des crimes[1899]. En outre, le même Europol souligne que la plate-forme est déjà utilisée pour mener des activités illégales[1900]. Les principaux délits dans lesquels ChatGPT peut être utilisé sont : fraude, fraude, fraude, désinformation, propagande, manipulation de l'opinion publique[1901]. Le dernier article sur le sujet est paru sur CNN en octobre 2024, présentant les résultats d'expériences dans lesquelles ChatGPT a été sollicité pour aider à commettre différents types de crimes, la plateforme aidant à les planifier plus rapidement[1902].

c). Modèles de responsabilité pénale de l'IA

755. Pour imposer la responsabilité pénale, il doit y avoir deux éléments principaux :l'acte physique de la Commission du délit - "**actus reus**" et l'intention criminelle ou l'élément mental - "**mens reau**"[1903]. Outre les actions délibérées, la responsabilité pénale s'étend également aux comportements négligents,[1904] où les dommages pourraient être anticipés et donc évités. Par

---

[1897] J. Sénéchal, *Le Règlement sur l'intelligence artificielle déjà obsolète face aux IA de nouvelle génération ? L'exemple de ChatGPT*, Dalloz Actualité, 2023. ChatGPT illustre la rapidité avec laquelle les avancées technologiques dépassent les instruments juridiques, en accentuant la nécessité d'une mise à jour constante du cadre normatif, d'une transparence accrue quant aux données d'entraînement et de mécanismes de contrôle adaptés aux IA génératives, qui produisent des contenus autonomes et difficilement prévisibles.

[1898] A. Sharkey, N. Sharkey, *We need to talk about deception in social robotics!,* Ethics Inf Technol*,* 2021*, p.*309–316. https ://doi.org/10.1007/s10676-020-09573-9

[1899]S. Fadilpašić, *Europol warns ChatGPT is being used to commit crime*, Techradar, 2023. https ://www.techradar.com/news/europol-warns-chatgpt-is-being-used-to-commit-crime

[1900]K. Quach, *Europol warns ChatGPT already helping folks commit crimes, There is no honor among chatbots*, The Register, 2023. https ://www.theregister.com/2023/03/28/chatgpt_europol_crime_report/

[1901] Interpol Innovation Centre, *ChatGPT: Impacts on Law enforcement*, Background paper, 2023.

[1902] A. Cooban, *ChatGPT can be tricked into telling people how to commit crimes, a tech firm finds,* CNN, 2024. https ://edition.cnn.com/2024/10/23/business/chatgpt-tricked-commit-crimes/index.html

[1903] S. William, *"Mens rea, Actus reus and the role of the state",* in *Unimaginable Atrocities : Justice, Politics, and Rights at the War crimes Tribunals*, Oxford Academic, 2012. https ://doi.org/10.1093/acprof:oso/9780199653072.003.0006, consulté le 11 octobre 2024.

[1904] J.R. Spencer, M. A. Brajeux, "*Criminal Liability for Negligence-A Lesson from across the Channel?",* The International and Comparative Law Quarterly, vol.59, no.1, 2010, p.1-24. *JSTOR*, http ://www.jstor.org/stable/25622267. Consulté le 11 octobre 2024.

conséquent, afin d'attirer la responsabilité pénale, la personne doit avoir "Mens Rea" et "actus reus" ou être considérée comme négligente[1905].

La responsabilité juridique « est une relation juridique de contrainte qui a pour objet la sanction légale »[1906]. La responsabilité pénale est une forme de responsabilité légale qui est imposée lorsqu'une règle de droit pénal est violée. Au niveau international, la responsabilité pénale individuelle est définie à l'article 25 du Statut de Rome de la Cour pénale internationale et[1907] comprend la Commission, la participation et la complicité. Elle est également définie comme une affaire individuelle qui ne peut pas être transférée. La responsabilité pénale peut être attribuée à des personnes physiques et morales et, ces dernières années, la réglementation de l'intelligence artificielle (IA) a également fait[1908] l'objet de discussions.

756. Opinions sur le cadre juridique de l'IA[1909]. Au vu de l'évolution actuelle de la technologie dans le domaine de l'intelligence artificielle, certaines voix considèrent qu'il est nécessaire d'encadrer légalement l'IA[1910], notamment pour maintenir le contrôle sur ces entités, ce sujet étant en demande depuis 80[1911].

Une façon de réglementer le délit consiste à encadrer les délits d'intelligence artificielle dans les limites législatives actuelles, le responsable étant considéré comme les fournisseurs d'IA[1912]. Cependant, étant donné que l'IA peut faire preuve d'un haut degré d'autonomie, peut prendre des décisions de manière indépendante, sans contrôle humain, il y a des voix qui

---

[1905] E. Beecher-Monas, E. Garcia-Rill, *Actus Reus, Mens Rea and Brain Science: What Do Volition and Intent Really Mean?,* Kentucky Law Journal, 2017. https ://core.ac.uk/download/pdf/346141164.pdf

[1906] G. Boboș, *Teoria generală a dreptului,* ed. Argonaut, 1999, p. 264.

[1907] K. Ambos, Article 25: Individual Criminal Responsibility, in *Triffterer/Ambos, Rome Statute of the International Criminal Court (Commentary),* 3rd edition, SSRN, 2016. https ://doi.org/10.2139/SSRN.2831626.

[1908] P.G.R. de Almeida, C.D. dos Santos, J.S. Farias, *Artificial Intelligence Regulation: a framework for governance*, Ethics Inf Technol*,* 2021, p.505–525. https ://doi.org/10.1007/s10676-021-09593-z

[1909] M. HO-DAC, *Législation européenne sur l'intelligence artificielle : point d'étape après la présidence française de l'Union européenne*, Dalloz IP/IT, 2022. Le cadre juridique actuel vise à promouvoir une intelligence artificielle digne de confiance, centrée sur l'humain, tout en respectant un équilibre entre objectifs économiques et exigences éthiques. La régulation européenne s'oriente vers un marché unique numérique compétitif, mais demeure insuffisamment ancrée dans les valeurs fondamentales de transparence, de responsabilité et de protection des droits de l'homme.

[1910] van den Hoven van Genderen, R. (2018). Do We Need New Legal Personhood in the Age of Robots and AI? In: Corrales, M., Fenwick, M., Forgó, N. (eds) Robotics, AI and the Future of Law. Perspectives in Law, Business and Innovation. Springer, Singapore. https ://doi.org/10.1007/978-981-13-2874-9_2

[1911] A Willick, Marshal S. Constitutional Law and Artificial Intelligence: The Potential Legal Recognition of Computers as "Persons", International Joint Conference on Artificial Intelligence, 1985. https ://www.semanticscholar.org/paper/Constitutional-Law-and-Artificial-Intelligence:-The-Willick/88c4d0d194a7b0823091b7254a450660682c3129

[1912] Bryson, Joanna & Theodorou, Andreas. (2019). How Society Can Maintain Human-Centric Artificial Intelligence. 10.1007/978-981-13-7725-9_16. https ://www.researchgate.net/publication/333572205_How_Society_Can_Maintain_Human-Centric_Artificial_Intelligence

préconisent de limiter la responsabilité pénale, en réglementant un « risque admissible » qui entraînerait les dommages imprévisibles causés par l'IA[1913].

Une autre approche serait l'introduction dans le droit pénal de l'entité IA/agent robot[1914], ils deviennent directement responsables de leurs actions, et les sanctions des robots comprennent la reprogrammation, l'incapacité, le service communautaire[1915]. Cela est particulièrement justifié lorsque les systèmes d'intelligence artificielle auront la capacité intellectuelle d'agir indépendamment de la volonté de leur créateur[1916].

757. Modèles de responsabilité pour les dommages causés par l'intelligence artificielle[1917]. Nous pouvons commencer ce débat avec la déclaration de Montesquieu : « la loi s'engage à ne punir que les faits », mettant ainsi l'accent sur l'équité, la modération et la prévention des abus[1918].

Gabriel Hallevy, professeur israélien de droit pénal, étudie le concept de Mens Rea dans le cas de l'intelligence artificielle, considérant qu'il s'agit d'un défi important pour la justice pénale. Ainsi, il présente 3 perspectives sur la responsabilité pénale de l'IA[1919] :

758. IA comme un instrument, responsabilité pénale de la personne qui la contrôle[1920]. Le modèle de la "perpétration par un autre" : basé sur l'idée que l'IA n'a pas de capacité

[1913] Gless, Sabine and Silverman, Emily and Weigend, Thomas, If Robots Cause Harm, Who ist o Blame? Self-Driving Cars and Criminal Liability (January 29, 2016). Available at SSRN : https ://ssrn.com/abstract=2724592 or http ://dx.doi.org/10.2139/ssrn.2724592

[1914] A. Mendoza-Caminade, *Le droit confronté à l'intelligence artificielle des robots : vers l'émergence de nouveaux concepts juridiques ?*, Dalloz, 2016. L'évolution vers des robots capables de décision et d'interaction indépendantes impose une redéfinition des notions d'agent, d'imputabilité et de faute. Plutôt qu'une révolution conceptuelle, l'IA des robots appelle une adaptation progressive des catégories juridiques existantes, destinée à maintenir l'équilibre entre le progrès technologique et la protection de la responsabilité humaine.

[1915] Hallevy, G.. (2013). When Robots kill: Artificial intelligence under criminal law. 1-244. https ://www.researchgate.net/publication/290246169_When_Robots_kill_Artificial_intelligence_under_criminal_law

[1916] Paulius Čerka, Jurgita Grigienė, Gintarė Sirbikytė, Is it possible to grant legal personality to artificial intelligence software systems?, Computer Law & Security Review, Volume 33, Issue 5, 2017, https ://doi.org/10.1016/j.clsr.2017.03.022

[1917] L. Grynbaum, chap. 3: *Responsabilité du fait d'une intelligence artificielle, Traité de droit civil – Responsabilité civile et assurance*, Paris, Dalloz, 2023. Luc Grynbaum examine la problématique de la responsabilité juridique liée à l'intelligence artificielle (IA) sous ses dimensions définitionnelle, technologique et normative, avec un accent particulier sur les évolutions européennes récentes. Il met en évidence une tension constante entre innovation et responsabilité. Bien que le droit positif offre déjà des instruments permettant de traiter les dommages causés par l'IA, l'absence d'un cadre européen unifié impose une réforme cohérente. La proposition de règlement et les futures directives constituent la base d'un régime de responsabilité hybride, adapté aux spécificités des technologies autonomes, dans lequel la transparence, l'éthique et la protection des droits fondamentaux doivent devenir des piliers centraux.

[1918] Trubowitz, A. (2017). Montesquieu's gentle prince: the law of majesty and the moderation of despotism in The Spirit of the Laws. *History of European Ideas*, 44, 194 - 209. https ://doi.org/10.1080/01916599.2017.1393764.

[1919] Hallevy, G. (2019). The Basic Models of Criminal Liability of AI Systems and Outer Circles. *SSRN Electronic Journal*. https ://doi.org/10.2139/ssrn.3402527.

[1920] P.-F. Laslier, *La responsabilité pénale du fait de l'intelligence artificielle : une approche par les risques ?*, Recueil Dalloz, 2025, p.1064. L'auteur souligne que, bien que l'IA soit déjà encadrée juridiquement par des mécanismes de conformité et des régulations, le droit pénal demeure insuffisamment adapté pour répondre aux situations dans lesquelles un système d'IA cause une infraction de manière autonome. Il rejette l'idée d'une «

cognitive, donc elle ne peut pas être assignée responsabilité pénale[1921], et la responsabilité incombe à la personne contrôlant l'IA. Par conséquent, ce modèle ne lui attribue pas la capacité mentale (« mens rea »), comme dans les cas où le délit est commis par un enfant[1922]ou par un aliéné mental[1923]. Cette catégorie comprend également les armes autonomes, utilisées dans les conflits armés, qui n'ont manifestement ni l'intention ni la volonté de commettre des crimes[1924].

La question demeure qui sera tenu responsable des délits causés par l'IA[1925] ? D'une part, le programmeur qui a développé le logiciel à la base de l'IA pourrait être responsable. Une autre option est la prise en charge de la responsabilité par l'utilisateur IA. Dans ce cas, cependant, ni le programmeur ni l'utilisateur ne répondent à l'exigence de « mauvais actus », puisque[1926] le délit a été commis par l'IA.

759. La commission tangentielle d'infractions. Le modèle des « conséquences naturelles probables » : le cas où la situation dans laquelle les systèmes D'IA sont créés dans un autre but (légal), mais à cause d'une séquence de code, ils finissent par commettre des actes illégaux. Dans ce modèle, il n'y a aucune intention de la part du programmeur ou de l'utilisateur de commettre un délit en utilisant l'IA. Un exemple est le malware BlackMamba[1927] qui, créé à l'origine pour détecter les virus, finit par devenir un spyware et envoyer des virus à d'autres systèmes en utilisant sa programmation de base[1928]. C'est aussi le cas du robot de la société Kawasaki. Il n'a pas été conçu pour tuer, mais le robot IA a considéré la personne qui est entrée pour le réparer comme une menace pour sa mission et l'a tuée.

En ce qui concerne la responsabilité pénale, il existe des experts dans le domaine qui soutiennent que les développeurs et les utilisateurs devraient prévoir et considérer tous les dommages potentiels causés par les systèmes d'IA qu'ils développent ou utilisent[1929]. Ainsi, la

---

responsabilité pénale de l'IA » en tant qu'entité et propose, en schimb, une analyse de la responsabilité « du fait de l'IA », imputée à l'opérateur humain ou à la personne morale qui la développe ou l'utilise.

[1921]L.B. Solum, *Legal Personhood for Artificial Intelligence,* 70N.C. L. Rev.1231, 1992. Available at: https ://scholarship.law.unc.edu/nclr/vol70/iss4/4

[1922] *Crichton v. United States*, 92 F.2d 224, 67 App. D.C. 300 (D.C. Cir. 1937)

[1923] *Johnson v State*, 142 Ala. 70, 38 So. 182 (1904)

[1924] V. Tzoufis, N. Petropoulos, *The commission of crimes using autonomous weapon systems: Issues of causation and attribution*, TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, vol.33, 2024, p.35-41

[1925] P. Lin, K. Abney ; G. A. Bekey, "*A Body to Kick, but Still No Soul to Damn: Legal Perspectives on Robotics*", in *Robot Ethics: The Ethical and Social Implications of Robotics*, MIT Press, 2012, https ://ieeexplore.ieee.org/document/6733967

[1926]J. Dressler, *Cases and materials on criminal law*, St. Paul, MN: Thomson/West, 2007. p.126. https ://archive.org/details/casesmaterialson0000dres_l5v2/page/n9/mode/2up

[1927] *Proof-of-concept: BlackMamba AI-developed malware,* N2K cyberwire, 2023. https ://thecyberwire.com/stories/8cb8a65a797341a4bacfbdf16e3f3e19/proof-of-concept-blackmamba-ai-developed-malware

[1928] L. Mauri, E. Damiani, *Hardening behavioral classifiers against polymorphic malware: An ensemble approach based on minority report*, Information Sciences, vol.689, 2025. https ://doi.org/10.1016/j.ins.2024.121499. (https ://www.sciencedirect.com/science/article/pii/S0020025524014130)

[1929] R. Dremliuga, N. Prisekina, *The Concept of Culpability in Criminal Law and AI Systems*, Journal of Politics and Law. 13. 256, 2020.

responsabilité pénale s'étend également à eux, le délit étant classé comme une « conséquence naturelle et probable »[1930] que le programmeur/utilisateur a encouragée ou même aidé En outre, le programmeur ou l'utilisateur peut être tenu responsable de la cybercriminalité et de la négligence[1931].

760. Développement d'algorithmes pour commettre des infractions. Modèle de responsabilité directe : ce modèle définit l'IA comme l'entité[1932] qui peut développer un algorithme pour commettre des délits par elle-même. Comme décrit ci-dessus, pour rendre une personne pénalement responsable, il doit y avoir à la fois « actus reus » et « mens rea ». Des auteurs comme Hallevy soulignent dans[1933] [1934]ses articles la capacité des robots à commettre à la fois actus reus et Mens Rea, croyant qu'ils doivent être punis pour leurs actions. Le professeur Noel Sharkey, président de la Fondation pour la robotique responsable (FRR), considère également que les réglementations sur les actions robotisées sont nécessaires et urgentes avant qu'elles ne causent de graves dommages à la société[1935].

d). L'IA en tant que personne morale

761. IA, entité non humaine, personnalité juridique?[1936] Selon le modèle de la responsabilité directe, l'IA remplit les deux conditions, il n'y a donc aucune raison de ne pas la tenir directement responsable du délit commis. Dans ce nouveau contexte, il est nécessaire de

https ://www.researchgate.net/publication/343981527_The_Concept_of_Culpability_in_Criminal_Law_and_AI_Systems

[1930] *United States v. Powell*, 929 F.2d 724 (D.C. Cir. 1991).

[1931] S. Zhao, *Theoretical Preconditions of Criminal Imputations for Negligence Crime Involving AI,* in book*, Principle of Criminal Imputation for Negligence Crime Involving Artificial Intelligence,* Springer, 2024. *p.25-57.* https ://www.researchgate.net/publication/378460722_Theoretical_Preconditions_of_Criminal_Imputation_for_Negligence_Crime_Involving_AI

[1932] R. Abbott, *The Reasonable Computer: Disrupting the Paradigm of Tort Liablity,* The George Washington Law Review, 2018. https ://www.gwlr.org/wp-content/uploads/2018/04/86-Geo.-Wash.-L.-Rev.-1.pdf

[1933]G. Hallevy, *Virtual Criminal Responsibility*, The Original Law Review, 6(1), 2010. p.6–27. https ://search.informit.org/doi/10.3316/informit.332394555889050

[1934] G. Hallevy, "*The criminal liability of artificial intelligence entities-from science fiction to legal social control*", Akron Intell. Prop J, 2010. p.171. https ://scholar.google.com/scholar?q=The+criminal+liability+of+artificial+intelligence+entities%E2%80%94from+science+fiction+to+legal+social+control

[1935] C. Cookson, "*Scientists appeal for ethical use of robots",* The Financial Times, UK, 2015.

[1936] G. Loiseau, *La personnalité juridique des robots : une monstruosité juridique*, JCP G (La Semaine juridique – Édition générale), 2018, n° 22, Actu. 597. Loiseau critique l'idée de reconnaître une personnalité juridique autonome aux robots ou aux systèmes d'intelligence artificielle, qu'il qualifie de « monstruosité juridique ». Il réagit en particulier aux propositions formulées par le Parlement européen en 2017 visant à instaurer une « personne électronique » pour les robots autonomes. La solution ne réside pas dans la « personnification des machines », mais dans l'engagement clair de la responsabilité des personnes humaines (fabricants, programmeurs, utilisateurs) pour les actes générés par ces systèmes autonomes.

discuter de la possibilité de reconnaître l'IA en tant que personne morale[1937]. Cette caractéristique est spécifique aux individus, naturels ou juridiques, imposant des droits et des obligations, et l'application de la notion de personnalité juridique à une entité telle que l'IA a de nombreuses implications juridiques, philosophiques et morales[1938].

Il n'existe actuellement aucune réglementation légale interdisant l'octroi de la personnalité juridique à des entités non humaines (voitures autonomes, sociétés, animaux, idoles diverses)[1939], ce qui rend ces dernières porteuses de droits et d'obligations[1940]. S'il n'y a vraiment pas de barrière juridique, il existe toujours un vide juridique qui semble difficile à réguler, puisque ces entités ne possèdent pas de processus cognitifs humains tels que la conscience, la morale, l'intérêt personnel, dont l'absence les rend vulnérables à ceux qui les contrôlent[1941]. À la lumière d'une analyse de l'histoire socioculturelle, nous rappelons que si les corporations/entreprises sont apparues dès le XIVe[1942] siècle, ce n'est[1943] qu'au XVIIe siècle que la responsabilité pénale leur a été assignée.

762. IA vs société commerciale. Hallevy compare des entités et des entreprises d'IA. Les deux sont présents dans la vie quotidienne, remplissant de nombreuses responsabilités, les deux sont impliqués dans divers crimes, ni n'a de représentation physique ni d'âme[1944]. Actuellement, nous avons 3 modèles de responsabilité pénale plus de nombreuses voix soutenant la nécessité d'élaborer une législation pour l'IA[1945].

[1937] R. Dremliuga, P. Kuznetcov, A. Mamychev, *Criteria for Recognition of AI as a Legal Person,* Journal of Politics and Law, 2019. https ://www.researchgate.net/publication/335305860_Criteria_for_Recognition_of_AI_as_a_Legal_Person

[1938] S M Solaiman, "*Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy*", Artificial Intelligence and Law, 2017. p.155-179, https ://www.researchgate.net/publication/310391598_Legal_personality_of_robots_corporations_idols_and_chimpanzees_a_quest_for_legitimacy

[1939] H. de Vauplane, *La personnalité juridique des robots*, in *Mélanges en l'honneur de Jean-Jacques Daigre*, Lextenso, 2017, p. 81. L'évolution technologique tend à estomper la frontière traditionnelle entre les sujets et les objets de droit. L'octroi de la personnalité juridique aux robots comporte de nombreux risques, en particulier en ce qui concerne la responsabilité et le contrôle éthique de leurs actions. De Vauplane conclut que, s'il peut être utile de recourir à des fictions juridiques limitées (par exemple en matière d'assurance ou de responsabilité civile), la reconnaissance d'une personnalité juridique pleine et entière aux robots serait prématurée et contraire à l'ordre juridique actuel, dans la mesure où elle romprait l'équilibre entre la personne humaine et la création technologique.

[1940] L.B. Solum, *Legal Personhood for Artificial Intelligence,* 70N.C. L. Rev.1231, 1992. Available at: https ://scholarship.law.unc.edu/nclr/vol70/iss4/4

[1941] J. J. Bryson, M. E. Diamantis, T. D. Grant, *Of, for, and by the people: the legal lacuna of synthetic persons,* CrossMark, 2017. https ://link.springer.com/content/pdf/10.1007/s10506-017-9214-9.pdf

[1942] H.W. Searle, *A history of English law*, Methuen, 1922. p.471-476 https ://archive.org/details/ahistoryenglish01holdgoog/mode/1up

[1943] F. Pollock, *Has the Common Law Received the Fiction Theory of Corporations?*, Q. Rev, 1911.

[1944] G. Hallevy, *The Criminal Liability of Artificial Intelligence Entities*, 2010. Available at SSRN : https ://ssrn.com/abstract=1564096 or http ://dx.doi.org/10.2139/ssrn.1564096

[1945] S. Chesterman, *From Ethics to Law: Why, When, and How to Regulate AI*, forthcoming in *The Handbook of the Ethics of AI* by D. J. Gunkel, Edward Elgar Publishing Ltd, 2023. Available at SSRN : https ://ssrn.com/abstract=4432941 or http ://dx.doi.org/10.2139/ssrn.4432941

Le véritable défi est de rendre l'IA mentalement capable (la présence de l'intention et de la conscience d'action) de commettre un crime[1946]. La connaissance est définie comme la perception de données ou de faits et, par la suite, leur compréhension[1947]. Dans le cas de l'être humain, la réception est réalisée à l'aide des organes sensoriels et la compréhension à l'aide de[1948] la substance cérébrale. Basés sur la cognition humaine, les algorithmes avancés d'IA développent un type d'intelligence basé sur la capacité de traiter et d'apprendre une quantité massive de données.[1949] Une autre fonction cognitive complexe, qui différencie réellement l'être humain du reste des mammifères, est la créativité, définie comme la capacité à chercher de nouvelles solutions lorsque la première échoue[1950]. Bien que la complexité de la créativité humaine (qui comprend les émotions, les expériences personnelles, le contexte social et culturel) soit difficile à reproduire, de plus en plus d'études explorent la créativité dans le domaine de l'IA, démontrant qu'elle peut développer une sorte de créativité relative[1951].

C. Initiatives de régulation et régime punitif de l'intelligence artificielle

763. Publilius Syrus[1952], un écrivain latin, a souligné l'importance de la punition dès le Ier siècle av. J.-C., déclarant que « à moins de punir les crimes, vous aiderez la méchanceté[1953] ». Le droit pénal moderne repose sur deux principes fondamentaux : la loi nullum crimen sine et la loi nulla poena sine[1954], qui prévoient qu'une action ne peut être sanctionnée que s'il existe une loi l'interdisant[1955].

[1946] A Padhy, *Artificial Intelligence and Intelligent Systems*, Oxford University Press, 2005. https ://books.google.ro/books?id=Kvd0QgAACAAJ

[1947] L. Anthony, *Understanding Data, Information, Knowledge And Their Inter-Relationships.* Journal of Knowledge Management Practice, Vol.7, 2007. https ://www.researchgate.net/publication/224937037_Understanding_Data_Information_Knowledge_And_Their_Inter-Relationships

[1948] A. Stroll, A.P Martinich, "*Epistemology",* Encyclopedia Britannica, 2024, https ://www.britannica.com/topic/epistemology. Consulté le 30 octobre 2024.

[1949] J.P.H.Coleman, *Ai and Our Understanding of Intelligence*, in: K. Arai, S. Kapoor, R. Bhatia(eds), *Intelligent Systems and Applications*, Springer, 2021. https ://doi.org/10.1007/978-3-030-55180-3_15

[1950] K.M. Heilman, S.E. Nadeau, D.O Beversdorf, *Creative Innovation: Possible Brain Mechanisms*, Neurocase, *9*(5), 2003.p.369-379. https ://doi.org/10.1076/neur.9.5.369.16553

[1951] H. Wang, J. Zou, et.all., *Can AI Be as Creative as Humans?,* arXiv, 2024. https ://doi.org/10.48550/arXiv.2401.01623

[1952] Britannica, The Editors of Encyclopaedia, "*Publilius Syrus*", Encyclopedia Britannica, 2024, https ://www.britannica.com/biography/Publilius-Syrus. Consulté le 9 novembre 2024.

[1953] Publilius Syrus, *Maxime,* trad. Camil Muresan, éd. Cartimplex, 2002. https ://jsri.ro/ojs/index.php/jsri/article/viewFile/84/84

[1954] Nullum crimen sine lege – pas de délit sans loi ; Nullum poena sine lege – pas de punition sans loi.

[1955] S. Dana, S., *Beyond Retroactivity to Realizing Justice : A Theory on the Principle of Legality in International Criminal Law Sentencing*, Journal of Criminal Law & Criminology, 99, 2009. p.857-928.

Selon Salmond, « le délit est un acte considéré par la loi comme nuisible à la société dans son ensemble, bien que la victime immédiate puisse être un individu ».[1956]

a). Peines pour l'intelligence artificielle

764. Technologies modernes, mesures juridiques modernes. Ainsi, étant donné que les dommages et les délits dans lesquels les systèmes d'IA sont impliqués sont[1957] de plus en plus fréquents, l'idée de punir l'IA devient de plus en plus prononcée et en même temps extrêmement difficile[1958]. Gabriel Halley est peut-être l'un des partisans les plus notoires de la punition contre l'IA, considérant que si toutes les exigences de la responsabilité pénale sont remplies, elle peut être imposée à n'importe quelle entité, qu'il s'agisse d'une personne physique, d'une personne morale ou d'une IA.[1959] En tant que promoteur de ce concept, Halley déclare que « les temps modernes exigent des mesures juridiques modernes ».[1960]

765. Le but de la peine, adapté à l'évolution. Dans son[1961] étude du concept de « punition », Michel Foucault, l'un des philosophes contemporains les plus influents, examine comment le but de la punition a changé au fil du temps, passant de la punition physique (au VIIIe siècle) à une forme de discipline du comportement et de l'esprit. Il catalogue également la punition comme un pouvoir important qui est devenu une partie de nos vies[1962].

Selon H.L.A. Hart[1963], un théoricien du droit bien connu, en particulier par son approche du droit par rapport à la morale, il analyse l'acte de punition philosophiquement et éthiquement, définissant la punition comme une caractéristique inévitable de la vie sociale[1964]. Selon lui, la punition comporte cinq objectifs : l'incapacité, la vengeance, la réadaptation, la dissuasion générale et la dissuasion spéciale. Il considère également que l'application de la peine est un

---

[1956] A. L. G., Review of *Jurisprudence, John Salmond*, The Cambridge Law Journal, vol.*2*, no.1, 1924. p.135-138 http ://www.jstor.org/stable/4515041

[1957] T. Blauth, O. Gstrein, A. Zwitter, *Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI.* IEEE Access, 2022. https ://doi.org/10.1109/access.2022.3191790.

[1958]J. K.C. Kingston, "*Artificial intelligence and legal liability*", in M.Bramer at al.,*Research and Development in Intelligent Systems XXXIII: Incorporating Applications and Innovations in Intelligent Systems XXIV*, Springer International Publishing, 2016. p.269-279

[1959]G. Hallevy, *The Punishibility of Artificial Intelligence Technology*, in *Liability for Crimes Involving Artificial Intelligence Systems*. Springer, 2014.

[1960]G. Hallevy, *When Robots Kill : Artificial Intelligence under Criminal Law*. Northeastern University Press, 2013.https ://www.researchgate.net/publication/290246169_When_Robots_kill_Artificial_intelligence_under_criminal_law

[1961]K. Thompson, *Foucault-Surveillance and Crime Control,* ReviseSociology, *2016.* https ://revisesociology.com/2016/09/21/foucault-surveillance-crime-control/

[1962]M. Foucault, *A supraveghea și a pedepsi, București, Humanitas, 1997.*

[1963]M. Kramer, *"H.L.A. Hart",* Encyclopedia Britannica, 2024. https ://www.britannica.com/biography/H-L-A-Hart. Consulté le 17 octobre 2024.

[1964]W. Cragg, *H.L.A. Hart and the Justification of Punishment*, Canadian Journal of Law & Jurisprudence, vol.5, no.1, 1992. p.43-55. https ://doi.org/10.1017/S0841820900000825

moyen de rétablir l'équilibre affecté par d'éventuels crimes. Le but de la peine est de réhabiliter et de réintégrer le délinquant dans la société, déclarant Hart : « nous ne vivons pas dans la société pour condamner, mais nous pouvons condamner pour vivre. »[1965]

Selon Ducasse, la punition doit être une action intentionnelle et consciente conçue pour provoquer une expérience/souffrance désagréable. Par conséquent, pour atteindre son objectif, il doit être appliqué à une entité capable d'être punie : consciente de la situation, capable de vivre des expériences désagréables, afin qu'elles puissent conduire à arrêter et à décourager un comportement criminel[1966].

766. Statut juridique de l'IA. Le débat sur la punition L'IA gagne du terrain dans le monde entier, avec les discussions les plus controversées sur **le manque de conscience et d'intention de l'IA**, mais aussi sur la façon dont la réalisation des objectifs traditionnels de la punition (punition, réhabilitation, dissuasion)[1967] peut être appliquée à l'IA[1968].

Après que le Parlement Européen a publié un projet soulignant l'importance de créer un statut juridique pour l'intelligence artificielle[1969], avec des droits et obligations spécifiques, la discussion est devenue encore plus importante, avec des opinions partagées. Une enquête menée en 2020 auprès d'environ 3000 internautes a montré que, bien qu'ils n'attribuent pas la conscience mentale à l'intelligence artificielle ou à l'indépendance physique, ils estiment que celle-ci doit être tenue responsable de ses actes[1970]. Cela peut s'expliquer par le caractère rétributif des personnes, le concept philosophique de toujours rechercher une personne responsable, qui doit être punie pour les délits commis et proportionnée aux délits commis, rétablissant ainsi l'équité morale, en plus d'empêcher la Commission de délits ultérieurs[1971].

767. Le manque de conscience, obstacle à la sanction pénale de l'IA. C'est ainsi que se pose le concept de **« écart de responsabilité »**, qui fait référence à la difficulté d'assigner une telle caractéristique à un robot, puisqu'il ne possède ni intentions, ni émotions, ni

[1965]H:L.A. Hart, *Punishment and Responsibility: Essays in the Philosophy of Law,* Oxford University Press, 1968. http ://doi.org/10.1093/acprof :oso/9780199534777.001.0001

[1966]C.J. Ducasse,"*Philosophy and Wisdom in Punishment and Reward*", Philosophical, 1968.

[1967]D.C. Clarke, I.D. Edge, A.N. Allott, et all., "*Punishment*", Encyclopedia Britannica, 2024. https ://www.britannica.com/topic/punishment. Consulté le 17 octobre 2024.

[1968]R. Abbott, *Punishing Artificial Intelligence*, in: *The Reasonable Robot: Artificial Intelligence and the Law*. Cambridge University Press; 2020. p.111-133. https ://www.cambridge.org/core/books/abs/reasonable-robot/punishing-artificial-intelligence/474B9814C6629636ED1CDE025C072D68

[1969] 2017. European Parliament report with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL))

[1970] G. Lima, M.Cha, C. Jeon, K.S. Park, *Explaining the Punishment Gap of AI and Robots*, arXiv, 2020. https ://www.researchgate.net/publication/339972166_Explaining_the_Punishment_Gap_of_AI_and_Robots

[1971] M. Kevin, J.Carlsmith, M. Darley, *Psychological Aspects of Retributive Justice, Advances in Experimental Social Psychology*, Academic Press, vol.40, 2008. https ://doi.org/10.1016/S0065-2601(07)00004-4. (https ://www.sciencedirect.com/science/article/pii/S0065260107000044)

conscience.[1972] Cela conduit à une impossibilité de responsabilité légale, qui est imposée dans les conditions du développement de robots de plus en plus autonomes[1973].

Certains chercheurs trouvent utile de prendre leurs responsabilités[1974] et de punir l'IA[1975]. Ils estiment que ce « fossé de responsabilité » (également appelé fossé de représailles) est de plus en plus évident avec l'action indépendante des agents de l'IA, et que sa couverture ne peut être atteinte qu'en réévaluant et en actualisant le cadre juridique afin de suivre le développement de la technologie[1976]. Dans son article de 2019, Turner a proposé d'adapter les lois existantes ainsi que d'adopter de nouvelles réglementations spécifiques à l'intelligence artificielle, tout en soulignant les défis posés par l'attribution de la responsabilité à l'IA[1977].

D'autre part, de nombreuses voix s'opposent à l'octroi de la personnalité juridique à l'intelligence artificielle, qui n'[1978]est ni bénéfique ni nécessaire. Il y a des auteurs qui soulèvent des questions sur l'éthique et la moralité d'une telle attitude, ce qui peut conduire à une érosion des droits humains, étant donné que les robots/IA n'ont ni intention ni conscience, et ne ressentent pas de douleur (ils n'ont pas d'émotions)[1979] [1980]. D'autres voix s'inquiètent des abus qui peuvent résulter de cette responsabilité juridique, ainsi que de l'incapacité de se représenter et de se défendre devant les tribunaux[1981]. Par conséquent, tenir l'IA responsable peut être interprété comme un mécanisme de protection des personnes physiques ou morales, permettant dans ce contexte le transfert de responsabilité à des entités robotiques[1982].

768. Le monde de science-fiction d'Asimov devenu réalité. Il y a près d'un siècle, Isaac Asimov créait un monde de science-fiction dans lequel les robots étaient intégrés dans la vie quotidienne, divisés par l'auteur en deux catégories : les robots menaçants : se rebeller contre leurs créateurs, selon le personnage mythologique Prométhée, et les bons robots : traité comme

---

[1972] J. Danaher, *Robots, law and the retribution gap*, Ethics Inf Technol, vol.18, 2016. p.299–309 https ://doi.org/10.1007/s10676-016-9403-3

[1973] L.B. Solum, *Legal Personhood for Artificial Intelligences*, North Carolina Law Review, vol.70, 1992, p.1231, available at SSRN : https ://ssrn.com/abstract=1108671

[1974] A. Matthias, *The responsibility gap: Ascribing responsibility for the actions of learning automata*. Ethics Inf Technol vol.6, 2004, p.175–183. https ://doi.org/10.1007/s10676-004-3422-1

[1975]J. Danaher, *Robots, law and the retribution gap*, Ethics Inf Technol vol.18, 2016, p.299–309. https ://doi.org/10.1007/s10676-016-9403-3

[1976] B.J. Koops, et all, *Bridging the Accountability Gap: Rights for New Entities in the Information Society?* Minnesota Journal of Law, Science & Technology, vol. 11, no. 2, 2010. pp. 497-561, 2010. available at SSRN : https ://ssrn.com/abstract=1647744

[1977] J. Turner, *Robot rules: Regulation Artificial Intelligence*, Springer, 2018.

[1978] S.Chopra, L. White, *Artifcial Agents – Personhood in Law and Philosophy*, DBLP, 2004, p.635-639.

[1979] S.M. Solaiman, "*Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy*" Artif Intell Law, vol.25, 2017. p.155-179. https ://doi.org/10.1007/s10506-016-9192-3

[1980] P. Lin, K. Abney, G.A. Bekey, "*A body to Kick, but Still No Soul to Damn : Legal perspectives on Robotics",* in *Robot Ethics : The Ethical and social implications of Robotics*, MIT Press, 2012. https ://ieeexplore.ieee.org/document/6733967

[1981] A. Kasap, *Artificial Intelligence and Legal Personhood: Current Developments in Turkish Law*, Turk-Alman Universitesi Hukuk Fakultesi Dergisi, 2022. p.485-556 available at SSRN: https ://ssrn.com/abstract=4506435

[1982] J. Bryson, M. Diamantis, T.D. Grant, *Of, for, and by the People: The Legal Lacuna of Synthetic Persons*, 25 Artificial Intelligence & L. 273, 2017. available at SSRN : https ://ssrn.com/abstract=3068082

esclave des hommes[1983]. Résumant toutes ces préoccupations, les experts en robotique adressent une lettre ouverte à la Commission européenne, appelant à la nécessité d'intégrer l'IA dans la société tout en respectant les principes éthiques et moraux. Par conséquent, les règlements adoptés à l'avenir doivent respecter, outre les droits fondamentaux de l'homme et ceux des robots/IA[1984].

Bien que les opinions divergent, il est généralement admis qu'une réglementation responsable de l'IA/robots est impétueusement nécessaire, ce qui est soutenu par l'attention de leaders mondiaux tels qu'Emmanuel Macron[1985] [1986] ou Theresa May[1987] sur ce sujet.

769. Il ne faut cependant pas confondre l'autonomie opérationnelle des robots avec l'autonomie morale des[1988] humains, et c'est pourquoi il y a encore des voix qui croient que les propriétaires, développeurs ou utilisateurs d'IA doivent rester responsables des actions des robots[1989]. À titre d'exemple, les robots utilisés dans les opérations militaires (les soi-disant « robots tueurs ») peuvent être mentionnés. En 2008, une unité robotique mobile en Irak a remis ses armes aux soldats du même camp. Les rapports suivants ne sont pas entièrement disponibles, mais les dysfonctionnements sont admis dès la phase de test[1990]. En 2007, un robot semi-automatique appartenant à l'armée sud-africaine tue 9 camarades et en blesse 14 autres[1991]. Afin de déterminer à qui la responsabilité pénale est adressée dans ces cas, il existe des auteurs dans le domaine qui considèrent qu'il est essentiel de classer les robots en trois catégories[1992] : robots apprenants non autonomes, autonomes (incapables d'apprendre) et autonomes (capables de développer de nouveaux schémas sans intervention humaine, allant ainsi au-delà du mode de

[1983] I. Asimov, *The Complete Robot*, Doubleday, 1982. https ://archive.org/details/completerobot00asim/page/n5/mode/2up

[1984] 2017. Open Letter to the European Commission on Artificial Intelligence and Robotics. Available at http ://www.robotics-openletter.eu/

[1985] N. Thompson, *Emmanuel Macron Talks to WIRED about France's AI Strategy*, Wired, 2018. available at https ://tinyurl.com/ychfw8cn

[1986] *Déclaration de M. Emmanuel Macron, président de la République, sur les efforts en faveur du développement de l'intelligence artificielle, à Paris le 21 mai 2024*, Vie pulique, 2024. https ://www.vie-publique.fr/discours/294258-emmanuel-macron-21052024-intelligence-artificielle

[1987] *Theresa May's Davos address in full*, World Economic Forum Annual Meeting, 2018. Available at https ://tinyurl.com/y3upenl5.

[1988] L'autonomie morale est caractérisée par les capacités suivantes : intention, raison et action, sentiment, autonomie, intelligence native, socialisation, personnalité.

[1989] W. Haselager, *Robotics, philosophy and the problems of autonomy*. Pragmatics and Cognition. vol.13, no.3, 2005.p.515-532. https ://www.researchgate.net/publication/233676691_Robotics_philosophy_and_the_problems_of_autonomy

[1990] P. Lin, *Robots in War : issues of Risk and Ethics*, AKA Verlag Heidelberg, 2009. p.7 https ://www.ethics.calpoly.edu/ONR_report.pdf

[1991] P. Lin, K. Abney, G. Bekey, *Robot ethics: Mapping the issues for a mechanized World*, Artificial Intelligence, Elsevier, vol.175, issues 5–6, 2011. page 945. https ://doi.org/10.1016/j.artint.2010.11.026

[1992] L. Royakkers, P. Olsthoorn, *Military Robots and the Question of Responsibility*, International Journal of TechnoEthics (IJT), vol.5, no.1, 2014. p.1-14 https ://www.academia.edu/7370762/Military_Robots_and_the_Question_of_Responsibility_Lamb%C3%A8r_Royakkers_and_Peter_Olsthoorn

fonctionnement initial)[1993]. Par conséquent, la responsabilité des robots s'impose avec l'augmentation de leur autonomie, définie comme leur capacité à apprendre des expériences antérieures et à agir sans intervention humaine[1994].

Des exemples sont également dans le domaine médical, quand un algorithme d'IA qui contrôlait la pharmacie de l'hôpital a libéré un mauvais médicament, ce qui a conduit plus tard à la mort du patient. Le médecin en charge du patient a été puni pour cette erreur[1995].

Selon la loi, les principaux types de peines sont la peine de mort, l'emprisonnement, les travaux d'intérêt général et les amendes[1996]. Diverses sanctions qui peuvent être appliquées à l'IA sont remises en question pour la rendre inapte ou l'empêcher de commettre des délits à l'avenir, telles que la suppression des logiciels qui régissent l'IA, la confiscation, l'interdiction d'utilisation ou la destruction de l'IA[1997].

b). Réglementation de l'IA et de l'Apprentissage automatique en droit pénal

770. Cybercrimes, évolution sur la liste des menaces. Chaque année, le gouvernement américain publie un rapport intitulé « évaluation mondiale des menaces »[1998] qui met en lumière les plus grandes menaces à la sécurité nationale. Dans le rapport de 2007[1999], il n'y avait aucune mention des cyber problèmes. En 2011[2000], la cybersécurité a été mentionnée, prenant la dernière place dans la liste des menaces[2001], et à partir de 2013, les cyber enjeux ont été placés au premier plan de ces rapports.

[1993] A. Matthias, *The responsibility fap: Ascribing responsibility for the actions of learning automata*, Ethics and Information Technology, vol.6, 2004. p.175-183. https ://www.researchgate.net/publication/225249319_The_responsibility_gap_Ascribing_responsibility_for_the_actions_of_learning_automata

[1994] R. Hakli, P. Mäkelä, *Robots, Autonomy and Responsibility*, in J.Seibt et al., *What social robots can and should do*, IOS Press, 2016. https ://philarchive.org/rec/HAKRAA

[1995]R.E. Ferner, *Medication errors that have led to manslaughter charges,* BMJ, 2000. p.321 :1212. https ://www.bmj.com/content/321/7270/1212.full

[1996]Sage Publications, Inc**.**, «*Chapter 3: Punishment and Sentencing (Florida)*», *SAGE Edge*, s.a. https ://edge.sagepub.com/sites/default/files/FL03_0.pdf

[1997]S. Jaha, S. Thrun, *Artificial Intelligence and Its Legal Personhood in Criminal Law: A Systematic Review*, Research Gate, 2024. https ://www.researchgate.net/publication/382597687_Artificial_Intelligence_and_Its_Legal_Personhood_in_Criminal_Law_A_Systematic_Review

[1998]Intel.gov, *Annual threat assessment*. https ://www.intelligence.gov/annual-threat-assessment

[1999]Intel.gov, *Annual threat assessment*, 2007. https ://www.dni.gov/files/documents/Newsroom/Testimonies/20070111_testimony.pdf

[2000]Intel.gov, *Annual threat assessment*, 2011. https ://www.dni.gov/files/documents/Newsroom/Testimonies/20110310_testimony_clapper.pdf

[2001]Intel.gov, *Annual threat assessment*, 2013. https ://www.dni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf

En 2010, un virus informatique, Stuxnet, attaque les centrales nucléaires iraniennes, représentant certaines des premières cyberarmes utilisées pour causer des dommages physiques aux infrastructures. Le virus a manipulé les systèmes logiciels de l'usine, affectant le fonctionnement des centrifugeuses utilisées pour enrichir l'uranium, entraînant de graves conséquences pour les opérations nucléaires iraniennes[2002]. Cette vulnérabilité n'a été que le début des discussions sur la menace de la cyberguerre et les réactions de la société civile à celle-ci, sur la gestion de la peur, l'incertitude et la protection de la vie privée[2003]. Ces raisons soutiennent l'introduction d'une forme de responsabilité pénale pour l'intelligence artificielle.

771. Restrictions sur les acteurs humains, pas sur le développement technologique. Bien que plus honorifique, il y a des voix qui préconisent l'utilisation des trois "lois" d'Asimov (interprétées plutôt comme des règles) comme base de la réglementation pénale de l'IA[2004]. Selon la première loi, les robots ne peuvent pas blesser un humain. Deuxièmement, les ordres humains doivent être obéis, et enfin, les robots doivent protéger leur propre existence, bien sûr sans enfreindre la première règle[2005] [2006]. En 2017, Balkin a critiqué ces lois, affirmant que derrière les robots et les algorithmes d'IA se trouvent des gens, qui les programment, les contrôlent et les utilisent, et que les restrictions devraient être dirigées contre eux et non contre le développement de la technologie[2007]. De plus, il propose 3 nouvelles règles, alignées sur les besoins actuels de la société, lorsque les robots ne sont plus seulement de la science-fiction[2008]. La première règle fait référence aux obligations fiduciaires que les développeurs d'algorithmes d'IA ont envers les utilisateurs. Ils doivent protéger la vie privée des utilisateurs et agir dans leur intérêt[2009]. La deuxième règle précise les devoirs que les opérateurs ont envers le grand public et la troisième interdit la création d'algorithmes à des fins négatives[2010].

En termes de **maintien du contrôle sur l'IA**, deux façons sont décrites. Le premier concerne la conception appropriée des algorithmes d'IA, en explorant soigneusement toutes les

---

[2002]J.P. Farwell, R. Rohozinski, *Stuxnet and the Future of Cyber War*, Survival, vol.*53*(1), 2011, p.23–40. https ://doi.org/10.1080/00396338.2011.555586

[2003] Y. Abramson, G. Baram, *Saving face in the cyberspace: Responses to public cyber intrusions in the Gulf*, Contemporary Security Policy, vol.*45*(2), 2023. p.210–238. https ://doi.org/10.1080/13523260.2023.2271794

[2004] S:L. Anderson, *Asimov's "three laws of robotics" and machine metaethics*, AI & Soc vol.22, 2008, p.477-493 https ://doi.org/10.1007/s00146-007-0094-5

[2005] R. Murphy, D. Woods, *Beyond Asimov : The Three Laws of Responsible Robotics*, IEEE Intelligent Systems, vol.24, no.4, 2009. p.14-20 https ://doi.org/10.1109/MIS.2009.69.

[2006]I. Asimov, *I Robot: Runaround,* Garden City, New York Doubleday & Company Inc., 1950.

[2007] J.M. Balkin, *Les trois lois de la robotique à l'ère du Big Data*, Ohio State Law Journal, vol.78, 2017. disponible à SSRN : https ://ssrn.com/abstract=2890965

[2008] D. Ichbiah, *Robots : From Science Fiction to Technological Revolution*, Harry N. Abrams 2005. https ://doi.org/10.5860/choice.43-1587.

[2009] J.M Balkin*, Information Fiduciaries and the First Amendment,* UC Davis Law Review, vol.49, no.4, 2016, available at SSRN : https ://ssrn.com/abstract=2675270

[2010] J.M Balkin, *The Three Laws of Robotics in the Age of Big Data,* Ohio State Law Journal, vol. 78, 2017. available at SSRN : https ://ssrn.com/abstract=2890965

possibilités et en dessinant des limites et des contraintes claires appropriées à leur autonomie. La deuxième façon est d'être responsable par la loi, par la réglementation de ceux qui développent, possèdent ou exploitent l'IA, conçue pour protéger les droits fondamentaux en matière de technologie moderne[2011].

c). Initiatives législatives et nécessité d'adaptation

772. En ce qui concerne les initiatives législatives, elles peuvent être imposées par les autorités nationales et internationales (Parlement Européen)[2012]. L'ordre inverse des événements est à noter dans ce domaine : d'abord le changement imposé par la technologie et, bien sûr, ses effets apparaissent, puis les règlements qui la régissent apparaissent.

En juin 2018, la Commission européenne a présenté la stratégie de l'UE en matière d'IA[2013]. Cela comprend 4 objectifs principaux :

- Soutenir l'évolution technologique dans divers domaines (santé, industrie, sécurité) en adoptant l'IA dans l'ensemble de l'économie
- Préparer le changement socio-économique
- Assurer un cadre éthique et juridique solide et approprié
- Unir les forces des états membres

773. Documents législatifs existants. Dans l'Union Européenne, les principaux documents visant à réglementer l'IA, à soutenir l'évolution technologique et à garantir en même temps un cadre juridique approprié sont :

- Stratégie européenne en matière d'IA, avril 2018[2014]
- Intelligence artificielle pour l'Europe, 2018[2015]

[2011] J. Bryson, A.Theodorou, *How Society Should Regulate Autonomous Technologies: A Framework for Legal Reforms*, European Journal of Technology and Ethics, vol.14(1), 2018. p.5 https ://www.joannajbryson.org/publications/how-society-can-maintain-human-centric-artificial-intelligence-pdf

[2012] F. Duina, T. Raunio, *The open method of co-ordination and national parliaments: Further marginalization or new opportunities?*, Journal of European Public Policy, vol.14, no.4, 2007, p.489-506. https://www.researchgate.net/publication/263496018_The_Open_Method_of_Coordination_and_National_Parliaments_Further_Marginalization_or_New_Opportunities

[2013] *Communication from the commission to the european parliament, the european council, the council, the european economic and social committee and the committee of the regions, Artificial Intelligence for Europe, SWD(2018) 137 final,* European Commission, 2018. https ://eur-lex.europa.eu/legal-content/EN/TXT/PDF/ ?uri=CELEX :52018DC0237&from=EN

[2014] *Communication from the commission to the european parliament, the european council, the council, the european economic and social committee and the committee of the regions Artificial Intelligence for Europe COM/2018/237 final*, European Commission law, 2018. https ://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=COM%3A2018%3A237%3AFIN

[2015] Commission staff working document, *Liability for emerging digital technologies Accompanying the document Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Artificial Intelligence for Europe*

- Livre blanc sur l'intelligence artificielle, 2020[2016]
- Communication de la Commission Européenne sur les données, 2020[2017]
- Plan coordonné sur l'intelligence artificielle, avril 2021
- Plan d'action pour l'éducation numérique 2021-2027[2018]

Le plan coordonné sur l'IA[2019], le dernier règlement de la Commission européenne axé sur les règles de sécurité dans l'utilisation des systèmes d'IA, sur l'interdiction des pratiques d'IA, définit des exigences spécifiques et des règles de transparence pour les systèmes de confidentialité de l'IA à haut risque (identification barométrique, Logiciels D'IA utilisés pour générer et manipuler des images, du contenu audio ou vidéo, des systèmes de surveillance et de surveillance). [2020]L'homme est également le pion principal, et les systèmes d'IA sont conçus pour soutenir ses activités.

774. Cadre législatif ciblé pour les domaines à risque. Dans les zones à haut risque, l'UE a élaboré un cadre législatif ciblé et plus détaillé assorti de réglementations spécifiques. Dans le domaine de la santé, l'utilisation de dispositifs avec IA est régie par : le règlement sur les dispositifs médicaux (MDR)[2021] et le règlement sur les dispositifs médicaux pour le diagnostic in vitro (IVDR)[2022]. L'utilisation des véhicules autonomes est coordonnée par le règlement sur la sécurité générale des véhicules (GVSR)[2023], le règlement relatif à la réception et à la

SWD/2018/137 final, European Commission law, 2018. https ://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52018SC0137

[2016] *Livre Blanc, Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance* European Commission law, 2020. https ://op.europa.eu/en/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1/language-ro

[2017] *Communication de la commission au parlement européen, au conseil, au comité économique et social européen et au comité des régions Une stratégie européenne en matière de données*, European Commission law, 2020. https ://eur-lex.europa.eu/legal-content/RO/TXT/HTML/ ?uri=CELEX :52020DC0066

[2018]European Education Area, *Plan d'action en matière d'éducation numérique (2021-2027*).https ://education.ec.europa.eu/focus-topics/digital-education/action-plan

[2019] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial intelligence act) and amending certain union legislative acts, COM/2021/206 final https ://eur-lex.europa.eu/legal-content/EN/TXT/ ?uri=celex%3A52021PC0206

[2020] N.T. Nikolinakos, (2023). *The Proposed Artificial Intelligence Act and Subsequent "Compromise" Proposals: Commission, Council, Parliament*, in: *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies – The AI Act,* Law, Governance and Technology Series, vol. 53. Springer, Cham, 2023. https ://doi.org/10.1007/978-3-031-27953-9_8

[2021] Regulation (UE) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) n° 178/2002 and Regulation (EC) n° 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC, OJ L 117 on 5.5.2017

[2022] Regulation (UE) 2017/745 of the European Parliament and of the Council of 5 April 2017 on in vitro iagnostic in vitro medical devices and repealing Directive 98/79/EC and Commission Decision 2010/2017/EU OJ L 117 on 5.5.2017.

[2023] Regulation (UE) 2019/2144 of the European Parliament and of the Council of 27 November 2019 http ://data.europa.eu/eli/reg/2019/2144/oj

surveillance du marché des véhicules[2024] (AMSVR) et la directive sur l'assurance des véhicules (MID)[2025].

Le premier cadre législatif de l'UE sur l'IA a été publié en 2021[2026], réglementant dans son article 5 les activités interdites de l'IA (dont la plupart se réfèrent à l'intrusion dans la vie privée) : pratiques subliminales (paragraphe 1, lettre a), exploitation des vulnérabilités (paragraphe 1, lettre b), évaluation du comportement social par les autorités (paragraphe 1) lettre c), l'utilisation de systèmes d'identification barométrique à distance en temps réel à des fins répressives (paragraphe 1, lettre d). La dernière version du « Règlement de l'UE établissant des règles sur l'intelligence artificielle »[2027] a été publiée le 13 juin 2024, faisant de l'Europe une étape importante dans la réglementation de l'IA.

Il est entré en vigueur en Roumanie le 1er août 2024[2028]. En outre, le gouvernement roumain adopte le projet de stratégie nationale dans le domaine de l'intelligence artificielle 2024-2027 (SN-A)[2029].

d). Rapport de la CNIL : la technologie IA respecte le droit à la vie privée

775. Implication de la CNIL dans la réglementation de l'IA. En France, la CNIL (Commission nationale de l'informatique et des libertés) a publié en 2023 un rapport sur l'utilisation de l'IA, assurant ainsi l'évolution des technologies tout en respectant le droit à la vie privée[2030]. En 2024, la même organisation a lancé un ensemble de règles visant à garantir la

[2024] Regulation 2018/858 of the European Parliament and of the Council of 30 May 2018 on the approval and market surveillance of motor vehicles and their trailers, and of the systems, components and separate technical units intended for such vehicles, OJ L 151 of 14.06.2018.
[2025] Directive 2009/103 of the European Parliament and of the Council of 16 September 2009 relating to insurance against civil liability in respect of the use of motor vehicles, and the enforcement of the obligation to insure against such liability.
[2026] The EU's Artificial Intelligence Act – Understand the EU regulations and which actions to take https ://2021.ai/wp-content/uploads/2021/06/eu-regulations-brochure.pdf
[2027] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) 168/2013, (EU) 2018/858, (EU) 2018/1139 and No 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 nd (EU) 2020/1828 (Artificial Intelligence Act) http ://data.europa.eu/eli/reg/2024/1689/oj
[2028] *Roumanie, le Règlement de l'UE sur l'intelligence artificielle : ce que les entreprises doivent savoir,* bnt attorneys in CEE, 2024.
https ://bnt.eu/ro/legal-news/romania-eu-artificial-intelligence-regulation-what-companies-need-to-know/
[2029] *Décision relative à l'approbation de la Stratégie nationale dans le domaine de l'intelligence artificielle 2024-2027 conformément à l'article 108 de la Constitution Roumaine, republiée, et à l'article 25 e) de l'Ordonnance d'Urgence n° 57/2019 sur le Code administratif, telle que modifiée et complétée*, Gouvernement de la Roumanie, https ://www.mcid.gov.ro/wp-content/uploads/2024/03/HG-SN-IA-2024-2027.pdf
[2030] CNIL, *Intelligence artificielle : le Plan d'action de la CNIL*, 2023. https ://www.cnil.fr/fr/intelligence-artificielle-le-plan-daction-de-la-cnil

vie privée et les droits des personnes impliquées dans le développement et l'utilisation de l'IA[2031].

Dans le rapport de 2011, j'ai souligné les principales lacunes décrites dans le régime réglementaire actuel. Une chose difficile à faire est d'établir la culpabilité, en tenant compte de la nature imprévisible et du manque de contrôle des algorithmes d'IA. Ainsi, si l'action d'un algorithme robot/IA ne peut être anticipée, comment l'utilisateur ou le propriétaire peut-il être tenu responsable[2032] ? Un autre problème est la preuve de causalité, si le dommage est le résultat d'un défaut logiciel de l'IA ou d'une mauvaise utilisation, dans ce cas la faute étant divisée entre les programmeurs et les utilisateurs[2033].enfin, la répartition des responsabilités entre programmeurs / producteurs, utilisateurs et fournisseurs de données est un défi, pas facile à établir[2034].

776. Réglementation IA : analyse européenne. En 2023, les auteurs Karolina Woszczcyna et Karolina Mania ont analysé les politiques de mise en œuvre de l'utilisation de l'IA dans les 27 pays de l'Union Européenne, analysant les solutions proposées par la France, l'Allemagne et la Pologne sur ce sujet[2035]. Le premier plan national de développement de l'IA[2036] a été rédigé en 2018 en France, qui a également été qualifié de pionnier du développement et de la régulation de l'intelligence artificielle. Il est à noter que, bien que le risque que pose l'IA en matière de vie privée soit connu, la France s'appuie sur l'utilisation de cette technologie pour l'égalité dans la société, pour créer un équilibre entre les sexes, stimuler la diversité, en d'autres termes pour accroître la sécurité de l'individu et le respect de ses droits fondamentaux[2037].

e). Juridiction des délits causés par l'IA

[2031] CNIL, *IA : la CNIL publie ses premières recommandations sur le développement des systèmes d'intelligence artificielle*, 2024. https ://www.cnil.fr/fr/ia-la-cnil-publie-ses-premieres-recommandations-sur-le-developpement-des-systemes-dintelligence

[2032] M. Lohmann, *Roboter als Wundertüten — eine zivilrechtliche Haftungsanalise*, Aktuelle Juristische Praxis, vol.2, 2017, p.152-162. https ://www.alexandria.unisg.ch/server/api/core/bitstreams/1d2cc6e0-e4e1-4fa2-aa18-8c17923fe3b3/content

[2033] W.D. Smart, C. Grimm, W. Hartzog, *An Education Theory of Fault for Autonomous Systems*, Notre Dame Journal on Emerging Technologies vol.33, 2021. p.12-13 available at SSRN : https ://ssrn.com/abstract=3854927

[2034] A.D. Selbst, *Negligence and AI's Human Users,* 100 Boston University Law Review 1315, 2020. available at SSRN : https ://ssrn.com/abstract=3350508

[2035] K. Woszczyna, K. Mania, "*The European map of artificial intelligence development policies: a comparative analysis"*, International Journal of Contemporary Management, vol.59, no.3, Sciendo, 2023. p.78-87. https ://doi.org/10.2478/ijcm-2023-0002

[2036] C. Villani, Y. Bonnet, B. Rondepierre, *For a meaningful artificial intelligence: Towards a French and European strategy*, Conseil national du numérique, 2018. https ://www.jaist.ac.jp/~bao/AI/OtherAIstrategies/MissionVillani_Report_ENG-VF.pdf

[2037] K. Woszczyna, K. Mania, "*The European map of artificial intelligence development policies: a comparative analysis"*, International Journal of Contemporary Management, vol.59, no.3, Sciendo, 2023. p.78-87. https ://doi.org/10.2478/ijcm-2023-0002

777. Une caractéristique de la cybercriminalité[2038] est qu'elle peut être effectuée à distance de n'importe où dans le monde, souvent l'emplacement du délit est difficile à détecter. Cela en fait un délit transnational[2039]. Selon l'ONU, un délit pour être considéré comme transnational doit remplir l'une des conditions suivantes : elle est commise dans plusieurs états ou dans un état, mais sa planification et sa préparation ont lieu dans un autre état ou sont impliquées dans un groupe criminel ayant des activités dans plusieurs états ou ayant des conséquences dans plusieurs états.[2040]

Qu'il s'agisse de la compétence de prescrire, de juger ou d'exécuter, toutes ces compétences sont fondées sur le principe du territoire[2041]. Un État ne peut appliquer son cadre législatif sur le territoire d'une autre nation[2042], comme le souligne la Cour suprême des États-Unis dans l'affaire The American Banana Company v. United Fruit Company, 213 U.S. 347, 356 (1909) : « La légalité ou l'illégalité d'une action doit être déterminée par la loi du pays dans lequel elle est commise ».[2043]

En 2000, le virus Love Bug a été créé aux Philippines et s'est propagé rapidement sur Internet dans le monde entier, affectant environ 45 millions d'utilisateurs dans plus de 20 pays[2044]. L'arrestation, la poursuite et la condamnation du créateur ont été difficiles, étant donné qu'à l'époque son action ne constituait pas un délit aux Philippines[2045].

La détermination de la compétence en matière de cybercriminalité relève un problème à la lumière de deux questions : quel pays est responsable de l'infraction ? Quel tribunal du pays a la compétence pour s'intéresser et gérer en conséquent ce délit ?[2046]

[2038] S.G. Isra, "*Cyber-Terrorism Definition Patterns and Mitigation Strategies : A Literature Review",* International Journal of Science and Research (IJSR), vol.6(1), 2017. pp. 180–186, – selon le Conseil Européen, la cybercriminalité couvre toutes les activités criminelles menées sur Internet. https ://www.ijsr.net/archive/v6i1/ART20163936.pdf

[2039] S.W. Brenner, *Cybercrime Jurisdiction*, Crime, Law and Social Change, vol.46, issue4-5, 2006. p.189-206 https ://www.ojp.gov/ncjrs/virtual-library/abstracts/cybercrime-jurisdiction#0-0

[2040] B.J. Holland, "*Transnational Cybercrime: The Sark Web*", in M. Knosrow, *Encyclopedia of Criminal Activities and the Deep Web,* IGI Global Scientific Publishing*,* 2020, p.108-128 https ://doi.org/10.4018/978-1-5225-9715-5.ch007

[2041] Tatarinov, M. (2021). THE TERRITORIAL JURISDICTION PRINCIPLES IN THEORETICAL AND COMPARATIVE LAW ASPECTS., 1, 8-11. https ://doi.org/10.18572/1812-3910-2021-1-8-11.

[2042] *United Nations Convention Against Transnational Organized Crime, Article 4* ("*Protection of Sovereignty*"), United Nations, 2000. http ://www.uncjin.org/Documents/Conventions/dcatoc/final_documents_2/convention_eng.pdf

[2043] *American Banana Co. v. United Fruit Co*., 213 U.S. 347 (1909). https ://supreme.justia.com/cases/federal/us/213/347/

[2044] M. Erbschloe, *Lessons from Love Crimes*, Information Systems Security*,* vol.*9*(6), 2001. p.1–9. https ://doi.org/10.1201/1086/43298.9.6.20010102/30986.5

[2045] M. Goodman, *The Emerging Consensus on Criminal Conduct in Cyberspace*, International Journal of Law and Information Technology, vol.10, 2002. p.139-223. https ://www.researchgate.net/publication/249242613_The_Emerging_Consensus_on_Criminal_Conduct_in_Cyberspace

[2046] L.Xiaobing, Q. Yongfeng, *Research on Criminal Jurisdiction of Computer Cybercrime*, ScienceDirect, 2018.

778. Réglementation législative transnationale. Au niveau européen, le premier traité international à coordonner les législations nationales en matière de cybercriminalité est la Convention sur la cybercriminalité, également connue sous le nom de Convention de Budapest, qui est entrée en vigueur le 1er juillet 2004[2047]. Sur 27 États membres, 26 l'ont ratifiée, renforçant ainsi la coopération internationale. L'article 22 est appelé « compétence » et stipule que chaque partie concernée est tenue de prendre les mesures législatives nécessaires pour établir sa compétence à l'égard des infractions présumées et se consulte en vue de parvenir à un dénominateur commun afin de choisir la juridiction la plus appropriée pour les poursuites[2048].

La présente Convention présente également quelques lacunes. Elle ne traite pas du problème de la détermination du lieu du crime (où les auteurs agissent, où les délits sont commis ou où les dommages sont ressentis)[2049]. Le paragraphe 2 de l'article 22 parle du principe de non-application de la compétence, ce qui peut conduire à un conflit judiciaire négatif dans lequel aucun pays ne revendique la compétence de la cybercriminalité et reste donc impuni[2050]. Le paragraphe 5 du même article prévoit la possibilité de se prévaloir de la compétence de plusieurs pays, contribuant ainsi à[2051] la création d'un conflit positif.

§2. DEEPFAKE, PROFILAGE COMPORTEMENTAL ET MANIPULATION DE L'INFORMATION

779. La complexité des deepfakes. Le mensonge et ses implications négatives ne sont pas nouveaux, mais ce qui inquiète vraiment à propos de deepfake, c'est la capacité à déformer la réalité, l'incapacité à la détecter et la vitesse avec laquelle elle peut être distribuée[2052].

[2047] M.A. O'Flynn, *Harmonisation and Cybercrime Jurisdiction: Uneasy Bedfellows?: An Analysis of the Jurisdictional Trajectories of the Council of Europe's Cybercrime Convention.* Queen Mary, University of London, 2015. http ://qmro.qmul.ac.uk/xmlui/handle/123456789/9548.

[2048] Conseil de l'Europe, *Convention on Cybercrime*, Budapest, 2001. https ://rm.coe.int/1680081561

[2049] "*International Initiative to Combat Cybercrime and Analysis of Jurisdictional Provisions in Convention on Cyber Crime*", Shodhganga. consulté le 20 juillet 2019. https ://shodhganga.inflibnet.ac.in/bitstream/10603/188821/9/7 chapter 5.pdf.

[2050] S. Brenner, *Cybercrime jurisdiction*, J. High Tech. L., 2004. https ://www.researchgate.net/publication/228796695_Cybercrime_jurisdiction

[2051] Ibid.

[2052] R. Chesney, Robert, D.K. Citron, *Deep Fakes : a Looming Challenge for Privacy, Democracy, and National Security*, 107 California Law Review 1753, 2019 available at SSRN : https ://ssrn.com/abstract=3213954 or http ://dx.doi.org/10.2139/ssrn.3213954

Un deepfake[2053] est une image artificielle ou une vidéo générée par un type spécial d'apprentissage automatique appelé « deep learning » [2054](d'où son nom). Les deepfakes sont créés par des algorithmes d'entraînement pour produire de fausses images qui ressemblent beaucoup aux vraies. Le deep learning, une branche du machine learning, utilise des algorithmes capables d'apprendre en analysant et en imitant une grande quantité de données complexes. De la même manière qu'un enfant apprend à reconnaître des objets après avoir interagi avec eux, les algorithmes apprennent après avoir analysé un grand volume de données complexes telles que des images, des sons, du texte[2055]. En d'autres termes, l'ordinateur peut imiter les fonctions cérébrales humaines telles que la mémoire et l'apprentissage, une découverte pour laquelle John J. Hopfield et Georfrey E. Hilton ont reçu le prix Nobel de physique en 2024[2056].

Actuellement, les appareils et dispositifs tels que les téléphones intelligents/smartphones, les tablettes, les appareils photo numériques ont conduit à une énorme augmentation du contenu des données disponibles, leur présence en ligne facilitant l'accès à ces données[2057]. De plus, les réseaux sociaux se sont avérés être la source principale du deepfake, favorisant le sensationnalisme et la prolifération des fausses nouvelles[2058].

780. L'algorithme des fausses nouvelles. Dans le cas des deepfakes, le processus implique deux algorithmes : l'un est entraîné à générer de fausses images et l'autre à détecter de fausses images. Ces algorithmes travaillent ensemble, chacun améliorant ses compétences, donc à la fin, l'algorithme qui crée de fausses images devient extrêmement efficace[2059].

781. Exemples de *deefake*. Le terme « deepfake » dans le sens d'informations artificielles est utilisé depuis 2017, lorsque Reddit crée un dossier appelé « deepfakes » dans lequel il télécharge diverses fausses vidéos[2060]. Les données analysées par le deep learning ne se limitent pas aux vidéos de personnes. Cette technologie peut traiter tout type de données, y compris des

---

[2053] A.F Gambín, A. Yazidi, A. Vasilakos, *et al., Deepfakes : current and future trends*, Artif Intell Rev, 2024. https ://doi.org/10.1007/s10462-023-10679-x

[2054] I.H. Sarker, *Deep Learning : A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions*, SN COMPUT. SCI, 2021. https ://doi.org/10.1007/s42979-021-00815-

[2055] Y. LeCun, Y. Bengio, G. Hinton, *Deep Learning*, Nature, 2015. p.436-444 https ://doi.org/10.1038/nature14539

[2056] M. Henninger A. Aupperlee, *Former CMU Faculty Geoffrey Hinton Awarded 2024 Nobel Prize in Physics*, Carnegie Mellon University, 2024.https ://news.pantheon.cmu.edu/stories/archives/2024/october/former-cmu-faculty-geoffrey-hinton-awarded-2024-nobel-prize-in-physics

[2057] Y. LeCun, Y. Bengio, G. Hinton, *Deep Learning*, Nature, 2015. (2015). p.436-444 https ://doi.org/10.1038/nature14539

[2058] J. Weedon, et al., "*Information operations and Facebook*", Facebook Security, 2017.

[2059] D.A. Coccomini, N. Messina, C. Gennaro, F. Falchi, *Combining EfficientNet and Vision Transformers for Video Deepfake Detection*, in S. Sclaroff, C. Distante, M. Leo, G. M. Farinella, F. Tombari(eds.), *Image Analysis and Processing — ICIAP 2022*, Springer International Publishing, 2022. p.219-229 https ://doi.org/10.1007/978-3-031-06433-3_19

[2060] L. Payne, "*Deepfake*", Encyclopedia Britannica, 2024. https ://www.britannica.com/technology/deepfake. consulté le 18 octobre 2024.

images et des vidéos avec des objets, du son et du texte[2061]. Par exemple, en 2020, le journaliste de OneZero Dave Gershgorn a rapporté la sortie sur le site OpenAI de « nouvelles » chansons créées artificiellement par des artistes célèbres comme Elvis Presley, Frank Sinatra et Jay-Z. [2062]Bien qu'elles aient été générées artificiellement, les chansons semblaient réelles, et la société de Jay-Z, Roc nation LLC, a intenté une action en justice contre YouTube pour supprimer ces morceaux[2063].

Un autre exemple de deepfake en évolution est le texte généré par l'IA, qui devient de plus en plus difficile à détecter, capable de créer un contenu faux mais très réaliste, ce qui menace gravement la confiance du public, la sécurité et la stabilité sociale[2064].

782. Une autre catégorie est le « cheapfake », qui implique l'utilisation de techniques simples, comme ralentir un discours ou accélérer une vidéo, pour modifier la perception d'un événement[2065]. Ces techniques peuvent avoir un impact significatif sur la façon dont les gens interprètent certaines informations[2066].

A. Deepfake et les médias synthétiques : une menace mondiale

783. Impossibilité de distinguer le vrai du faux. Les deepfakes sont un segment d'un phénomène plus large connu sous le nom de « média synthétique » ou de « contenu synthétique ». Il s'agit de toutes les formes de médias créées ou modifiées par l'intelligence artificielle et l'apprentissage automatique (IA/ML)[2067]. Les médias synthétiques sont définis comme tout contenu créé ou modifié par des moyens numériques ou artificiels avec une précision incroyable, la distinction entre les vraies et les fausses nouvelles étant extrêmement difficile à établir[2068].

[2061] M. Somers, *Deepfakes, explained*, MIT Management – Sloan School, 2020. https ://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained

[2062] D. Gershgorn, *Deepfake Music Is So Good It Might Be Illegal*, OneZero, 2020. https ://onezero.medium.com/deepfake-music-is-so-good-it-might-be-illegal-c11f9618d1f9

[2063] J. Goodrich, *Jay-Z's YouTube Strike Attempt Raises Audio Deepfakes Copyright Debate*, Screen Rant, 2020.

[2064] F. Abbas, A. Taeihagh, *Unmasking deepfakes : A Systematic review of deepfake detection and generation techniques using artificial intelligence,* Expert Systems with Applications, vol.252, partB, 2024. https ://www.sciencedirect.com/science/article/pii/S0957417424011266

[2065] D. Gerguri, *Cheapfakes,* Reasearch Gate, 2024. https ://www.researchgate.net/publication/384064482_Cheapfakes

[2066] M. Hameleers, *Cheap Versus Deep Manipulation: The Effects of Cheapfakes Versus Deepfakes in a Political Setting,* International Journal of Public Opinion Research, vol.36, nr.10, 2024. https ://www.researchgate.net/publication/378655334_Cheap_Versus_Deep_Manipulation_The_Effects_of_Cheapfakes_Versus_Deepfakes_in_a_Political_Setting

[2067] I. Kalpokas, *Problematising reality: the promises and perils of synthetic media*, SN Soc Sci. vol.1,no.1 2021. https ://pmc.ncbi.nlm.nih.gov/articles/PMC7649059/

[2068] I. Kalpokas, Ignas, *Call for Papers – Synthetic Media and Synthetic Reality: From Deepfakes to Virtual Worlds,* Research Gate, 2020. https ://www.researchgate.net/publication/340930120_Call_for_Papers_-_Synthetic_Media_and_Synthetic_Reality_From_Deepfakes_to_Virtual_Worlds

Bien sûr, les médias synthétiques ont des avantages importants, car elles peuvent créer du contenu de haute qualité, peuvent recréer des événements historiques, divers scénarios, peuvent contribuer de manière significative à l'innovation dans de vastes domaines.

Le principal problème avec ce type d'information est qu'en rendant si floue la frontière entre le réel et le faux, non seulement il transmet l'information, mais il façonne aussi la perception et l'interprétation de la réalité, manipulant la vérité, conduisant à l'érosion de la confiance dans les sources d'information ainsi qu'à influencer les décisions des individus, restructurer leur vie privée[2069]. Certaines voix soutiennent que, dans ce contexte, les deepfakes représentent une menace réelle pour la démocratie, compromettant la vie privée des individus avec des conséquences dévastatrices pour la réputation et la vie privée des individus[2070].

784. Augmentation inquiétante des deepfakes. En 2023, Sumsub Research[2071] a publié les résultats d'une recherche sur l'utilisation des deepfakes, faisant état d'une augmentation inquiétante (plus de 10 fois) du nombre d'incidents liés au *deepfake* entre 2022 et 2023[2072]. L'augmentation massive de ces incidents souligne la nécessité de développer des solutions de détection ainsi que de mettre en place des réglementations plus strictes pour prévenir l'utilisation abusive des deepfakes.

C'est une vérité généralement acceptée que les deepfakes (ainsi que d'autres technologies de l'époque actuelle) compromettent la vie privée et la réputation des gens, envahissant la vie privée. Il faut pour cela élaborer des cadres juridiques adaptés au développement naissant[2073]. À titre d'exemple, nous rappelons la décision de la Cour suprême du Canada dans l'affaire R.v.Jarvis de[2074] 2019, où la Cour souligne la nécessité de protéger le droit à la vie privée des individus à une époque où la technologie facilite la surveillance et la capture d'images sans consentement[2075].

[2069] J.C Kwitonda, S. Campbell, "*The Medium is the Massage/Message": Functions of Synthetic Media in Sense-Making Conditions*, in: K. Langmia(eds), *Black Communication in the Age of Disinformation,* Palgrave Macmillan, Cham, 2023. https ://doi.org/10.1007/978-3-031-27696-5_7

[2070] R. Chesney, D.K.Citron, *Deep Fakes : a Looming Challenge for Privacy, Democracy, and National Security* 107 California Law Review 1753, 2019. available at SSRN : https ://ssrn.com/abstract=3213954 or http ://dx.doi.org/10.2139/ssrn.3213954

[2071] Sumsub Research est une société privée, fondée en 2015, qui s'occupe de la vérification de l'identité numérique et de la conformité, fournissant des solutions pour la prévention de la fraude numérique. https ://sumsub.com

[2072] Sumsub, *Global Deepfake Incidents Surge Tenfold from 2022 to 2023*, Identity fraud report, 2023. https ://sumsub.com/fraud-report-2023/

[2073] K. Thomasen, S. Dunn, *Reasonable Expectations of Privacy in an Era of Drones and Deepfakes: Expanding the Supreme Court of Canada's Decision in R v Jarvis*, SSRN, 2021. https ://ssrn.com/abstract=3869764

[2074] Supreme Court Judgments – *R.v.Jarvis.* https ://decisions.scc-csc.ca/scc-csc/scc-csc/en/item/17515/index.do

[2075] S. Reisman, J. Silver, R. Shah, *R. v. Jarvis : privacy is not an "all-or-nothing" concept*, Ontario Bar Association, 2019. https ://www.oba.org/Sections/Privacy-Law/Articles/Articles-2019/May-2019/R-v-Jarvis-privacy-is-not-an-all-or-nothing%E2%80%9D-c#:~:text=The%20Supreme%20Court%20of%20Canada%E2%80%99s%20decision%20in%20R,filmed%20his%20female%20students%20with%20a%20hidden%20camera.

a). Utilisations bénéfiques de la technologie DeepFake

785. Les connotations positives des deepfakes. En général, ils ont une connotation négative, étant utilisés pour la désinformation, pour intimider, dénigrer, pour rabaisser[2076]. Cependant, il y a aussi des situations où les deepfakes sont utilisés à des fins positives[2077]. Par exemple, dans le domaine de l'éducation, cette technologie peut aider à livrer des leçons novatrices et passionnantes[2078]. Dans ce domaine, il peut offrir de nombreuses opportunités, stimuler l'intellect et en même temps éveiller et maintenir l'intérêt des apprenants[2079].

Un autre domaine est la médecine[2080]. Team Gleason[2081] aide les patients atteints de SLA[2082] à retrouver leur capacité à parler à l'aide d'algorithmes basés sur une technologie de fausse technologie profonde[2083]. Il peut également aider à établir des diagnostics, en particulier en radiologie, en détectant avec une grande précision les détails qui pourraient être omis par l'œil humain[2084].

L'art et la culture sont d'autres domaines qui peuvent bénéficier de la technologie deepfake, l'utilisation de l'IA dans l'art étant une caractéristique de l'art contemporain [2085]Ainsi, de véritables représentations d'artistes historiques peuvent être créées, ouvrant de nouveaux horizons créatifs, interpellant le public et modifiant la perception de la réalité[2086]. Un

---

[2076] J. Palfrey, "*Misinformation and disinformation*", Encyclopedia Britannica, 2024. https ://www.britannica.com/topic/misinformation-and-disinformation. Consulté le 18 octobre 2024.

[2077] A. Jaiman*, Deepfakes & Synthetic Media : Humanity at the Edge of an Uncanny Valley*, Kindle edition, 2022. https ://www.amazon.com/Deepfakes-aka-Synthetic-Media-Humanity-ebook/dp/B0B846YCNJ/

[2078] S. Erduran, "*Deepfakes and students" deep learning: A harmonious pair in science*?, Science, 2024. DOI :10.1126/science.adr8354

[2079] A. Evans, *Pros and Cons of Virtual Reality in the Classroom*, Chron Higher education, 2018. https ://www.chronicle.com/article/ProsCons-of-Virtual/243016 [https ://perma.cc/TN84-89SQ

[2080] G. Goth, *Medical Deepfakes Are the Real Deal Can deepfakes be beneficial in healthcare?*, MD+DI, 2022.https ://www.mddionline.com/artificial-intelligence/medical-deepfakes-are-the-real-deal

[2081] *Team Gleason* https ://teamgleason.org/

[2082] Sclérose latérale amyotrophique – affection neurologique grave, sans traitement curatif à l'heure actuelle. Au cours de la maladie, les patients perdent progressivement leur capacité neuro-musculaire, y compris la capacité de parler.

[2083] C. Hale, *Using AI and brain implants, researchers reconnect ALS patient with their lost voice*, Fierce Biotech, 2024.https ://www.fiercebiotech.com/medtech/using-ai-and-brain-implants-researchers-reconnect-als-patient-their-lost-voice

[2084] T.J. Carroll, M.C. Hurley, *When "Deep Faking" Results Means "Improving Diagnosis",* Radiology, vol.303, no.1, 2022. p.60-161. doi :10.1148/Radiol.212939 https ://pmc.ncbi.nlm.nih.gov/articles/PMC8961718/

[2085] K. Browne , *Who (or What) Is an AI Artist?,* Leonardo, vol.55, no.2, 2022 , p.130–134 doi: https ://doi.org/10.1162/leon_a_02092

[2086] Z. Hasnain, I P. Stojanović, *Aesthetics of deepfake-sphere of art and entertainment industry*, Facta Universitatis Series Visual Arts and Music, 2024, p.87-100.

exemple est l'animation d'œuvres célèbres, comme la Joconde, par le Samsung ai Center en collaboration avec l'Institut Skolkovo des sciences et de la technologie de Moscou[2087].

b). Pourquoi les deepfakes sont-ils un problème?

Si nous devions regarder les utilisations néfastes de la technologie deepfake, nous pouvons nous rappeler : exploitation, sabotage, distorsion, manipulation, érosion de la confiance, exacerber les divisions sociales, miner la sécurité publique, miner la diplomatie, miner le journalisme, mettre en danger la sécurité nationale[2088]. Certains d'entre eux sont illustrés ci-dessous

786. Manipulation de l'opinion publique. Un phénomène, la « post-vérité », caractérisé par la désinformation dans le but de manipuler l'opinion publique, est maintenant décrit. Ce phénomène de « fausses nouvelles » menace la démocratie, la vie privée et les principes fondamentaux de la liberté d'expression[2089]. Dans ce paysage d'expansion de l'information et de mondialisation, la capacité de discerner entre la vraie et la fausse information devient un défi, les rapports sur ce sujet indiquant que les humains n'ont qu'une capacité de 54% à identifier une arnaque[2090].

Si l'apprentissage profond a généralement des connotations positives[2091], les fausses profondeurs, qui reposent sur un modèle d'apprentissage profond, représentent un véritable problème de manipulation, de désinformation et de détérioration de la crédibilité, qui ébranle de manière cruciale la démocratie et la confiance du public. [2092]

787. Désinformation dans le but de tromper. Lors de la Conférence pour la vérité et la confiance en 2021, un thème central était la fausse profonde et son impact sur la vie privée des individus[2093]. Sur le plan personnel, cette forme de désinformation peut tromper les gens,

---

[2087] *Deepfake technology brings the Mona Lisa to life and it's too spooky, Russian researchers are blurring the lines between art and reality*, Dazed, 2019. https ://www.dazeddigital.com/art-photography/article/44678/1/deepfake-technology-brings-mona-lisa-to-life-too-spooky-russia-dali-einstein

[2088] R. Chesney, D.K. Citron, *Deep Fakes : a Looming Challenge for Privacy, Democracy, and National Security*, 107 California Law Review 1753, 2019. disponible au SSRN : https ://ssrn.com/abstract=3213954 or http ://dx.doi.org/10.2139/ssrn.3213954

[2089] Z. Zhou, et al., "*Edge intelligence: Paving the last mile of artificial intelligence with edge computing",* IEEE, vol.107, issu.8, 2019. https ://ieeexplore.ieee.org/abstract/document/8736011

[2090] S. Girgis, E. Amer, M. Gadallah, *Deep Learning Algorithms for Detecting Fake News in Online Text*, Research Gate, 2018. https ://www.researchgate.net/publication/328694360_Deep_Learning_Algorithms_for_Detecting_Fake_News_in_Online_Text

[2091] V.B. Kovač, D. Nome, A.R. Jensen, L. Skreland, *The why, what and how of deep learning: critical analysis and additional concerns,* Education Inquiry, 2023 p.1–17. https ://doi.org/10.1080/20004508.2023.2194502

[2092] C. Vaccari, A. Chadwick, *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News,* Social Media + Society, vol.6(1), 2020.

[2093] Truth and Trust online, Conference for truth and trust online, TTO, 2021. https ://truthandtrustonline.com/tto-2021/call-for-papers-2021/

générant du matériel compromettant avec des effets extrêmement négatifs sur la vie personnelle[2094]. Globalement, de fausses vidéos de dirigeants mondiaux peuvent générer des tensions politiques, voire inciter à la violence ou à la guerre. On se souvient de la vidéo parue sur BuzzFeed en avril 2018 avec le président Barack Obama adressant des mots offensants du Bureau Ovale à son adversaire, le président Trump[2095]. Cette vidéo, devenue virale, a été réalisée en utilisant l'intelligence artificielle en utilisant des techniques de plus en plus courantes, généralement appelées « faux profonds ». [2096]Les faux-semblants politiques profonds sont de plus en plus répandus, difficiles à détecter et peuvent avoir des implications profondes sur l'évolution de la démocratie et la qualité de vie personnelle des citoyens[2097].

Lors des élections françaises de 2017[2098], des tentatives ont été faites pour manipuler et modifier l'information afin d'empêcher l'élection du président Emmanuel Macron. Andrew Jenks, directeur des médias de Microsoft, a déclaré que les deepfakes poseraient un gros problème lors de l'élection présidentielle de 2024, et que l'atténuation de leur impact était une priorité[2099]. En politique, le contenu deepfake peut propager la désinformation à une échelle sans précédent, et les opposants qui cherchent à manipuler l'opinion publique peuvent utiliser ces techniques pour créer des images, des vidéos, des fichiers audios et du texte très réalistes[2100].

788. La génération des théories du complot. On soupçonne qu'en 2016, la Russie a tenté d'accroître les divisions sociales américaines, de promouvoir les théories du complot[2101], de

[2094] D.Gamage, et all., *The Emergence of Deepfakes and its Societal Implications: A Systematic Review*, Reasearch Gate, 2021. https ://www.researchgate.net/publication/355583941_The_Emergence_of_Deepfakes_and_its_Societal_Implications_A_Systematic_Review

[2095] Facebook, *Vous ne croirez pas ce que dit Obama dans cette vidéo, 2018.* https ://www.facebook.com/watch/?v=10157675129905329

[2096] C. Vaccari, A. Chadwick, *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News,* Social Media + Society, vol.6(1), 2020. https ://doi.org/10.1177/2056305120903408

[2097] W.L. Bennett, S. Livingston, *The disinformation order: Disruptive communication and the decline of democratic institutions*, European Journal of Communication, vol.33(2), 2018, p.122-139. https ://doi.org/10.1177/0267323118760317

[2098] A. Breeden et al., *Macron Campaign Says It Was Target of „Massive" Hacking Attack*, N.Y.Times, 2017. https ://www.nytimes.com/2017/05/05/world/europe/france-macronhacking.html [https ://perma.cc/4RC8-PV5G]

[2099] E. Strickland, *Content credentials will fight deepfakes in the 2024 elections*, IEEE Spectrum, 2023. https ://spectrum.ieee.org/deepfakes-election

[2100] C. Vaccari, A. Chadwick, *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News,* Social Media + Society, vol.6(1), 2020. https ://doi.org/10.1177/2056305120903408

[2101] J. White, *Dismiss, Distort, Distract, and Dismay: continuity and change in russian disinformation,* Inst. for European Studies ed., 2016. https ://www.ies.be/node/3689 [https ://perma.cc/P889-768J].

promouvoir un mouvement indépendantiste du Texas[2102] ou de protester contre l'islam à Houston[2103].

Il y a un siècle, l'attention a été portée sur le danger du bruit d'un tir de fusil dans un auditorium bondé[2104]. Actuellement, il s'estompe par rapport aux dommages qu'un deepfake peut causer[2105]. En 2015, une armée de trolls russes a tenté de provoquer le chaos en créant une catastrophe chimique en ligne en Louisiane et une épidémie d'Ébola à Atlanta[2106].

On soupçonne que deepfake a été impliqué dans le conflit diplomatique de 2017 entre l'Arabie Saoudite et le Qatar, en attribuant de fausses déclarations à l'émir du Qatar[2107].

789. Capacités minimales requises pour créer des deepfakes. Une autre préoccupation importante est que toute personne avec des compétences minimales peut créer des deepfakes, qui peuvent influencer massivement l'opinion publique dans des contextes sociaux, politiques ou sécuritaires, compromettre la réputation, harceler, frauder et affecter gravement la vie privée des personnes ciblées[2108]. Aujourd'hui, la création Deepfakes est plus disponible que jamais, avec des algorithmes d'IA existants permettant la création rapide et réaliste de fausses images ou vidéos sans programmation avancée ou connaissances informatiques[2109].

En conclusion, les faux profonds sont un réel danger, ayant une énorme capacité à manipuler la réalité. Les fausses rumeurs rattrapent parce que les gens ont besoin de « chaos », d'événements sensationnels, négatifs, pas nécessairement intéressés par les conséquences[2110]. L'effet cumulatif de ces faux messages conduit à l'incertitude et à la désorientation[2111], et dans ce chaos, les gens cessent de chercher la vérité[2112].

[2102] *The CalExit campaign in another illustration of Russian disinformation campaign. "Russian Trolls" Promoted California Independence*, BBC, 2017. http ://www.bbc.com/news/blogstrending-41853131 [https ://perma.cc/68Q8-KNDG].

[2103] S. Scott, *How Unwitting Americans Encountered Russian Operatives Online*, N.Y. Times, 2018. https ://www.nytimes.com/2018/02/18/us/politics/russian-operatives-facebooktwitter.html [https ://perma.cc/4C8Y-STP7].

[2104] *Schenck v. United States*, 249 U.S. 47, 52 (1919) https ://supreme.justia.com/cases/federal/us/249/47/

[2105] R. Chesney, D. K. Citron, *21st Century style Truth Decay : Deep Fakes and the Challenge for Privacy, Free expression, and National Security*, Maryland Law Review, vol.78, issue4, 2019. https ://digitalcommons.law.umaryland.edu/cgi/viewco

[2106] A. Chen, *The Agency*, N.Y. Times magazine., 2015), https ://www.nytimes.com/2015/06/07/magazine/the-agency.html [https ://perma.cc/DML3-6MWT].

[2107] K. Calamur, *Did Russian hackers Targeted Qatar ?*, Atlantic, 2017. https ://www.theatlantic.com/news/archive/2017/06/qatar-russian-hacker-fake-news/529359 [https ://perma.cc/4QAW-TLY8]

[2108] T. T. Nguyen, et al*., Deep learning for Deepfakes creation and image Detection: A Survey, Computer Vision and Image Understanding*, Elsevier, vol.223, 2022. https ://doi.org/10.1016/j.cviu.2022.103525

[2109] P. Mehta, et al., *Can deepfakes be created on a whim?*, Association for Computing Machinery, New York, 2023. p.1324-1334. https ://doi.org/10.1145/3543873.3587581

[2110] M.B. Petersen, M. Osmundsen, K. Arceneaux, *A „need for chaos" and the sharing of hostile political rumours in advanced democracies*. PsyArXiv Preprints, 2018. https ://psyarxiv.com/6m4ts/

[2111] W. Phillips, R.M. Milner, *The ambivalent internet: Mischief, oddity and antagonism online*, Polity, 2017.

[2112] P. Pomerantsev, *Inside Putin's information war,* Politico, 2015. https ://www.politico.com/magazine/story/2015/01/putin-russia-tv-113960

c). Lutte contre les deepfakes

Bien qu'il n'existe pas de solutions parfaites au problème des deepfakes et des fausses nouvelles, les experts explorent quelques pistes.

790. Implication des plateformes de réseaux sociaux. Par exemple, la vérification de l'information par les plateformes de médias sociaux, ainsi que l'utilisation de messages d'avertissement[2113], sont des mesures qui peuvent lutter contre la désinformation. Ces mesures peuvent être ajoutées à la mise en œuvre de campagnes d'éducation des utilisateurs, de discernement entre l'information correcte et la fausse information[2114]. Toutes ces mesures doivent toutefois être couronnées par des règlements appropriés qui protègent le droit à la vie privée contre les progrès rapides de la technologie[2115].

La technologie de l'intelligence artificielle (IA) pourrait jouer un rôle important dans la détection des deepfakes, car les algorithmes peuvent être formés pour identifier les signes subtils de falsification que l'œil humain ne peut pas percevoir.

791. Deepfake, catégorie de risque inacceptable. En juin 2024, le règlement sur l'intelligence artificielle (RIA) a été publié dans[2116] le Journal de l'Union Européenne. Il classe les systèmes d'IA en fonction de leur risque en 4 catégories : inacceptable, élevé, limité et minimal. Selon le mode d'utilisation, les deepfakes peuvent être classés soit comme à haut risque, soit comme inacceptables (s'ils sont utilisés à des fins de manipulation, de fraude, de désinformation, de harcèlement, de diffamation), ces derniers sont interdits (art. 5, par. 1) et sévèrement sanctionnés. Le règlement est entré en vigueur en août 2024 et les États membres disposent de deux ans pour se conformer à ces règles[2117].

[2113] K. Clayton, S. Blair, J.A. Busam, et al*., Real Solutions for Fake News? Measuring the Effectiveness of General Warnings and Fact-Check Tags in Reducing Belief in False Stories on Social Media*, Polit Behav, vol.42, 2020. p.1073–1095. https ://doi.org/10.1007/s11109-019-09533-0

[2114] J. Smith, G. Jackson, S. Raj, *Designing against misinformation*. Medium, 2017. retrieved 2018, from https ://medium.com/facebook-design/designing-against-misinformation-e5846b3aa1e2.

[2115] M.K.Land, J.D Aronson, *Human Rights and Technology: New Challenges for Justice and Accountability*, Annual Review of Law and social Science (Forthcoming), 2020. available at SSRN : https ://ssrn.com/abstract=3690635 or http ://dx.doi.org/10.2139/ssrn.3690635

[2116] Règlement (UE) 2024/1689 du Parlement Européen et du Conseil du 13 juin 2024 établissant des règles harmonisées en matière d'intelligence artificielle et modifiant les Règlements (CE) no 300/2008, (UE) 167/2013, (UE) no. 168/2013, (UE) no 2018/858, (UE) no. 2018/1139/2013 et (UE) 2019/2144 ainsi que les directives 2014/90/UE, (UE) 2016/797 et (UE) 2020/1828 (Règlement sur l'intelligence artificielle) (texte présentant de l'intérêt pour l'EEE). http ://data.europa.eu/eli/reg/2024/1689/oj

[2117]CNIL, *Entrée en vigueur du règlement européen sur l'IA : les premières questions-réponses de la CNIL,*2024. https ://www.cnil.fr/fr/entree-en-vigueur-du-reglement-europeen-sur-lia-les-premieres-questions-reponses-de-la-cnil

792. Le deepfake dans le Code pénal français. Compte tenu de l'évolution de la technologie, la France modifie l'article 226-8 du Code pénal, ciblant le deepfake, avec des sanctions extrêmement sévères[2118]. Depuis mai 2024, il est qualifié de délit et puni par le Code pénal (art. 226-8-1), protégeant ainsi le droit à l'image et au respect de la vie privée[2119]. La loi SREN[2120] renforce et étend également les compétences des autorités de l'ARCOM[2121] et de la CNIL[2122].

793. Nécessité d'une réglementation en Roumanie. Actuellement, la Roumanie n'a pas de législation spécifique pour deepfake. Cependant, il existe un projet de loi sur l'utilisation responsable de la technologie dans le contexte de ce phénomène[2123], qui a été soumis au vote du Parlement au début de l'année 2024 et qui a reçu au début du mois d'octobre 2024 un avis favorable de la Commission juridique, disciplinaire et des immunités[2124]. L'autorité de régulation chargée de vérifier la diffusion sur Internet/les médias de contenus deepfake est le Conseil National de l'Audiovisuel (CNA)[2125], qui, conformément à la loi susmentionnée, peut faire appel à l'aide de l'Institut National de recherche et développement en informatique – ici.

B. Big Data et profilage comportemental

794. Des quantités massives de données en ligne. « Nous n'avions pas de meilleurs algorithmes, juste plus de données »[2126], a déclaré Peter Norvig, directeur de recherche chez Google il y a plus de 10 ans, synthétisant la valeur colossale du Big Data[2127].

[2118] M. Musson, J. Moulin, L. Josserand*, Loi SREN : renforcement des pouvoirs de l'ARCOM et de la CNIL au service de la protection des internautes*, Dalloz. https ://www-dalloz-fr.docelec.u bordeaux.fr/documentation/Document ?id=ACTU0222966

[2119] Le Code pénal, section 2 : de l'atteinte à la représentation de la personne (articles 226-8 à à 226-9) https ://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000049567458

[2120] LOI n° 2024-449 du 21 mai 2024 visiteur à sécuriser et à réguler l'espace numérique. https ://www.legifrance.gouv.fr/jorf/id/JORFTEXT000049563368

[2121] ARCOM – une autorité publique indépendante pour la régulation (a le pouvoir légal) et la supervision des communications audiovisuelles et numériques, créée en 2022.

[2122] CNIL – autorité administrative indépendante, instituée par la loi informatique et libertés du 6 janvier 1978.

[2123] Chambre des députés, *Projet de loi sur l'utilisation responsable de la technologie dans le contexte du phénomène Deepfake,* 2023.PL-x No 471/2023

[2124] Parlement roumain, Chambre des députés, *Avis sur le projet de loi sur l'utilisation responsable de la technologie dans le contexte du phénomène Deepfake,* Commission juridique, disciplinaire et des immunités, 2024. https ://cdep.ro/comisii/juridica/pdf/2024/av471_23.pdf

[2125] Conseil national de l'audiovisuel, loi et code Loi n° 504/2002 sur l'audiovisuel et décision n° 220/2011 relative au code de réglementation du contenu audiovisuel, CNA.https ://cna.ro/-Legea-audiovizualului-si-Codul-.html

[2126] H. Cimen, E. J. Palacios-Garcia, M. Kolaek, N. Cetinkaya, J. C. Vasquez, J. M. Guerrero, "*Smart-building applications : deep learning-based, real-time Load Monitoring"*, IEEE Industrial Electronics Magazine, vol.15, no.2, 2021. p.4-15 https ://ieeexplore.ieee.org/document/9310683

[2127] A. McAfee, E. Brynjolfsson, T.H. Davenport, D. Patil, D. Barton,*"Big Data : The management revolution",* Harvard Business Review vol.90(10) , 2012. https ://pubmed.ncbi.nlm.nih.gov/23074865/

Le Big Data, terme à la mode, entouré d'ambiguïté, n'a pas de définition unique et généralement acceptée, ce qui stimule de nombreux débats[2128]. Il n'existe pas de définition unique pour les mégadonnées, mais le terme est généralement utilisé pour décrire des quantités massives de données produites et collectées sous diverses formes. Presque tout ce que font les individus génère des données – recherches en ligne, réseaux sociaux, portails web, blogs, partage de médias et transmission quotidienne d'informations au gouvernement, aux entreprises et aux réseaux sociaux, ou même simplement le port d'un smartphone – toutes ces données (intentionnellement ou non) génèrent d'énormes quantités d'informations sur les individus, ils sont conservés dans les journaux de transactions[2129].

a). Big Data, IA et la vie privée

795. Le big data, carburant de l'IA. La relation entre le big data et l'IA est bidirectionnelle, se potentialisant mutuellement. Les mégadonnées contiennent de grandes quantités de données brutes qui, avec l'aide de l'IA, sont exploitées et transformées en connaissances utiles[2130]. Dans le sens inverse des mégadonnées, qui fournissent une source d'information énorme et diversifiée à l'IA, elle se développe et la rend plus efficace. En ce sens, l'IA et le big data sont étroitement liés[2131].

D'une manière lyrique, on peut dire que le Big Data est le carburant qui alimente l'intelligence artificielle, soutenant et améliorant ses performances[2132]. Inspirée par la célèbre déclaration de Kant[2133], l'IA sans données est dépourvue de contenu et les données sans algorithmes sont aveugles.

[2128] A. De Mauro, M. Greco, M. Grimaldi, *What is Big Data ? A consensual Definition and a Review of Key Research Topics*, Research Gate, 2014. https ://www.researchgate.net/publication/265775800_What_is_Big_Data_A_Consensual_Definition_and_a_Review_of_Key_Research_Topics

[2129] Z. Jin , W. Dietmar, M. Feicheng ,*The impact of big data on research methods in information science*, Data and Information Management, vol.7, Issue2, 2023. https ://doi.org/10.1016/j.dim.2023.100038. (https ://www.sciencedirect.com/science/article/pii/S2543925123000128)

[2130] D. Yanqing, J. S. Edwards, Y. K Dwivedi, *Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda,* International Journal of information Management, vol.48, 2019. https ://doi.org/10.1016/j.ijinfomgt.2019.01.021.(https ://www.sciencedirect.com/science/article/pii/S0268401219300581)

[2131] L. Jin Li, Ziwei YE, Cighting Zhang*, Study on the interaction between big data and artificial intelligence,* Systems Research and Behavioral Science, vol.39, issue3, 2022. p.641-648 https ://doi.org/10.1002/sres.2878

[2132] A. Gandomi, M. Haider, *Beyond the hype : Big Data concepts, Methods, and Analytics,* International Journal of information Management, vol.35, Issue2, 2015. p.137-144 https ://doi.org/10.1016/j.ijinfomgt.2014.10.007. (https ://www.sciencedirect.com/science/article/pii/S0268401214001066)

[2133] I. Kant, *Critique of Pure Reason*, Guyer P, Wood AW,(eds) Cambridge University Press , 1998. (”[T]houghts without content are empty, intuitions without concepts are blind.”) https ://www.cambridge.org/core/books/critique-of-pure-reason/259C2355B74458963EC285F53337AAF0

796. Les algorithmes de l'IA utilisant le Big Data peuvent influencer le comportement et les décisions des individus,[2134] telles que les décisions financières[2135], les recommandations d'embauche[2136] ou les diagnostics médicaux,[2137] avec un impact majeur sur la qualité de vie. Si ces systèmes ne sont pas conçus ou gérés correctement, des problèmes de partialité ou de discrimination peuvent survenir, en particulier lorsque les données sur lesquelles ils sont fondés ne sont pas diversifiées ou gérées correctement[2138].

À mesure que l'Internet des objets[2139] (IoT) étend le réseau dans l'environnement physique et les espaces personnels[2140], **la quantité de données créées et collectées augmente de façon exponentielle**. Ces données deviennent de plus en plus envahissantes dans la vie personnelle des individus. L'utilisation de ces données par les systèmes d'IA pose des défis importants en termes de confidentialité, de sécurité de l'information, de sécurité et de confiance individuelles[2141] et de protection des données. Avec d'énormes quantités de données personnelles disponibles, telles que l'analyse du comportement en ligne, des interactions sociales ou de la localisation physique, il existe un risque de surveillance excessive ou de surveillance involontaire[2142].

797. Le défi du respect de la vie privée dans ce contexte a soulevé et continue de soulever de nombreuses préoccupations[2143]. Une mesure de protection a été la mise en œuvre du projet P3P (Privacy Preferences Project)[2144] dans le cadre de l'initiative World Wide Web Consortium

---

[2134] D. Yanqing, J. S. Edwards, Y. K Dwivedi, *Artificial intelligence for decision making in the era of Big Data – evolution, challenges and research agenda,* International Journal of information Management, vol.48, 2019. https ://doi.org/10.1016/j.ijinfomgt.2019.01.021.(https ://www.sciencedirect.com/science/article/pii/S0268401219300581)

[2135] L. Zhang, I. Pentina, Y. Fan, *Who do you choose? Comparing perceptions of human vs robo-advisor in the context of financial services,* J. Serv. Marché, 2021.

[2136] D.L. Diab, S.Y. Pui, M. Yankelevich, S. Highhouse, *Lay perceptions of selection decision aids in US and non-US samples,* Int. J. Sel. Assess., vol.19, 2011. pp. 209-216

[2137] C. Castelluccia, D. Le Métayer, *Understanding algorithmic decision-making: opportunities and challenges,* EU publications, 2019. https ://doi.org/10.2861/536131.

[2138] H. Mahmud, A.K.M. Najmul Islam, S.A. Ishtiaque, K. Smolander, *What influences algorithmic decision-making? A systematic literature review on algorithm aversion*, Technological Forecasting ans Social Change, Vol.175, 2022. https ://www.sciencedirect.com/science/article/pii/S0040162521008210#bib0184

[2139] S. Greengard, "*Internet of Things",* Encyclopedia Britannica, 2024. https ://www.britannica.com/science/Internet-of-Things. Consulté le 7 octobre 2024.

[2140] L. Xiaofuet et all., *Generalisable Model Development for fluid-nerter Integrated amortissages Devices*, Mechanism and machine Theory, vol.137, 2019. https ://doi.org/10.1016/j.mechmachtheory.2019.03.010. (https ://www.sciencedirect.com/science/article/pii/S0094114X18316161)

[2141] F. Allhoff, A. Henschke, *The Internet of Things : Foundational ethical issues*, Internet of Things, vol.1–2, 2018. https ://doi.org/10.1016/j.iot.2018.08.005. (https ://www.sciencedirect.com/science/article/pii/S2542660518300532)

[2142] A. Karale, *The Challenges of IoT Addressing Security, Ethics, Privacy and Laws*, Internet of Things, vol.5, 2021. https ://doi.org/10.1016/j.iot.2021.100420. (https ://www.sciencedirect.com/science/article/pii/S2542660521000640)

[2143] S.Misra, et all., *Security Challenges and Approaches in Internet of Things*, Springer Briefs in Electrical and Computer Engineering. Cham.: Springer, 2016.
Google Scholar

[2144] L. F. Cranor, S. Egelman, S. Sheng, A. M. McDonald, A. Chowdhury, *P3P deployment on websites*, Electronic commerce Research and applications, vol.7, issue3, 2008. https ://doi.org/10.1016/j.elerap.2008.04.003.

(W3C), qui a malheureusement pris fin prématurément en raison du manque d'acceptation et d'adoption par les utilisateurs[2145]. La lourdeur de la mise en œuvre des mesures de sûreté souligne la nécessité de cadres juridiques solides ainsi que de protocoles de sécurité solides[2146].

798. Big data : domaines d'activité. Aujourd'hui, les mégadonnées sont utilisées avec succès dans des domaines tels que la santé, le marketing, la production, la distribution, le secteur public[2147]. L'un des aspects déterminants des Big Data est l'utilisation d'énormes quantités de données, générant des algorithmes pour découvrir des schémas et des corrélations[2148]. Cette première étape de « découverte » est suivie de l'application d'un nouvel algorithme pour agir sur la base des corrélations trouvées. Ce processus, également connu sous le nom d'apprentissage automatique, permet au système d'identifier des critères pertinents en analysant les données sans intervention humaine directe.

Un exemple très visible de notre époque est la façon dont **le** volume et **la diversité des informations dans au niveau des Big Data** affinent la recherche et l'enseignement supérieur, offrant des opportunités infinies. Cependant, ces avantages s'accompagnent de préoccupations concernant la confidentialité et la protection des données personnelles[2149]. Les experts dans ce domaine soulignent la nécessité de réglementations plus claires pour la protection de ces données. Par exemple, le Règlement général sur la protection des données (RGPD) de l'Union Européenne aborde une perspective globale de l'utilisation des données personnelles, en ne sachant pas clairement quel est le destinataire des données de recherche numériques (qui a le droit de les recevoir : le sujet, l'utilisateur, le chercheur ?)[2150].

799. Risques pour la vie privée. Les mégadonnées, tout comme l'intelligence artificielle, les NBIC, l'Internet des objets,[2151] sont considérés comme de nouveaux risques pour la vie privée de l'individu, leur vie privée et leur vie privée, et leur développement permanent

(https ://www.sciencedirect.com/science/article/pii/S1567422308000185)

[2145] I. Reay, S. Dick, J. Miller, „*A Large-Scale Empirical Study of P3P Privacy Policies: Stated Actions vs. Legal Obligations*", ACM Transactions on the Web (TWEB) vol.3, issue2, 2009. p.6.
Web of Science ®Google Scholar

[2146] C. Maple, *Security and privacy in the inyternet of things*, Journal of Cyber Policy, vol.*2*(2), 2017, p.155–184. https ://doi.org/10.1080/23738871.2017.1366536

[2147] J. Koo, G. Kang, Y.G. Kim, *Security and Privacy in Big Data Life Cycle: A Survey and Open Challenges*, Sustainability, vol.12, 2020. https ://doi.org/10.3390/su122410571

[2148] A.A. Rehma, M.J. Awan, I. Butt, *Comparison and Evaluation of Information Retrieval Models*, VFAST transactions on Software Engineering, vol.*6*(1), 2018. p.7–14. https ://doi.org/10.21015/vtse.v13i1.496

[2149] T. Omer, J. Polonetsky, *Big Data for All : Privacy and User Control in the Age of Analytics*, NJTIP, vol.11, iss.5, 2013. p.239. https ://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1

[2150] D. Florea, S. Florea, *Big Data and the Ethical Implications of Data Privacy in Higher Education Research*. Sustainability vol.12, 2020. https ://doi.org/10.3390/su12208744

[2151] L. Portmesss, S. Tower, *Data barns, ambient intelligence and cloud computing: the tacit epistemology and linguistic representation of Big Data*, Ethics Inf Technol, vol.17, 2015. p.1–9 https ://doi.org/10.1007/s10676-014-9357-2

nécessite l'adoption et la mise à jour périodique des règles régissant l'utilisation des données personnelles[2152].

Un autre élément distinctif est la reconversion des données, c'est-à-dire l'utilisation des données collectées à des fins différentes de celles d'origine[2153]. Cette capacité à traiter et à réorienter les données a des implications importantes pour la protection des données et la vie privée des utilisateurs, soulevant des questions sur la transparence des processus et l'utilisation des informations personnelles[2154].

800. Avantages. Les bénéfices de cette technique dans des domaines tels que la médecine sont colossaux, facilitant la recherche et aidant à faire des découvertes significatives.[2155] L'accord conclu entre le plus grand fournisseur de soins de santé américain et Google (le projet « Nightingale »)[2156] sur la fourniture de renseignements personnels aux utilisateurs de Google à des fins de recherche en santé en[2157]est un exemple. En l'absence d'une législation adéquate, le projet suscite des protestations, des éclaircissements[2158] et une enquête fédérale[2159].

801. Réglementation relative à la collecte et au traitement des données à caractère personnel. La législation sur la protection des données est fondée sur le principe de la minimisation des données[2160], ce qui signifie que les organisations doivent limiter la collecte et le traitement des données à ce qui est strictement nécessaire aux fins définies et ne les conserver que aussi longtemps que nécessaire. Le règlement général sur la protection des données (RGPD) souligne que les données personnelles doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire » aux fins pour lesquelles elles sont traitées.

[2152] Larcier, *La vie privée à l'heure de la société du numérique, Section 2 - Les enjeux sociétau des libertés à la non-discrimination, à la dignité et à la justice sociale*, Dalloz, 2019. p.24-30 *https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=LRVP*

[2153] X. Wang,Q. Duan, M Liang, *Understanding the process of data reuse: An extensive review*. J Assoc Inf Sci Technol., vol.72, 2021. p.1161-1182. https ://doi.org/10.1002/asi.24483

[2154] J.J Boté-Vericad, M. Térmens, "*Reusing data: technical and ethical challenges*." Desidoc Journal of Library & information Technology, vol.39, no6, 2019. p.329-337 https ://www.webofscience.com/wos/woscc/full-record/WOS:000503418300009

[2155] L. Marelli, G. Testa, I. Van Hoyweghen, *Big Tech platforms in health research: Re-purposing big data governance in light of the General Data Protection Regulation's research exemption*, Big Data & Society, vol.8(1), 2021. https ://doi.org/10.1177/20539517211018783

[2156] R. Copeland, S.E. Needleman, *Le projet Google Nightingale lance une enquête fédérale*, The Wall Street Journal, 2019. disponible à l'adresse suivante : https ://wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867

[2157] J. Cohen, *Google, Ascension Data Partnership Sparks Federal Probe*, Modern Healthcare, 2019. disponible à l'adresse suivante : https ://modernhealthcare.com/information-technology/google-ascension-data-partnership-sparks-federal-probe

[2158] E. Shaukat, *Our partnership with Ascension*, Google Cloud Blog, 2019. available at : https ://cloud.google.com/blog/topics/inside-google-cloud/our-partnership-with-ascension

[2159] R.Copeland, S.E Needleman, *Google's "project nightingale" triggers federal inquiry*, Wall Street Journal, 2019. available at: https ://wsj.com/articles/behind-googles-project-nightingale-a-health-data-gold-mine-of-50-million-patients-11573571867

[2160] P. de Hert, V. Papakonstantinou, "*The New General Data Protection Regulation: Still a Sound System for the Protection of Individuals?",*Computer Law & Security Review, vol.32, issue 2, 2016, p.179-194.

Bien que le RGPD garantisse une utilisation éthique et responsable des données, il fait face à des incertitudes dans la recherche en santé[2161]. Ainsi, en 2021, le Conseil Européen de la protection des données apporte des éclaircissements sur l'application cohérente du RGPD dans le domaine de la recherche en santé[2162].

b). Le profilage comportemental compromet-il le libre arbitre ?

802. D'autre part, le profilage comportemental devient un élément clé, car l'analyse des données peut révéler des détails sur le comportement, les préférences et les habitudes de consommation des utilisateurs.[2163] En recueillant et en analysant les données disponibles sur les réseaux sociaux[2164], les entreprises peuvent acquérir une compréhension approfondie des utilisateurs, sans se limiter à des enquêtes représentatives ou à des échantillonnages[2165]. Cette approche est fréquemment utilisée dans le marketing et la publicité, où les données collectées, y compris à partir des réseaux sociaux ou de l'historique des achats, sont traitées pour adapter les offres et les messages aux consommateurs[2166].

803. Interférences dans la vie privée. L'utilisation des Big Data pour comprendre, décoder et prédire le comportement humain crée une inférence, ce qui entraîne de nombreux défis juridiques en matière de confidentialité des données personnelles[2167]. De plus, faire un profilage comportemental basé sur des algorithmes augmente le risque de discrimination, et peut amplifier les préjugés existants[2168]. Le Règlement général sur la protection des données

---

[2161] I. Marelli, E. Lievevrouw, I. Van Hoyweghen, *Fir for purpose? The GDPR and the governance of European digital health,* Policy Studies, vol.41(5) , 2020, p.447–467. https ://www.tandfonline.com/doi/full/10.1080/01442872.2020.1724929

[2162] European Data Protection Board, *EDPB Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, adopted on 2 February 2021. https ://edpb.europa.eu/sites/edpb/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf

2163 M.U. Tariq, M. Babar, M. Poulin, A.S. Khattak, M.D. Alshehri, S. Kaleem, Human Behaviour Analysis Using Intelligent Big Data Analytics. Front. Psychol. vol.12, 2021.
https ://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.686610/full

2164 J. Blomberg, Twitter and Facebook Analysis: It's Not Just for Marketing Anymore, vol.309. Denver, 2012.

2165 V. Mayer-Schönberger, K. Cukier, Big Data : a Revolution That Will Transform How We Live, Work, and Think, John Murray, 2013. p. 129. Mayer-Schönberger et Cukier discutent de l'analyse des données massives et de la réaffectation des données, soulignant comment les entreprises collectent et utilisent de grandes quantités d'informations pour extraire de nouveaux modèles et perspectives.

2166 S. Stieglitz, M. Mirbabaie, B. Ross, C. Neuberger, Social media Analytics – Challenges in Topic Discovery, data collection, and data preparation, International Journal of information Management, vol.39, 2018. https ://doi.org/10.1016/j.ijinfomgt.2017.12.002.
https ://www.sciencedirect.com/science/article/pii/S0268401217308526

2167 L. Floridi, Group Privacy – A Defense and an Interpretation, SSRN Electronic Journal, 2017. https ://www.researchgate.net/publication/352161872_Group_Privacy_-_A_Defense_and_an_Interpretation

2168 N. Eder, Privacy, Non-Discrimination and Equal Treatment: Developing a Fundamental Rights Response to Behavioural Profiling, in M.Ebers, M. Cantero Gamito, Algorithmic Governance and Governance of Algorithms,Springer, 2021.https ://www.researchgate.net/publication/346147259_Privacy_Non-

(RGPD), conçu pour protéger les données personnelles, offre une protection limitée contre les inférences[2169] ainsi que des recours insuffisants pour les contester ou contester des décisions prises en leur nom[2170].

En approfondissant le sujet, nous pouvons définir le principe d'inférence comme le concept utilisé pour inférer de nouvelles informations basées sur l'analyse de données existantes. Ces dernières peuvent être des informations apparemment insignifiantes, mais à partir desquelles des données sensibles peuvent être déduites[2171]. Au cours des dernières années, il y a eu beaucoup de débats sur la question de savoir si ce principe relevait de la protection juridique du droit à la vie privée[2172]. La question a fait l'objet de nombreuses jurisprudences de la Cour de justice des Communautés européennes[2173] [2174].

Il y a des voix qui défendent le principe de l'inférence et qui soutiennent qu'il ne compromet pas la vie privée[2175] des individus, arguant que si les renseignements sur lesquels les inférences sont fondées sont obtenus légalement, le droit à la vie privée n'est pas violé.

804. Conclusion. En conclusion, le Big Data apporte à la fois des risques et des opportunités. Si certaines voix soulèvent la question que l'émergence et le développement de cette technologie peuvent marquer[2176] la fin du concept de vie privée il existe également des contre-opinions selon lesquelles, correctement réglementées et dotées de cadres juridiques solides, les mégadonnées peuvent se transformer en un bouclier de protection de la vie privée et des droits individuels[2177].

Discrimination_and_Equal_Treatment_Developing_a_Fundamental_Rights_Response_to_Behavioural_Profilin g

2169 GDPR, Art. 9, Processing of special categories of personal data. https ://gdpr.eu/article-9-processing-special-categories-of-personal-data-prohibited/?cn-reloaded=1

2170 S. Wachter, B. Mittelstadt, A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI, Research Gate, 2018. https ://www.researchgate.net/publication/328257891_A_Right_to_Reasonable_Inferences_Re-Thinking_Data_Protection_Law_in_the_Age_of_Big_Data_and_AI

2171 S. Barocas, H. Nissenbaum, "Big Data's End Run around Anonymity and Consent", Book of Anonymity, 2014, p.55 https ://www.cs.cornell.edu/~shmat/courses/cs5436/barocas-nissenbaum.pdf

2172 S. Wachter, *Data protection in the age of big data*, Nature Electronics, vol.2, 2019. p.6-7 https ://doi.org/10.1038/s41928-018-0193-y

2173 Judgment of the Court (Second Chamber) of 20 December 2017. *Peter Nowak v. Data Protection Commissioner. Case C-434/16.* https ://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CJ0434

2174 Judgment of the Court (Grand Chamber) of 29 June 2010. *European Commission v The Bavarian Lager Co. Ltd. Case C-28/08 P*. https ://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62008CJ0028

2175 J.T. Mayence, „*Inferences and the Right to Privacy",* The Journal of Value Inquiry, 2022. https ://philpapers.org/archive/MAIIAT-2.pdf

2176 I. Rubinstein, *Big data : The end of privacy or a new beginning?,* International Data Privacy Law. vol.3, 2013,p.74-87. https://academic.oup.com/idpl/article-abstract/3/2/74/709082?redirectedFrom=fulltext

2177 A. Mantelero, *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, Springer-T.M.C. Asser Press, 2022. https ://www.researchgate.net/publication/380165902_Beyond_Data_Human_Rights_Ethical_and_Social_Impact_Assessment_in_AI_Sringer-TMC_Asser_Press_The_Hague

c) L'attentat terroriste contre *Charlie Hebdo* – un nouveau paradigme juridique pour le profilage comportemental

Le profilage comportemental[2178] en tant qu'instrument de protection de l'ordre public[2179], tel qu'il est compris depuis les révélations faites par le lanceur d'alerte américain Edward Snowden[2180], n'est pas une création *ex nihilo* de la période postérieure au 11 septembre 2001[2181] et n'a, en réalité, presque rien en commun avec le profilage classique de l'auteur d'un crime[2182], construit à partir de l'image de la « scène du crime »[2183] et utilisant des déductions sur ce qui s'est passé avant, pendant ou après l'événement[2184]. L'équilibre entre le besoin de sécurité de la société et la vie privée individuelle semble négociable. Concrètement, ce type de

[2178] R. Perray, « Données à caractère personnel. – Champ d'application territorial de la réglementation relative à la protection des données personnelles », *JurisClasseur Administratif*, fasc. 274-13, LexisNexis - « le profilage comprend tout rassemblement d'informations à propos d'un individu (ou d'un groupe d'individus) en vue de seulement évaluer leurs caractéristiques ou leurs comportements et, ce faisant, les placer dans une catégorie ou un groupe spécifique déterminé(e) par exemple au regard de la capacité à effectuer une tâche, de leurs centres d'intérêts ou leurs comportements probables. »

[2179] Nous avons abordé la redéfinition de la notion d'« ordre public » dans le contexte de l'évolution technologique dans l'introduction de la présente étude, dans la section « Le nouveau rapport entre ordre public et vie privée ». Après les attentats du 11 septembre 2001, la redéfinition de la notion d'ordre public prend une dimension radicalement nouvelle : la logique de prévention et de neutralisation des risques terroristes a justifié le passage d'une protection ponctuelle et réactive à un modèle structurel de sécurité basé sur la collecte massive de données, l'interconnexion des bases d'informations, le profilage et l'analyse algorithmique des comportements. Dans ce contexte, l'« ordre public » ne désigne plus seulement la sécurité physique des personnes et des institutions, mais inclut également la sécurité de l'information et l'anticipation des menaces par des outils numériques intrusifs, ce qui déplace le centre de gravité de la relation entre l'État et l'individu. L'équilibre entre les libertés individuelles (vie privée, protection des données, liberté d'expression et de circulation) et les impératifs de sécurité nationale est reconfiguré en faveur d'une surveillance préventive étendue, soulevant la question de savoir si le nouvel ordre public « post-11 septembre » ne devient pas, en soi, un vecteur de normalisation du profilage généralisé et d'érosion des garanties classiques de la vie privée.

[2180] Compte tenu de l'impact juridique qu'ont eu les preuves présentées par Snowden dans l'espace public concernant la surveillance de masse et le profilage comportemental coordonnés par des organismes étatiques, d'autres références peuvent être trouvées dans le présent mémoire, en particulier dans la Partie II, au Chapitre : « Intrusion gouvernementale : du mandat de perquisition à l'interception des conversations », Section « Interception des communications téléphoniques, dans le contexte européen ».

[2181] Les révélations d'Edward Snowden en 2013 ont montré que les programmes de surveillance ne visent pas seulement les personnes suspectes, mais opèrent à l'échelle mondiale dans le but d'intercepter, de filtrer et de profiler en masse : collecte massive de métadonnées et de contenus (PRISM, Upstream), accès direct ou privilégié aux flux de communications internationales et coopération systématique entre les agences de renseignement et les grands fournisseurs privés de services numériques. Ces pratiques permettent de dresser des profils détaillés des individus (réseaux sociaux, déplacements, préférences, vulnérabilités), d'une manière opaque, difficile à contrôler juridiquement et incompatible avec la notion de « suspicion individualisée » sur laquelle reposent, en principe, le droit pénal et les mécanismes classiques d'ingérence dans la vie privée. Les révélations de Snowden ont ainsi servi de déclencheur à une réévaluation, y compris dans la jurisprudence européenne, des limites admissibles de la surveillance de masse et de l'obligation des États de mettre en place des garanties efficaces contre le profilage généralisé.

[2182] M. Agrapart-Delmas, *De l'expertise criminelle au profilage. Une psychocriminologue sur la piste des grands meurtriers et en guerre contre les pseudo-profilers*, Favre, Lausanne, 2001.

[2183] B. Bouloc, *Droit pénal général*, 29e éd., Paris, Dalloz, coll. Précis, 2025, p.38 – « À partir des constatations effectuées par l'identité judiciaire scènes du crime) on infère le profil de la personnalité de l'auteur. »

[2184] M. Bénézech, T. Toutin, P. Le Bihan, H. Mathieu, « Les composantes du crime violent : une nouvelle méthode d'analyse comportementale de l'homicide et de sa scène », in *Annales médico-psychologiques*, vol. 164, no. 10, 2006, p.828-833.

profilage[2185] du potentiel auteur commence avant la commission du « crime »[2186], le profilage étant déjà réalisé même si le comportement criminel soupçonné par les services de renseignement ou les autorités judiciaires n'est jamais mis en œuvre ou s'il n'y a même pas eu le moindre risque qu'il se concrétise.

La première forme de cadre juridique concernant l'échange de données obtenues par les services de renseignement américains et européens[2187] grâce à l'interception et à la surveillance technique des citoyens a été créée par des accords signés dès 1968[2188], mais les attentats ont accéléré et légitimé le passage d'un profilage axé sur certaines catégories de suspects[2189] à un profilage quasi généralisé de la population[2190], dans un premier temps des passagers des vols entrant sur le territoire des États-Unis[2191]. Au nom de la prévention du terrorisme, en invoquant un droit fondamental à la sécurité[21922193], qui est en réalité discutable de ce point de vue[2194], la vérification préalable des passagers, l'interconnexion des bases de données et l'évaluation algorithmique des risques ont été institutionnalisées en tant que mécanismes structurels de

[2185] J. McCulloch, D. Wilson, *Pre-crime: Pre-emption, Precaution and the Future*, Routledge, Abingdon/New York, 2016.
[2186] L. Zedner, « Pre-crime and post-criminology? », *Theoretical Criminology*, vol. 11, n° 2, 2007, p.261-281 – „Conventionally, crime is regarded principally as harm or wrong and the dominant ordering practices arise post hoc. In the emerging pre-crime society, crime is conceived essentially as risk or potential loss, ordering practices are pre-emptive and security is a commodity sold for profit."
[2187] « Germany 'not a surveillance state', says Angela Merkel », The Telegraph, 19 juillet 2013, disp. en ligne : https://www.telegraph.co.uk/news/worldnews/europe/germany/10190946/Germany-not-a-surveillance-state-says-Angela-Merkel.html
[2188] L'impact provoqué par ces divulgations d'informations considérées comme des secrets d'État, qui n'auraient dû en aucun cas être rendues publiques, a remis en question l'efficacité des accords signés en 1968 concernant l'échange de données sur les personnes surveillées, et tous ces accords ont été annulés. Après l'adoption en Allemagne de la loi G10 en 1968, qui autorise la restriction du secret de la correspondance et des communications à des fins de sécurité nationale par le biais d'interceptions autorisées et contrôlées, le cadre réglementaire de la surveillance n'est pas resté isolé au niveau national, mais a été intégré dans un programme de coopération entre les services de renseignement allemands, français, du Royaume-Uni et des États-Unis, coopération qui comprenait des mécanismes de partage des informations obtenues par interception et surveillance technique, consolidant ainsi un système transnational d'échange de données au nom de la sécurité nationale. Pour plus de détails, voir la partie II, au chapitre : « Intrusion gouvernementale : du mandat de perquisition à l'interception des conversations » – Partenariats d'échange de données entre la France, l'Allemagne, les États-Unis et le Royaume-Uni.
[2189] C.J. Bennett, C. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge (Mass.), 2006.
[2190] D. Lyon, *Surveillance After September 11*, Polity Press, Cambridge, 2003.
[2191] M.B. Salter (dir.), *Politics at the Airport*, University of Minnesota Press, Minneapolis, 2008.
[2192] X. Dupré de Boulois, « Existe-t-il un droit fondamental à la sécurité ? », in *Revue des droits et libertés fondamentaux* (RDLF), 2018, chron. n° 13. Dans cet article, l'auteur réalise une analyse qui conclut que la sécurité ne peut être un droit fondamental : « L'exigence de protection de la sécurité des personnes est donc très largement prise en compte dans les différentes branches du droit. Cependant elle est rarement formulée à travers l'affirmation d'un droit fondamental à la sécurité. »
[2193] V. Champeil-Desplats, « Les enjeux normatifs de la fondamentalisation du droit à la sécurité », in M. Touillier (dir.), *Le Code de la sécurité intérieure, artisan d'un nouvel ordre ou semeur de désordre*, Dalloz, coll. « Les sens du droit », 2017, p.81.
[2194] P. Bon, *Prévention du terrorisme et protection des droits fondamentaux*, AIJC 2002 Économica PUAM 2003 p.352. Peu après les attentats du 11 septembre 2001, certaines voix doctrinales se sont élevées pour se demander si nous assistions à l'émergence d'un droit fondamental à la sécurité. À cet égard, la question de l'existence d'un tel droit fondamental se retrouve dans l'ouvrage du professeur français Pierre Bon.

gouvernance de la mobilité[2195], préfigurant l'apparition du dispositif juridique relatif aux données du dossier passager (PNR)[2196]. On trouve des débats timides dans la littérature juridique[2197] concernant l'interconnexion des bases de données de l'UE avant l'apparition de ce régime de collecte massive des données des passagers.

Le moment qui a encouragé la mise en place d'un cadre juridique européen pour le profilage comportemental est lié à l'attentat contre les journalistes du magazine Charlie Hebdo le 7 janvier 2015[2198]. Cette attaque a agi comme un accélérateur normatif, critiqué par certains auteurs pour la rapidité et l'incohérence excessives de la législation[2199], d'un paradigme en matière de sécurité qui était déjà en train de se former. En France, elle a légitimé l'adoption de la loi sur les renseignements du 24 juillet 2015[2200], qui étend massivement les possibilités de

[2195] S. Peyrou-Bartoll (dir.), *Nouvelles technologies et droit européen : quel droit face à la disruption numérique ?*, Mare & Martin, Paris, 2022.

[2196] Le cadre juridique PNR désigne l'ensemble des dispositions qui habilitent les autorités compétentes à collecter, traiter, stocker et utiliser les données contenues dans les dossiers de réservation de voyage (Passenger Name Record) – données d'identification, coordonnées, itinéraire, mode de paiement, attribution des sièges, informations sur les bagages, préférences et mentions opérationnelles – en vue de prévenir, détecter et poursuivre les infractions terroristes et autres formes de criminalité grave. Ce régime confère à des données initialement techniques et administratives une fonction probatoire et d'évaluation des risques, en les intégrant dans un dispositif sécuritaire transnational et en instaurant un modèle de contrôle anticipatif de la circulation des personnes. Son importance résulte, d'une part, de son insertion au cœur de la coopération policière et judiciaire européenne et, d'autre part, du fait qu'il organise, à l'échelle structurelle, le profilage algorithmique des passagers.

[2197] J.-M. Delarue, « L'Europe des fichiers. Dialogues des juges, des policiers, des autorités administratives indépendantes », in *Le dialogue des juges. Mélanges en l'honneur du président Bruno Genevois*, Dalloz, 2009, p.233-304; F. Rolin, S. Slama, « Les libertés dans l'entonnoir de la législation antiterroriste », in *AJDA*, 2006, p.975-982.

[2198] L'attaque contre la rédaction de Charlie Hebdo, commise par les frères Chérif et Saïd Kouachi au nom d'Al-Qaïda dans la péninsule arabique, visait explicitement à sanctionner les caricatures du Prophète et le symbole « blasphématoire » de la liberté d'expression. Douze personnes ont été tuées et une vague de violences coordonnées (dont l'attaque de l'Hyper Cacher) s'est déclenchée en trois jours, révélant les failles majeures du dispositif antiterroriste français. Sur le plan social, « Je suis Charlie » a cristallisé une solidarité massive, mais aussi de profondes divisions sur la laïcité, l'offense religieuse, l'islamophobie et les limites de la satire. Sur le plan politique, cet événement a accéléré le discours sur l'importance de la sécurité nationale et a préparé le terrain pour la loi sur le renseignement du 24 juillet 2015 (extension de la surveillance), le renforcement de la coopération entre les services et une tolérance accrue à l'égard des outils intrusifs (interceptions étendues, capteurs de données, algorithmes de détection).

[2199] C. Lazerges, H. Henrion-Stoffel, « Politique criminelle, renseignement et droits de l'homme. À propos de la loi du 24 juillet 2015 relative au renseignement », in *Revue de science criminelle et de droit pénal comparé*, 2015, p.761-775 - « L'élaboration à un rythme effréné de projets de loi ne permet pas une évaluation complète et rigoureuse du droit en vigueur, afin que soit établi un bilan de la pertinence et de l'efficacité des mesures existantes. »

[2200] La loi n° 2015-912 du 24 juillet 2015 relative au renseignement organise pour la première fois dans un cadre unitaire l'activité des services de renseignement en France, en introduisant le Livre VIII « Du renseignement » dans le Code de la sécurité intérieure.

→ consacre le renseignement comme une politique publique de l'État, liée à la défense des intérêts fondamentaux de la nation ;

→ définit des finalités précises mais larges (sécurité nationale, prévention du terrorisme, de la grande criminalité organisée, de la prolifération des armes, des cyberattaques majeures, des ingérences étrangères, etc.) ;

→ autorise des techniques spéciales : interception des communications, accès aux données de connexion, géolocalisation, installation de dispositifs de surveillance audio-vidéo, accès aux systèmes informatiques, dispositifs de capture et de collecte de données en temps réel ;

→ prévoit la possibilité d'utiliser des « traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste », appliqués aux données de connexion fournies par les opérateurs (article L.851-3)

surveillance administrative[2201] (interceptions, dispositifs de collecte de données, algorithmes de détection) sous contrôle quasi juridictionnel, avec un impact direct sur la vie privée, le secret de la correspondance et la liberté de la presse. Cette loi très critiquée[2202] a contribué à normaliser l'état d'urgence et à renforcer le droit pénal et administratif du « suspect potentiel », qui n'a commis aucun délit, pour lequel il n'existe aucune indication qu'il en commettra un, mais qui doit néanmoins être surveillé[2203]. Au niveau de l'UE, le contexte post-Charlie Hebdo a débloqué l'adoption de la directive (UE) 2016/681 sur les données PNR[2204], instaurant le contrôle systématique préalable des passagers et le profilage algorithmique de la mobilité comme outil structurel de la coopération policière. Le discours sur la sécurité européenne s'aligne sur les tendances post-11 septembre : extension de la conservation et de l'interconnexion des bases de données, facilitation de l'accès aux métadonnées et assouplissement des normes relatives aux autorisations de surveillance, avec pour effet cumulatif de déplacer le centre de gravité de la protection des droits individuels vers la gestion préventive des risques par le profilage[2205].

En 2025, l'ordre juridique régissant l'activité des services de renseignement en France repose sur la loi n° 2015-912 du 24 juillet 2015. C'est sur cet acte normatif qu'a été construit tout un édifice législatif dont l'objectif déclaré est de protéger les intérêts individuels et étatiques tout en préservant la vie privée[2206]. En réalité, certains auteurs évoquent le danger de voir apparaître un « droit du renseignement »[2207], qui masquerait un recul catégorique du droit à la

---

→ instaure un régime d'autorisation administrative (décision du Premier ministre après avis), avec des durées déterminées et un contrôle spécialisé (organisme de contrôle et possibilité de saisir la juridiction administrative suprême) ;

→ établit un régime spécifique pour la surveillance internationale des communications.

[2201] La présente étude fournit davantage de détails sur la vision du droit français en matière de surveillance administrative dans la Partie II, Titre II. Intrusion de l'État dans la vie privée. Synchronisation du droit pénal avec l'évolution technologique.

[2202] B. Warusfel, « La (re)définition d'un droit du renseignement », in J. Alix, O. Cahn (dir.), *L'hypothèse de la guerre contre le terrorisme*, Dalloz, 2017; B. Warusfel, « Le contentieux de la sécurité nationale », in *Annuaire droit de la sécurité et de la défense*, 2018; R. Parizot, « Surveiller et prévenir… à quel prix ? », in *JCP* 2015, doctr. 1077; C. Lazerges, H. Henrion-Stoffel, « Politique criminelle, renseignement et droits de l'homme. À propos de la loi du 24 juillet 2015 », in *RSC*, 2015, p.761.

[2203] S. Desmoulin-Canselier, D. Le Métayer*, Décider avec les algorithmes. Quelle place pour l'Homme, quelle place pour le droit ?*, Dalloz, coll. « Les sens du droit », 2020; A. Garapon, J. Lassègue*, Justice digitale. Révolution graphique et rupture anthropologique*, PUF, 2018.

[2204] Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention, la détection, l'enquête et la poursuite des infractions terroristes et des formes graves de criminalité, JOUE L 119, 4 mai 2016, p.132-149.

[2205] L. Bonelli, « Les caractéristiques de l'antiterrorisme français : parer les coups plutôt que panser les plaies », in D. Bigo, L. Bonelli, T. Deltombe (dir.), *Au nom du 11 septembre… Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, 2008, p.168-187.

[2206] Une déclaration de principe à ce sujet est reprise dans la loi mentionnée à l'article 801-1 du Code de la sécurité intérieure : « Le respect de la vie privée, dans toutes ses composantes, notamment le secret des correspondances, la protection des données à caractère personnel et l'inviolabilité du domicile, est garanti par la loi. L'autorité publique ne peut y porter atteinte que dans les seuls cas de nécessité d'intérêt public prévus par la loi, dans les limites fixées par celle-ci et dans le respect du principe de proportionnalité. »

[2207] B. Warusfel, « La (re)définition d'un droit du renseignement », in J. Alix, O. Cahn (dir.), *L'hypothèse de la guerre contre le terrorisme*, Dalloz, 2017, p.151-160.

vie privée[2208]. Dans le cadre de la mission d'évaluation parlementaire de 2020[2209], la loi sur les activités des services de renseignement est décrite comme représentant un cadre unifié et stable de la politique publique en matière de collecte d'informations, qui ne nécessite que des ajustements et non un changement de modèle. La simple activité de collecte d'informations « porte en lui le germe d'une menace permanente sur les citoyens, procédant de moyens technologiques les plus sophistiqués, à la mesure des progrès de l'informatique et des communications électroniques ».[2210]

Dans cette évolution des dix dernières années, depuis les attentats terroristes jusqu'à aujourd'hui, la loi n° 2017-1510 du 30 octobre 2017 (SILT)[2211] joue un rôle intermédiaire décisif, mettant formellement fin à l'état d'urgence, mais transfère dans le droit commun des instruments initialement exceptionnels – périmètres de protection, mesures individuelles de contrôle administratif[2212] et de surveillance, fermeture de lieux de culte, perquisitions administratives – « le législateur en convient, qui, conscient de la dimension peu ordinaire des mesures en cause »[2213]. Concrètement, cette loi consolide un modèle de prévention administrative axé sur la gestion anticipée des risques sur la base de soupçons[2214], complémentaire aux techniques de collecte d'informations mises en place en 2015[2215]. Alors

[2208] F. Johannès, « Commentaire de l'avis de la CNCDH du 16 avril 2015 relatif au projet de loi sur le renseignement », in *Les grands avis de la CNCDH commentés*, Paris, Dalloz, janv. 2016 ; C. Castets-Renard, « Quels liens établir entre les USA et l'UE en matière de vie privée et protection des données personnelles ? », in *Dalloz IP/IT*, 2016, n° 3, p.115 ; W. Maxwell, C. Zolynski, « Protection des données personnelles », in *Recueil Dalloz*, 2022, n° 39, p.2002.

[2209] L. Kervran, J.-M. Mis, *Rapport d'information sur l'évaluation de la loi n° 2015-912 du 24 juillet 2015 relative au renseignement*, Assemblée nationale, 15e législature, n° 3069, 10 juin 2020. Ce rapport montre que le Premier ministre a autorisé l'utilisation du premier algorithme dans le processus de collecte d'informations, conformément aux exigences de cette loi, le 12 octobre 2017. Au moment de la rédaction du rapport, trois algorithmes étaient opérationnels, mais les résultats devaient être améliorés : « D'après les informations qui ont été transmises à la mission d'information, les trois algorithmes ont fourni des résultats intéressants. Ils sont néanmoins moins probants qu'ils ne pourraient l'être eu égard au champ relativement limité des données qui peuvent faire l'objet de l'algorithme. Les données pouvant nourrir l'algorithme sont en effet limitées aux seules données de connexion ne révélant aucun contenu, à l'exception donc des URL. Les membres de la mission d'information ont donc envisagé plusieurs pistes de réflexion permettant d'améliorer l'efficacité des algorithmes. »

[2210] Y. Mayaud, « Terrorisme – Prévention – Renseignement », *Répertoire de droit pénal et de procédure pénale*, Dalloz, févr. 2020, actualisation févr. 2025.

[2211] Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme, JORF n°0255 du 31 octobre 2017, texte n° 2.

[2212] Les mesures individuelles de contrôle administratif, instituées en droit commun, reprennent la logique de l'obligation de ne pas quitter son domicile prévue par l'article 6 de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence : elles permettent de placer une personne sous contrainte territoriale et sous obligation de se présenter, non pas sur la base d'une condamnation pénale ou d'une mesure préventive dans le cadre d'une procédure pénale, mais en raison d'une suspicion sérieuse liée à une menace pour la sécurité publique. Ce transfert d'un instrument exceptionnel dans l'ordre juridique ordinaire marque le déplacement du centre de gravité de la réaction pénale vers la gestion administrative anticipative du risque.

[2213] Y. Mayaud, *op. cit.*

[2214] A. Ashworth, L. Zedner, *Preventive Justice*, Oxford, Oxford University Press, 2014.

[2215] M. Gaye-Palettes, « Coup de frein en demi-teinte pour le traitement algorithmique des URL », *Actualité juridique Droit administratif*, 2025, p.1760.

que la doctrine condamne à l'unisson « Le jour sans fin de l'état d'urgence »[2216] et soutient qu'en réalité, l'utilité de l'état d'urgence et l'invocation de la loi de 1955 dans le but de lutter contre le terrorisme sont pratiquement nulles, pour reprendre une expression imagée : « la montagne a accouché d'une souris »[2217]. En réalité, cette procédure administrative[2218], qui était déjà autorisée par le droit français, vise à surveiller et à profiler la population en l'absence d'un contrôle classique, judiciaire[2219]. D'autre part, les rapports parlementaires[2220] soulignent la complémentarité fonctionnelle et efficace entre la police administrative et la police judiciaire.

Le droit roumain ne consacre pas de mécanisme comparable à celui mis en place en France, par lequel la compétence de prendre des mesures individuelles restrictives des droits, sur la base d'un simple soupçon et en dehors d'un cadre pénal, est transférée de l'autorité judiciaire à l'organe administratif. La Roumanie reste, sur le plan formel, dans un modèle où la restriction individuelle sévère de la liberté de circulation est liée soit à la procédure pénale, soit à un régime exceptionnel limité, tandis qu'en France, il existe un ensemble de mesures administratives permanentes qui visent à la surveillance individuelle à long terme, en dehors de toute poursuite ou condamnation pénale.

Le cadre réglementaire français est complété en 2021 par la loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement, qui transpose dans l'activité quotidienne les dispositifs introduits en 2015, en particulier les traitements automatisés[2221], confirmant le passage définitif à un droit commun de la surveillance préventive. Estimant qu'en réalité, le législateur promulgue des lois abusives qui diminuent la protection de la vie privée sous prétexte de lutter contre le terrorisme, la doctrine a cette fois-ci tenu des propos acerbes : « Le terrorisme a bon dos. (...) Une fois de plus, la peur l'emporte sur la raison.

[2216] S. Hennette-Vauchez, S. Slama, « Le jour sans fin de l'état d'urgence », in *Dalloz actualité*, 9 juin 2017 ; R. de Massol de Rebetz, « Marianne's liberty in jeopardy? A French analysis on recent counter-terrorism legislation », in *European Review of Public Law*, 2020 ; S. Hennette-Vauchez, S. Slama, « Harry Potter au Palais-Royal ? La lutte contre le terrorisme comme cape d'invisibilité de l'état d'urgence et la transformation de l'office du juge administratif », in *Les Cahiers de la justice*, Dalloz, 2017/2, p.281; O. Cahn, J. Leblois-Happe, « Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme : *perseverare diabolicum* », in *Actualité juridique Pénal*, 2017, n° 11, p.468.

[2217] S. Hennette-Vauchez, S. Slama, « Harry Potter au Palais-Royal ? La lutte contre le terrorisme comme cape d'invisibilité de l'état d'urgence et la transformation de l'office du juge administratif », in *Les Cahiers de la justice*, 2017, n° 2, p.281-298.

[2218] M. Sirinelli, « Police administrative et terrorisme : quel contrôle juridictionnel ? », in *Revue française de droit administratif*, 2013, p.1024.

[2219] S. Hennette-Vauchez, S. Slama, « Harry Potter au Palais-Royal ?… », *op. cit.* : « (...)Les mesures que la mise en application de la loi du 3 avril 1955 a permis de prendre n'ont pas ciblé spécifiquement les réseaux terroristes. Bien plutôt, celles-ci ont été dirigées vers des objectifs en lien avec la surveillance, la discipline et la mise au pas de divers groupes perçus comme menaçant, de manière générale, l'ordre public. »

[2220] M.-P. Daubresse, *Rapport d'information n° 348 (2019-2020) – La loi renforçant la sécurité intérieure et la lutte contre le terrorisme : 2 ans après – bilan et propositions*, Sénat, Commission des lois, 26 févr. 2020.

[2221] Y. Mayaud, *op. cit*. : « La prévention du terrorisme ne saurait être sans des moyens à la disposition des services de renseignement pour détecter et stopper le plus en amont possible les projets de nature terroriste. Le recours à des fichiers a toujours été une pratique reconnue, surtout depuis l'entrée de l'informatique dans le système, avec des possibilités quasiment illimitées d'exploitations et de croisements, mais non sans risques pour les libertés. »

Une fois de plus, nos libertés sont rognées au nom de la sécurité. Une fois de plus, l'illégalité d'autrefois devient la légalité d'aujourd'hui »[2222].

Dans le même contexte d'interaction entre le droit pénal, la vie privée et la technologie, il convient de mentionner la loi n° 2023-380 relative aux Jeux Olympiques de Paris 2024[2223], qui autorise, à titre expérimental[2224] et pour une durée limitée[2225], créant ainsi un précédent décisif[2226], l'utilisation de systèmes de vidéosurveillance augmentés par des algorithmes[2227] pour la détection automatique de situations considérées comme potentiellement risquées[2228] (mouvements de panique, objets abandonnés, intrusions dans des zones réglementées, etc.), justifiée explicitement par la nécessité de prévenir les attentats et de gérer rapidement les menaces graves dans les espaces publics très fréquentés[2229]. Ce projet expérimental est innovant dans l'espace juridique européen, il a été prolongé jusqu'en 2027 et ne sera très probablement jamais abandonné dans le cadre de la procédure pénale[2230]. Bien qu'il ait eu un impact social et juridique assez fort, les résultats présentés dans les rapports de suivi[2231] sont assez négatifs : « un total de 1 552 signalements dont 657 sont des faux positifs. Ainsi, 42 % des signalements sont, soit une erreur d'appréciation du traitement, soit une situation qui n'a pas d'intérêt particulier pour les opérateurs vidéo »[2232].

Dans la même logique préventive, tout aussi critiquée[2233], la loi n° 2024-850 relative à la prévention des ingérences étrangères a été adoptée dans le but de renforcer la surveillance

---

[2222] A. Denizot, « Quand l'instruction ministérielle illégale fait la loi », in *Revue trimestrielle de droit civil*, 2021, p.949.

[2223] Loi n° 2023-380 du 19 mai 2023 relative aux Jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions, JORF n° 0116 du 20 mai 2023, texte n° 3.

[2224] R. Chatellier, « Des premières caméras à l'expérimentation des algorithmes : un panorama du développement territorial, technologique et de l'encadrement juridique de la vidéosurveillance », in *Revue française d'administration publique*, 2024/1, n° 185, p.223-235.

[2225] S. Bouvier, « Vidéosurveillance augmentée : de l'expérimentation à la pérennisation », in *Jurisport*, 2025, n° 262, p.38.

[2226] L. Laref, M. Laref (dir.), *Surveillance*, Paris, Dalloz, coll. « Themes & commentaires – Actes », 1re éd., 28 nov. 2024, p.300.

[2227] H. Adda, « IA et vidéoprotection : quelles solutions pour les collectivités ? », in *Actualité juridique Collectivités territoriales*, 2025, p.152.

[2228] CNIL, « Caméras "augmentées" ou algorithmiques dans l'espace public », site de la CNIL, contenu actualisé en 2024.

[2229] Art. 10, alin. 1: « À titre expérimental et jusqu'au 31 mars 2025, à la seule fin d'assurer la sécurité de manifestations sportives, récréatives ou culturelles qui, par l'ampleur de leur fréquentation ou par leurs circonstances, sont particulièrement exposées à des risques d'actes de terrorisme ou d'atteintes graves à la sécurité des personnes, les images collectées au moyen de systèmes de vidéoprotection autorisés sur le fondement de l'article L. 252-1 du code de la sécurité intérieure ou au moyen de caméras installées sur des aéronefs autorisées sur le fondement du chapitre II du titre IV du livre II du même code, dans les lieux accueillant ces manifestations et à leurs abords ainsi que dans les véhicules et les emprises de transport public et sur les voies les desservant, peuvent faire l'objet de traitements algorithmiques. »

[2230] N. Blanchard, « Un nouveau projet de loi "olympique" déposé », in *Jurisport*, 2025, n° 264, p.6.

[2231] Ministère de l'Intérieur, « Expérimentation, en temps réel, de caméras "augmentées" », actualité du 7 février 2025, disponible sur le site du Ministère de l'Intérieur.

[2232] S. Bouvier, *op. cit.*

[2233] F. Duverger, « Lutter contre les ingérences étrangères envers le système démocratique. Analyse comparée des lois française et hongroise », in *Revue des droits et libertés fondamentaux,* RDLF 2025, chron. n° 28 ; A. Denizot,

des activités d'influence et de la circulation de l'information, en vue d'identifier à un stade précoce les formes de manipulation, de déstabilisation ou de soutien indirect au terrorisme et autres menaces contre les intérêts fondamentaux de l'État. La motivation derrière l'adoption de cette loi est précisément l'impact que la technologie a eu sur le droit et sur la manière dont les données privées peuvent être consultées et manipulées. Le professeur Beaussonie[2234] identifie plusieurs sources à l'origine de cette loi, parmi lesquelles l'ingérence étrangère dans le processus électoral, un phénomène rencontré dans la plupart des pays européens.

C. Manipulation de l'information, un danger réel pour le droit à la vie privée

La manipulation de l'information est un phénomène complexe de plus en plus présent dans la société contemporaine, qui influence les perceptions, les décisions et les actions des individus et des groupes collectifs[2235].

805. L'impact du phénomène de désinformation. Le Centre d'analyse, de prévision et de stratégie (CAPS) en France a déjà produit une étude montrant que la manipulation de l'information est une menace pour les démocraties[2236]. Il est clair que les législations nationales et européennes ont commencé à accorder une importance particulière au phénomène de la désinformation, en essayant de trouver des solutions pour prévenir les *fake news* ou même les punir. La manipulation de l'information à travers les médias numériques (messagerie instantanée, blogs, forums, réseaux sociaux, presse, etc.) est un danger actuel et imminent, aussi important que la cybercriminalité, le cyber-espionnage, le piratage informatique[2237], etc. Le programme de sécurité et de défense élaboré par la France pour la période 2008-2020[2238]

« Ingérence étrangère : la France sur les pas du Nicaragua », in *Revue trimestrielle de droit civil*, RTD civ., Dalloz, 2024, n° 4, p.991.

[2234] G. Beaussonie, M. Segonds, « À propos de la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France », in *Revue de science criminelle et de droit pénal comparé*, 2024, p.857 : « "Macron leaks", "Qatargate", "pseudo-invasion des punaises de lit", "étoiles de David peintes sur les murs de la capitale", "affaire Pegasus", "Portal Kombat" : mêlant déstabilisation des processus électoraux et démocratiques, désinformation, manipulation de l'opinion, cyberattaques, ou encore recherche de la participation d'anciens dirigeants politiques aux conseils d'administration de grands groupes étrangers, telles sont les sources "réelles" du droit de la lutte contre l'ingérence étrangère. »

[2235] *« Manipulation à travers les médias »*, Magazine Intelligence (blog), 2010. https://intelligence.sri.ro/manipulare-prin-mass-media/.

[2236] J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, *Les Manipulations de l'information: un défi pour nos démocraties*, rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, Paris, 2018.

[2237] S. Taillat, A. Cattaruzza, D. Danet, A Colin (ed.), *La Cyberdéfense - Politique de l'espace numérique*, Collection U, 2018. https://shs.cairn.info/la-cyberdefense--9782200634223?lang=fr

[2238] Le Livre blanc sur la défense et la sécurité nationale 2008, publié le 17 juin 2008, est un Livre blanc chargé de définir une stratégie globale de défense et de sécurité pour la France de 2009 à 2020. Le programme, élaboré par une commission, servira de base aux deux prochains projets de loi de programmation militaire, qui seront votés par le Parlement français.

indique clairement que la protection du cyberespace est l'une des priorités et un domaine d'importance stratégique. Par la suite, ce type de politique publique a été promu au sein de l'Union Européenne, et il s'agit aujourd'hui d'un thème quasi-présent dans les plans stratégiques communautaires.

a). Réseaux sociaux, forme de gouvernance hybride[2239]

806. De la manipulation classique aux fausses nouvelles et à la désinformation. À l'ère de la technologie, où l'accès à l'information est rapide et facile, la capacité des individus à faire la distinction entre les vraies et les fausses informations est devenue un défi de taille. La manipulation de l'information est une stratégie ancienne, mais les développements technologiques ont rendu possibles de nouvelles dimensions et méthodes d'application, en particulier réseaux sociaux[2240]. Dans ce contexte, la manipulation de l'information peut prendre diverses formes, des fake news à la désinformation, en passant par la propagande numérique ou les deepfakes[2241].

807. Le rôle des réseaux sociaux. À ce stade, les sites de réseautage social ne sont plus simplement un moyen de satisfaire le narcissisme des utilisateurs[2242], mais forme de gouvernance juridico-institutionnelle hybride qui « exerce un pouvoir énorme en dehors des limites de la réglementation ou d'autres contraintes traditionnelles »[2243]. La position dominante des sites de réseaux sociaux, même par rapport à la législation étatique ou européenne, est signalée par la majorité des avis doctrinaux récents : « appliqué aux "réseaux", le paradoxe juridique est le suivant : alors qu'ils sont censés apporter la transparence, la démocratie directe, l'accessibilité du droit aux citoyens, on constate que leur puissance accumulée, leur nombre, leur espace planétaire, les placent souvent dans une position tellement dominante que le droit juges finissent par trembler »[2244].

[2239] L'idée est tirée de la présentation faite par Cătălin Boacnă lors de la conférence internationale génériquement appelée « Doctoriale », organisée en partenariat par l'Université de Bucarest et l'Université de la Sorbonne, du 28 au 29 juin 2024, sous le titre « La désinformation par les réseaux sociaux - un défi pour le droit français dans le contexte européen » (à l'heure où nous écrivons ces lignes, les documents de la conférence n'ont pas été publiés).
[2240] S. Bonnett, "*The Dangers of Social Media Manipulation and Its Impact on Society*, LinkedIn, 2023. consulté le 28 novembre 2024. https://www.linkedin.com/pulse/dangers-social-media-manipulation-its-impact-society-simone- bonnett-/.
[2241] Antje, "*Disinformation and 7 Common Forms of Information Disorder*", The Commons, 2024. https://commonslibrary.org/disinformation-and-7-common-forms-of-information-disorder/.
[2242] G. Brunaux, *Réseaux sociaux et professionnels du droit : le risque disciplinaire*, Dalloz IP/IT, 2019, p.476.
[2243] J. Cohen, *Networks, Standards, and Network-and-Standard-Based Governance*, en K. Werbach (ed.), *After the Digital Tornado: Networks, Algorithms, Humanity*, Cambridge University Press, 2020, p.58.
[2244] P.-Y. Gautier, *De l'influence des réseaux sociaux sur l'édiction du droit*, Dalloz IP/IT, 2019. p.492

808. L'affaire Cambridge Analytica. Un cas populaire de délit de manipulation de l'information en lien avec l'atteinte à la vie privée des internautes dans la situation de Cambridge Analytica en 2018, où les données de plus de 87 millions d'utilisateurs de Facebook ont été collectées sous la forme de tests de personnalité sans leur autorisation explicite[2245]. Ces données ont été utilisées par Cambridge Analytica pour créer des profils psychologiques, qui ont ensuite été utilisés pour modifier les résultats des campagnes politiques par le biais de messages et de publicités individualisés. Les exemples les plus notoires sont la participation de Cambridge Analytica à la campagne présidentielle de Donald Trump en 2016[2246] et à la campagne du Brexit[2247], qui ont toutes deux utilisé des techniques de profilage psychographique basées sur des données illégales. Le scandale a conduit à des amendes record de 5 milliards de dollars[2248] infligées à Facebook par la Commission Fédérale pour le Commerce, à la faillite de Cambridge Analytica et à des préoccupations accrues en matière de confidentialité des données[2249].

b). Attaque contre la liberté de volonté. Réaction du droit pénal contre la manipulation

809. La France, pionnière dans la lutte contre les monopoles des grandes entreprises en ligne. La France a été le premier pays de l'Union Européenne à entrer en confrontation directe avec les géants de l'informatique dès 2000, lorsque le Tribunal de grande instance de Paris a jugé que les tribunaux français étaient compétents pour connaître d'une affaire alléguant un comportement illégal de Yahoo Inc, même si l'entreprise en question était basée aux États-Unis[2250]. Cette décision a encouragé l'Europe à réagir à la réglementation du commerce électronique par le biais de la directive 2000/31/CE du Parlement Européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique ») et l'introduction ultérieure de mesures visant à lutter contre les monopoles des

[2245] The Guardian, *The Cambridge Analytica Files*. https://www.theguardian.com/news/series/cambridge-analytica-files.
[2246] R. González, *Hacking the citizenry? Personality profiling, 'big data' and the election of Donald Trump*, Anthropology Today, vol.33, 2017, p.9-12. https://doi.org/10.1111/1467-8322.12348.
[2247] J. Rone, *Beyond Brexit? Public Participation in Decision-Making on Campaign Data During and After Referendum Campaigns*, Media and Communication, 2023. https://doi.org/10.17645/mac.v11i1.6200.
[2248] M. Hu, *Cambridge Analytica's black box*, Big Data & Society, vol.7, 2020. https://doi.org/10.1177/2053951720938091
[2249] N. Arora, D. Zinolabedini, *The Ethical Implications of the 2018 Facebook-Cambridge Analytica Data Scandal*, University of Texas Libraries, 2019. https://doi.org/10.26153/TSW/7590
[2250] N.M. Poujol, *Droit des communications électroniques*, Légipresse, 2016, p.241.

grandes sociétés Internet, y compris l'imposition d'amendes très élevées en cas d'infraction aux politiques de concurrence[2251].

c). De la première fausse nouvelle (1815) à la première loi de lutte contre la désinformation (1881)

810. Les *fake news* à l'époque napoléonienne. Le concept de fausse nouvelle est apparu pour la première fois dans une loi du 9 novembre 1815, alors que la monarchie établie après l'exil de Napoléon Bonaparte était mise en danger par de faux écrits annonçant le retour au pouvoir de l'ancien leader politique sur l'île d'Elbe. La peine encourue à l'époque était de cinq ans d'emprisonnement et terme de fausses nouvelles était défini dans des termes similaires à ceux d'aujourd'hui[2252].

811. Les bases législatives de la lutte contre la désinformation. La France a introduit des innovations juridiques dans la lutte contre la désinformation. L'article 27 de la loi du 29 juillet 1881 sur la liberté de la presse[2253] prévoit que la diffusion de fausses informations est passible d'une amende pénale. Aujourd'hui, cette base juridique devant sanctionner la publication de fausses nouvelles n'a plus d'applicabilité directe en pratique en raison du « caractère restreint de ses éléments constitutifs »[2254]. Le délit de diffusion de fausses nouvelles tel que régi par la loi de 1881 comporte trois éléments constitutifs, outre la publicité elle-même, qui ne sont plus adaptés à l'époque actuelle : le « caractère mensonger de la nouvelle ; la possibilité de troubler l'ordre public et la mauvaise foi ». De 2010 à 2018, seules trois condamnations ont été prononcées sur la base de cet article. Parallèlement, dans la pratique, il a été constaté que l'article 27 ne peut être appliqué à l'encontre des sociétés informatiques qui hébergent ou propagent des *fake news* via les médias sociaux, au motif que la diffusion se fait en ligne et non par voie de presse[2255].

[2251] *Pratiques anticoncurrentielles: la Commission inflige à Google une amende de 2,42 milliards d'euros pour abus de position dominante sur le marché des moteurs de recherche en favorisant son propre service de comparaison de prix – Factsheet,* Fiche d'information, Commission européenne, 2017. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_1785.

[2252] Europa 1, *De quand date le délit de "fausse nouvelle",* 2018. *„Alexis Corbière affirme que le délit de "fausse nouvelle" date de 1852".* https://www.europe1.fr/emissions/Le-vrai-faux-de-l-info2/de-quand-date-le-delit-de-fausse-nouvelle-3542042.

[2253] *La publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique ou aura été susceptible de la troubler, sera punie d'une amende de 45 000 euros. Les mêmes faits seront punis de 135 000 euros d'amende, lorsque la publication, la diffusion ou la reproduction faite de mauvaise foi sera de nature à ébranler la discipline ou le moral des armées ou à entraver l'effort de guerre de la Nation* (https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722/).

[2254] G. Sauvage, *Quel(s) outil(s) juridique(s) contre la propagation de "fake news" ?,* Légipresse, 2017. p.427.

[2255] N. Bénoit, *La mise en œuvre de la responsabilité des prestataires d'hébergement toujours incertaine*, Légipresse, 2015. p.339.

d). Développements juridiques récents dans la lutte contre la manipulation et la désinformation

812. Directives pénales, civiles et électorales contre les fausses informations. Il existe également d'autres dispositions légales sur la lutte contre la désinformation, tant dans le Code Pénal[2256] que dans le Code Civil[2257] ou le Code Électoral[2258], mais elles ne couvrent qu'indirectement les activités liées à la désinformation par le biais des médias sociaux. La première référence directe à la diffusion de fausses informations sur les médias sociaux a été faite dans une loi de 2016 modifiant le Code de la Consommation[2259], et entre autres sur les faux avis en ligne et sur la manière dont les plateformes numériques devraient empêcher la diffusion de fausses informations[2260].

Il convient de noter que le 22 mars 2017, une proposition visant à modifier le code pénal pour définir et punir les *fake news* a été enregistrée au Sénat[2261], y compris une tentative d'introduire un régime de sanctions beaucoup plus sévères pour les utilisateurs de médias sociaux qui diffusent de fausses informations, avec une peine maximale trois ans d'emprisonnement. Ce projet de loi n'a jamais été adopté, mais il visait précisément à lutter contre la désinformation via les réseaux numériques. Toutefois, cette proposition constituait un préambule aux débats publics à venir sur la réglementation de la lutte contre les contenus manipulateurs diffusés sur les plateformes de réseaux sociaux en ligne.

813. La désinformation, composante distincte de la manipulation en ligne. En assumant un débat public incisif avec des critiques de la société civile et des médias traditionnels, la France a adopté la LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information[2262], un texte de loi ciblant directement la désinformation via les plateformes de médias sociaux en ligne. Cette loi vise principalement à prévenir l'ingérence

---

[2256] Article 226-8 du *Code pénal - Délit de photomontage ou de montage sonore sans consentement et sans précision qu'il s'agit d'un montage.*
[2257] Article 9 du *Code civil - Droit au respect de la vie privée.*
[2258] Article L. 97 du *Code électoral - Délit de fausses nouvelles ayant altéré un scrutin.*
[2259] L.121-2 – « *Les faux avis entrent dans le domaine des pratiques commerciales trompeuses, qui sanctionnent les allégations, indications ou présentations fausses ou de nature à induire le consommateur en erreur le consommateur, pouvant porter notamment sur les caractéristiques essentielles d'un bien ou d'un service* ».
[2260] Article L. 111-7-2 dans le Code de la consommation – « *toute plateforme qui collecte, modère ou diffuse des avis en ligne rédigés par des consommateurs doit informer les utilisateurs de manière loyale, claire et transparente sur le processus de publication des avis, et indiquer en particulier si le traitement comprend une modération des avis et, le cas échéant, le contrôle mis en œuvre dans ce cadre.* »
[2261] N. Goulet, *Définir et sanctionner les fausses nouvelles ou «fake news»,* no.470, Sénat, 2017. https://www.senat.fr/leg/ppl16-470.html.
[2262] *Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information*. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559/

étrangère dans le processus électoral, puisqu'il s'agit d'une loi visant à modifier le code électoral. Dans le même temps, elle offre également une protection contre d'autres types de désinformation s'ils représentent un risque pour l'ordre public ou violent d'autres droits individuels[2263], y compris ceux générés par la crise sanitaire.

814. Respect du principe de proportionnalité. La construction moderne de la législation repose également sur le principe de proportionnalité, principe selon lequel l'individu n'est plus l'auteur originel des règles de droit, mais seulement leur destinataire. La loi devient légitime parce qu'elle équilibre de manière appropriée le rapport entre le bénéfice collectif et la protection collective ou les droits généraux[2264], qui peuvent être violés par certaines restrictions privées et individuelles[2265]. En ce qui concerne le respect du principe de proportionnalité dans la construction de la loi sur la lutte contre la manipulation de l'information, il a été soigneusement analysé à la fois dans les phases préliminaires de son adoption et par les membres du Conseil Constitutionnel. En mettant en balance les droits gagnés et les droits perdus, la loi a été approuvée et est maintenant en vigueur.

815. Domaines d'application de la loi, définis par le Conseil constitutionnel. Avec beaucoup d'enthousiasme, la loi a passé l'examen du Conseil constitutionnel, avec certaines réserves, expliquées assez clairement. Les opposants à la loi lui reprochaient un certain nombre de dispositions inconstitutionnelles, alléguant notamment : la violation de la liberté d'expression et de communication, la violation du principe d'égalité devant la loi, de la méconnaissance de la liberté d'entreprendre et le manque de clarté dans la définition des termes et dans l'application de la procédure visant à obtenir la cessation de la diffusion de fausses informations dans l'environnement numérique[2266]. À cette occasion, le Conseil constitutionnel a rejeté les critiques formulées à l'encontre de la loi et a précisément délimité son champ d'application[2267]. Plus précisément, au paragraphe 18 de la décision n° 2018-773 DC du 20 décembre 2018, le Conseil indique que « le législateur a entendu lutter contre le risque que les citoyens soient trompés ou manipulés dans l'exercice de leur droit de vote par la diffusion massive de telles informations

---

[2263] P. Mouron, *Coronavirus et fausses informations. Les aléas de la liberté d'expression en période de crise sanitaire,* Droit pénal, RDLF, no.33, 2020. http://www.revuedlf.com/droit-penal/coronavirus-et-fausses-informations-les-aleas-de-la-liberte-dexpression- en-periode-de-crise-sanitaire/

[2264] C. Thornhill, *Before the Law ? In The Sociology of Law and the Global Transformation of Democracy* ,Global Law Series, Cambridge University Press, 2018. p.228.

[2265] *Op. cit.* 11 – « *Dans sa forme courante actuelle, la doctrine de la proportionnalité implique que les organes publics peuvent adopter des lois restreignant les droits fondamentaux établis de certains sujets si une telle restriction est dictée et justifiée par le fait qu'elle génère un avantage ou une valeur collective qui est proportionnée aux conséquences de la restriction* ».

[2266] Conseil Constitutionnel, *Décision n° 2018-773 DC du 20 décembre 2018.* https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm.

[2267] Gouvernement.fr, «*Contre la manipulation de l'information*», 2018. La référence a été publiée dans le cadre de la loi n° 2018-1202 du 22 décembre 2018, relative à la lutte contre la manipulation de l'information. https://www.gouvernement.fr/action/contre-la-manipulation-de-l-information.

sur des services de communication au public en ligne »[2268] la procédure d'exclusion des fausses informations débute « trois mois avant le premier jour du mois précédant une élection générale ou un référendum et s'achève à la date du tour de scrutin au cours duquel elles sont acquises »[2269].

Dans le même temps, le Conseil souligne que « le législateur a strictement délimité les informations pouvant faire l'objet de la procédure de renvoi contesté » en ce sens que les fausses informations « ne comprennent pas les opinions, les parodies, les inexactitudes partielles ou les simples exagérations ». Avec ce type de raisonnement, le Conseil constitutionnel limite quelque peu le champ d'application de la loi en ce sens que ce ne sont pas tous les propos mensongers qui peuvent suivre la procédure d'exclusion des médias sociaux, mais uniquement les propos qui, par leur caractère trompeur, sont de type « manifeste »[2270]. Dans ce contexte, les allégations inexactes ou trompeuses entrent dans le champ d'application de la loi si trois conditions essentielles sont cumulativement réunies[2271] : les allégations sont manifestement fausses ou trompeuses ; elles ont une influence sur le scrutin[2272] ; elles doivent être diffusées délibérément, artificiellement ou automatiquement à un grand nombre d'utilisateurs par l'intermédiaire d'une plateforme en ligne.

816. Le Tribunal de Paris a interdit l'utilisation des robots dans les campagnes électorales. Concernant ce dernier critère, le Tribunal de grande instance de Paris a expliqué dans sa décision du 17 mai 2019, à l'occasion des élections pour le Parlement Européen, que la diffusion de fausses informations cible les contenus promus ou sponsorisés par des robots. Il convient de noter que la loi promulguée le 22 décembre 2018 comporte trois piliers importants sur la base desquels elle cherche à lutter contre la désinformation via les médias sociaux : l'obligation pour les plateformes de s'autoréguler, la création de systèmes de signalement des *fake news* et l'octroi de pouvoirs accrus au Conseil Supérieur de l'Audiovisuel, y compris en termes d'interdiction de diffusion de chaînes de télévision étrangères sur le territoire français.

817. La loi controversée sur la lutte contre les contenus incitant à la haine en ligne. La réaction du droit français en termes de limitation de la désinformation par les médias sociaux

[2268]Conseil Constitutionnel, *Décision n° 2018-773 DC du 20 décembre 2018*. https://www.conseil-constitutionnel.fr/decision/2018/2018773DC.htm.
[2269] Paragraphe 19 de la *Décision n° 2018-773 DC du 20 décembre 2018* du Conseil Constitutionnel.
[2270] Paragraphe 23 de la *Décision n° 2018-773 DC du 20 décembre 2018* du Conseil Constitutionnel.
[2271] G. Haas, A. Dubarry, *Lutter contre les fake news, un défi juridique et démocratique*, Dalloz IP/IT, 2020. p.240.
[2272] Le Conseil Constitutionnel rappelle que cette influence doit être avérée et non pas seulement potentielle.

ne s'est pas limitée à ce qui précède. Bien qu'elle ait suscité une vive controverse de la part de l'opinion publique, des acteurs politiques et des représentants des plateformes numériques, la loi du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet a été promulguée par le Président de la République. Même le Conseil constitutionnel a admis de nombreuses critiques concernant l'inconstitutionnalité de cette loi au regard de l'atteinte à la liberté d'expression[2273]. Il est évident que l'adoption d'une loi présentant de graves problèmes constitutionnels constitue un précédent dangereux pour le droit français[2274], mais, en application du même principe de proportionnalité décrit ci-dessus, le législateur a estimé que les valeurs à protéger par cette loi étaient particulièrement importantes. Cette loi aborde la question de la diffusion de fausses informations sur les réseaux sociaux. Les contenus illicites diffusés sur les plateformes numériques sont principalement visés et un observatoire de suivi de ce type de contenus, qu'il s'agisse de textes, de photos ou de vidéos, a été créé au sein du Conseil supérieur de l'audiovisuel pour surveiller la haine sur Internet.[2275]

L'article 24 de la Loi pour une sécurité globale préservant les libertés, adopté par le Parlement le 15 avril 2021[2276],est tout aussi controversé. Cet article a donné lieu à des manifestations massives[2277] en France à la fin de 2020 et au début de 2021, étant donné que la liberté d'expression des journalistes était affectée et que la diffusion d'images de policiers, y compris via les plateformes de médias sociaux, était interdite. Initialement, l'article 24 voté par l'Assemblée Nationale en octobre 2020 complétait la loi du 29 juillet 1881 sur la liberté de la presse en ce qu'il était puni d'une peine d'emprisonnement ou d'une amende de 45 000 €, « le fait de diffuser, par n'importe quel moyen ni quel support, ayant le but de blesser l'intégrité physique ou psychique d'une personne »[2278]. Dans la version adoptée par le Parlement, cet article a été entièrement réécrit en ce sens qu'il ne fait plus référence à la Loi sur la presse et que l'article 226-4-1-1 est ajouté au Code pénal, avec le délit de « provocation à l'identification ».

[2273]Conseil Constitutionnel, *Décision n° 2020-801 DC du 18 juin 2020*. https://www.conseil-constitutionnel.fr/decision/2020/2020801DC.htm.

[2274] G. Beaussonie, *L'essor des lois pénales inconstitutionnelles*, RSC, 2020. p.975.

[2275] M. Quéméner, *Haine en ligne : présentation de la circulaire du garde des Sceaux relative à la lutte contre ce fléau*, Dalloz IP/IT, 2021. p.110.

[2276] Europe 1, «*Le Parlement adopte définitivement la proposition de loi controversée sur Global Security*», https://www.europe1.fr/politique/le-parlement-adopte-definitivement-la-proposition-de-loi-controversee-sur-global-security-4038809.

[2277] France24, «*Des milliers de personnes manifestent contre la loi sécurité globale*», 2020. https://www.france24.com/fr/france/20201121-des-milliers-de-personnes-manifestent-contre-la-loi-s%C3%A9curit%C3%A9-globale.

[2278] *Proposition de loi relative à la sécurité globale, n° 3452, déposée le mardi 20 octobre 2020*, Assemblée nationale. https://www.assemblee-nationale.fr/dyn/15/textes/l15b3452_proposition-loi.

818. Détection et contre-attaque des ingérences numériques étrangères. Dans ce contexte juridique et social, le décret n° 2021-922 du 13 juillet 2021[2279], pris par le Président de la République, a créé le « Service de vigilance et de protection contre les ingérences numériques extérieures » (VIGINUM), établissement placé sous l'autorité du secrétaire général de la défense et de la sécurité nationale. Concrètement, VIGINUM est un service technique et opérationnel de l'État qui vise à détecter les contenus d'information faux ou trompeurs susceptibles d'affecter le débat public dans l'environnement en ligne en France[2280].

819. L'impact de la loi SREN sur les deepfakes. La lutte contre la désinformation dans l'environnement en ligne a atteint son apogée avec l'adoption de la loi n° 2024-449 du 21 mai 2024 « visant à sécuriser et à réguler l'espace numérique », également connue sous le nom de loi SREN. Cet acte normatif comporte un volet visant à protéger les mineurs de l'accès à des sites à contenu pornographique[2281] et un autre volet visant à réprimer la manipulation de l'information dans le cyberespace. Une réglementation présente dans la loi 21 mai 2024, qui a suscité des débats tant dans l'opinion publique[2282] que dans la doctrine juridique[2283], est celle concernant l'incrimination du phénomène du *deepfake*, également connu sous le nom d'hyper-trucage.[2284] Dans ce contexte, l'art. 226-8 du Code pénal de punir d'un an d'emprisonnement ou de 15.000 € d'amende le fait de rendre public « un montage de paroles ou d'images d'une personne sans son consentement, sauf s'il est manifeste qu'il s'agit d'un montage ou s'il n'est pas expressément mentionné comme tel ». La peine est portée à deux ans d'emprisonnement si l'infraction est commise via « un service de communication au public en ligne ». Bien que le contenu de la loi semble novateur, certains auteurs[2285] considèrent que la répression du deepfake ne révolutionne pas le système juridique et que l'impact sur la société ne se fera réellement sentir que lorsque se façonnera une certaine pratique judiciaire.

[2279] *Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères*. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043788361.

[2280] *Service de vigilance et protection contre les ingérences numériques étrangères,* SGDSN, 2022.„*VIGINUM est le service technique et opérationnel de l'État chargé de la vigilance et de la protection contre les ingérences numériques étrangères".* https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques

[2281] C. Lamy, *Publication de la loi SREN sans le délit d'outrage en ligne*, Observations sous Conseil constitutionnel, n°866, Dalloz IP/IT, 2024. p.314.

[2282] Y. Baranes, *Deep Fake : Régulation française et européenne*, laboratoire de Cyberjustice, 2024. https://www.cyberjustice.ca/en/2024/07/22/deep-fake-regulation-francaise-et-europeenne/.

[2283] A. Guedj, *L'apport de la loi SREN sur le deepfake : une obsolescence annoncée ?*, Dalloz IP/IT, 2024. p.391.

[2284] N. Nevejans, *L'appréhension de l'IA générative par le règlement sur IA*, Dalloz IP/IT, 2024. p.502.

[2285] J. Bossan, *La protection de la représentation à l'ère du numérique et du deepfake : le délit de montage version 2.0*, Légipresse, 2024. p.380. « *En conclusion, il serait imprudent de dire que le délit de montage a été révolutionné par la loi du 21 mai 2024 du fait de l'< hypertrucage>. Pourtant, cette évolution liée à l'IA aura l'intérêt de mettre en évidence la qualification. La question est désormais de savoir dans quelle mesure la pratique s'emparera de cette version 2.0 délit de montage* ».

f). Astroturfing, swarming et « l'armée des 50 cents »

820. Méthodes de manipulation de l'information. La manipulation de l'information se fait par le biais d'série de techniques bien définies, chacune ayant pour objectif principal de déformer la réalité et d'influencer l'opinion du public général.[2286] À l'ère de l'accès à l'information et à la technologie, ces techniques deviennent de plus en plus sophistiquées, d'autant plus que l'accessibilité de la population aux plateformes de médias sociaux a facilité une diffusion plus rapide des contenus médiatiques manipulés. La désinformation est une technique de manipulation de l'information qui consiste à diffuser intentionnellement des informations fausses ou altérées afin de manipuler l'opinion publique[2287]. La désinformation se retrouve dans les *fake news*, les théories du complot, les informations déformées ou d'autres types de contenus conçus pour influencer négativement les perceptions sociales, économiques ou politiques[2288]. Le plus souvent, la désinformation est utilisée par des acteurs étatiques et non étatiques pour saper la confiance dans les institutions ou pour déstabiliser l'ordre social dans certains contextes[2289].

Parmi les techniques de manipulation les plus intrusives dans les environnements dominés par la puissance des algorithmes, on trouve celles qui touchent directement à l'autonomie de la volonté. Les environnements synthétiques[2290], en particulier ceux créés par l'utilisation d'algorithmes d'intelligence artificielle, représentent un défi de plus en plus important pour l'environnement juridique. Le *swarming* et l'*astroturfing* sont deux termes de plus en plus utilisés dans le contexte de la discussion sur la désinformation via les médias de masse, en particulier les médias sociaux.

821. Manipulation de l'information par l'*astroturfing*. L'*astroturfing*[2291] est un terme inspiré du nom d'une marque américaine de gazon artificiel et se réfère notamment à la manipulation de l'opinion publique par le biais des médias sociaux[2292]. Plus précisément, il s'agit

---

[2286] S. A. McCornack, "*Information Manipulation Theory*", Communications Monographs, 1992. https://doi.org/10.1080/03637759209376245.

[2287] *Disinformation Definition & Meaning*, Merriam-Webster, consulté le 26 novembre 2024, https://www.merriam-webster.com/dictionary/disinformation.

[2288] *Du fake news au désordre informationnel,* Magazine Intelligence (blog), 2023. https://intelligence.sri.ro/de-la-fake-news-la-dezordinea-informationala/.

[2289] *Désinformation et division. Le cercle vicieux de la méfiance*, Magazine Intelligence (blog), le 2 mai 2023. https://intelligence.sri.ro/dezinformare-si-divizare-cercul-vicios-al-neincrederii/.

[2290] *AI Generated Synthetic Media, aka Deepfakes*, Medium Data Science, 2020. https://towardsdatascience.com/ai-generated-synthetic-media-aka-deepfakes-7c021dea40e1.

[2291] *Astroturfing* , Lexico.https://www.lexico.com/definition/astroturfing.

[2292] *L'astroturfing, ou comment bidonner des initiatives citoyennes,* https://www.franceinter.fr/emissions/les-legendes-du-web/les-legendes-du-web-13-mai-2016.

de donner l'impression qu'une idée particulière est soutenue par un très grand nombre de personnes, alors qu'en réalité de faux comptes sont utilisés pour viraliser le message initial[2293]. En substance, l'astroturfing consiste à créer une illusion de soutien populaire afin de manipuler les perceptions du public et d'influencer la prise de décision. Généralement, les messages de soutien, qu'ils proviennent de faux comptes gérés par de vraies personnes ou d'algorithmes, promeuvent l'idée d'un mouvement populaire, spontané et authentique.

822. **L'attitude internationale**. En septembre 2024, aux États-Unis, la Commission Fédérale du Commerce a annoncé qu'elle avait imposé des règles juridiques claires pour empêcher l'Astroturfing, pour éliminer les évaluations par intelligence artificielle ou les commentaires générés par des chatbots.

En Chine, le phénomène d'envoi de messages répétitifs exprimant l'idée d'un soutien populaire et inconditionnel au dirigeant politique est entretenu par des fonctionnaires qui surveillent les communications sur les médias sociaux et publient des commentaires exprimant ce soutien. La publication de commentaires ou de messages se fait en échange d'une rémunération de 50 cents, d'où le nom d'« armée des 50 cents ». Selon les estimations, des millions de messages ou de commentaires sont ainsi postés chaque année, dans le seul but d'influencer la perception des utilisateurs du réseau. Ces messages sont également postés sur des sites web hors de Chine et expriment des louanges et de l'admiration pour le gouvernement chinois, le parti communiste et le président. Cette « armée » comprend environ 300.000 personnes[2294].

823. Quant au swarming, ce terme est de nature plus militaire et décrit une tactique dans laquelle de grands groupes de soldats travaillent simultanément pour submerger une cible adverse. Cette technique se caractérise par une supériorité numérique et une rapidité de mouvement.

g). Arme stratégique pour déstabiliser les gouvernements et les sociétés

824. **Les influences actuelles de la désinformation**. La Roumanie a été une cible privilégiée de la manipulation de l'information pendant la pandémie de COVID-19, la désinformation et les théories du complot largement répandues. Les réseaux sociaux ont été la principale cible des campagnes de désinformation ayant comme but principal la nuisance de la confiance du public

[2293] C. Harbulot, « *Fabricants d'intox. La guerre mondialisée des propagandes* », Lemieux Éditeurs, Paris, 2016.
[2294] G. King, J. Pan, M. Roberts, *How The Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument,* Cambridge University Press, 2017. Cet article fournit des preuves du phénomène et des détails sur l'activité de ceux qui postent des messages sur les réseaux sociaux. https://doi.org/10.1017/S0003055417000144

dans le système médical, provoquant une résistance substantielle aux mesures de protection et aux campagnes de vaccination.[2295] Sur les réseaux sociaux on a présenté des campagnes de désinformation, avec des messages tels que « la pandémie est un canular » et « la vaccination obligatoire est une forme de dictature médicale », qui ont été diffusés dans l'environnement numérique et ont suscité des réactions mitigées au sein du public[2296].

825. Mobilisation des plateformes en ligne contre les fausses informations. Au même moment, Facebook a lancé un programme de vérification des informations pour l'espace roumain, en partenariat avec l'agence de presse française Agence France-Presse (AFP), qui a ensuite été introduit sur la plateforme Instagram. Essentiellement, toute information jugée fausse atteindra à un nombre plus réduit de personnes, son activité de distribution étant considérablement réduite[2297]. Toujours en novembre 2022, X a introduit le programme *Community Notes*, similaire au programme introduit par Facebook et Instagram, qui vise à signaler toute tentative de promotion et de diffusion d'informations falsifiées[2298].

826. La menace d'une guerre hybride. Un autre aspect important de la désinformation est son utilisation dans la guerre hybride en tant qu'arme stratégique pour déstabiliser les gouvernements et les sociétés. Dans le contexte de la sécurité nationale, les services de renseignement roumains ont mis l'accent sur les effets majeurs de la désinformation, principalement sur la stabilité de l'État, en influençant l'opinion publique ainsi que les décisions politiques et économiques. Des techniques telles que « la plantation » consistent à introduire des fausses nouvelles par le biais de médias contrôlés ou de trolls sur Internet afin de créer un état de confusion au sein de la population[2299]. Cette technique est utile et fructueuse car elle repose sur la division de la population en fonction de ses croyances, et un groupe qui s'identifie au message véhiculé promouvra de plus en plus l'information malveillante. La technique du planting est également utilisée dans la guerre hybride menée par la Fédération de Russie en Ukraine.

[2295] « *Désinformation, pandémie de l'ombre* », Magazine Intelligence (blog), 2021. https://intelligence.sri.ro/dezinformarea-pandemia-din-umbra/.

[2296] C. Pam, « *Radiographie de la désinformation sur COVID-19 en Roumanie* », Cotidianul, 2020. consulté le 26 novembre 2024, https://www.cotidianul.ro/radiografia-dezinformarii-despre-covid-19-in-romania/.

[2297] C. Dobreanu, « *Filtre anti-désinformation, utilisé par Facebook en Roumanie. Expert : les Roumains sont relativement vulnérables aux fake news* », Europe Libre, 2020. consulté le 26 novembre 2024, https://romania.europalibera.org/a/facebook-baga-filtru-anti-dezinformare-romania-expert-romanii-sunt-relativ-vulnerabili/30955411.html.

[2298] *About Community Notes*, X Help, consulté le 26 novembre 2024, https://help.x.com/en/using- x/community-notes.

[2299] « *La désinformation, une arme pour tous les fronts* », Magazine Intelligence (blog), 2020. https://intelligence.sri.ro/dezinformarea-o-arma-pentru-orice-front/

.

Conclusion §2.

827. Les utilisateurs en France ne vivent pas dans un environnement vraiment neutre, les efforts de la France contre les *fake news*. En conclusion, les efforts de la France pour limiter la diffusion de fausses informations via les sites de réseaux sociaux sont visibles, mais à ce stade, ils ne sont pas suffisants pour donner aux internautes l'assurance qu'ils vivent dans un environnement réellement neutre[2300] et sûr. L'exemple le plus éloquent est que la France est aujourd'hui devenue l'un des pays les plus sceptiques en matière de vaccination, des études récentes[2301] ayant montré que le nombre d'utilisateurs francophones partageant de faux contenus anti-vaccination est passé de 3,2 millions à 4,1 millions en 2020.

Dans le même temps, la diffusion de fausses informations peut affaiblir davantage la crédibilité du message officiel des autorités et générer un manque de confiance dans les institutions publiques. La pandémie de Covid-19 l'a amplement démontré en France. Parmi les nombreux exemples d'informations devenues rapidement virales sur facebook[2302], tweeter, youtube et autres réseaux similaires, l'Institut Pasteur a été accusé d'avoir créé le virus du SRAS-Cov 2 et de 'avoir disséminé dans la ville de Wuhan en Chine. Dans cette situation, le célèbre institut de recherche a dû lancer une contre-campagne pour démentir ces fausses informations[2303].

Parallèlement, le pouvoir d'enquête pénale dans l'environnement numérique[2304] ou le pouvoir de contrôle des organisations dotées de pouvoirs spéciaux sur les plateformes en ligne doivent également être renforcés afin d'assurer un climat de sécurité et de sûreté dans l'environnement virtuel. Dans ce contexte, la vigilance juridique doit être adaptée à ces nouveaux défis technologiques et les mesures législatives de protection de la démocratie doivent être aussi rapides et fermes que possible. L'impact de ces techniques est majeur, touchant non seulement les sphères sociales et politiques, mais aussi l'économie et la vie privée des citoyens.

[2300] *Qu'est-ce que la neutralité du Net ?*, La Monde, 2017. https://www.lemonde.fr/pixels/article/2017/11/22/qu-est-ce-que-la-neutralite-du-net_5218670_4408996.html.
[2301] *The vaccine misinformation battle raging in France*, BBC Trending, 2021. https://www.bbc.com/news/blogs-trending-56526265.
[2302] *Le coronavirus a-t-il été créé en laboratoire?,* Facebook. https://www.facebook.com/watch/?ref=search&v=190781758892563&external_log_id=a7b1682c-cfc1-47e5-a97b-36fef125594e&q=institut%20pasteur%20a%20cree%20coronavirus.
[2303] *Coronavirus: Institut Pasteur warns against false information circulating on social media*, Institut Pasteur, 2020. https://www.pasteur.fr/en/home/research-journal/news/coronavirus-institut-pasteur-warns-against-false-information-circulating-social-media.
[2304] J.-C. Saint-Pau, *Investigations numériques et le droit au respect de la vie privée*, AJ pénal, 2017. p.321.

Section 2. **DÉFIS IMMINENTS POUR LE DROIT PÉNAL : LE DROIT À L'ANONYMAT ET LA VIE PRIVÉE DANS LE MÉTAVERS**

828. Le droit à l'anonymat n'est pas absolu. « Dès la naissance, chaque personne est capturée par la société, qui lui impose sa marque : l'identification. Il faut un nom, un prénom, un domicile, un numéro de sécurité sociale », explique l'introduction de la thèse de doctorat soutenue par le Professeur Jean Christophe Saint-Pau à l'Université de Bordeaux[2305]. L'obligation de déclarer son identité dans tous les actes officiels ne peut être évitée en aucune façon. « C'est un consommateur potentiel qui a besoin d'être « ciblé » à travers les fichiers clients et qui a besoin de s'identifier lorsqu'il devient un véritable consommateur », a-t-il déclaré en 1998, alors qu'il était difficile de prédire que les médias sociaux transformeraient le « consommateur » en un produit.

829. Termes incompatibles: anonymat, sécurité, ordre public. L'anonymat est bien évidemment incompatible avec la notion de sécurité et d'ordre public. Garder l'anonymat est impossible dans la société d'aujourd'hui, car les gouvernements et les géants de l'informatique collectent suffisamment de données privées pour que, dans certaines situations, ils puissent même prédire des événements futurs en fonction de l'historique de recherche de Google. « Anonymous a quelque chose à cacher »,[2306] a été l'une des conclusions de l'article mentionné ci-dessus, et l'anonymat est spécifique au délit.

Si en « offline » il y a, en théorie, la possibilité que l'anonymat soit préservé par un isolement complet du monde, après une inscription préalable dans les bases de données gouvernementales immédiatement après la naissance, en « online » les choses se positionnent dans un paradoxe que la loi ne peut toujours pas résoudre entièrement. L'isolement dans une forêt désertique peut fournir une certaine forme d'anonymat vis-à-vis de la société. L'anonymat sur internet, bien que garanti à la fois par l'ordre public des géants de l'informatique et par la jurisprudence de la CEDH, est « assuré » après authentification préalable et acceptation des termes et conditions des contra standards des prestataires de services. On ne vous demande pas votre pièce d'identité comme si vous étiez à un comptoir pour payer vos impôts, ni comme si vous remettiez votre passeport pour monter dans l'avion. C'est un peu comme utiliser des données biométriques déjà collectées et stockées par un aéroport qui a supprimé des documents physiques. Fondamentalement, la connexion à Internet se fait en fournissant une identité du

[2305] *L'anonymat et le droit*, thèse présentée et soutenue publiquement pour l'obtention du grade de Docteur en Droit par Jean-Christophe Saint-Pau, le 14 janvier 1998. La thèse n'a pas été publiée et a été consultée à la bibliothèque de l'Institut de sciences criminelles et de la Justice de l'Université de Bordeaux
[2306] Op. cit. pg 2

système informatique utilisé, ce qui peut conduire à l'identification de l'utilisateur. La garantie de l'anonymat n'est pas absolue[2307].

830. Le droit à l'anonymat, un droit défensif. Les caractéristiques essentielles du droit à l'anonymat sont d'être défensif (de bénéficier du respect) et d'être non patrimonial – « L'existence d'une liberté de vivre anonymement découle naturellement d'une prérogative destinée à défendre ce droit d'action : il s'agit du droit au respect de l'anonymat. Cette prérogative est un droit subjectif, c'est-à-dire un pouvoir juridique. Mais c'est surtout un droit de personnalité, car l'anonymat est en effet un intérêt moral. » [2308]

Certains auteurs[2309] notent que la notion d'anonymat sur Internet n'est pas bien comprise par les utilisateurs, et que cette forme de protection de l'identité ne devrait pas être en fait une forme d'acquisition d'un niveau absolu de liberté d'expression. Dans le même contexte, un fait qui devrait nous amener à réfléchir est montré : « L'équilibre entre vie privée et vie publique tend à s'inverser : la publication ne coûte rien, tandis que la protection de la vie privée nécessite des efforts. Dans le même temps, la notion d'anonymat sur internet est souvent mal comprise ».

§1. EFFETS JURIDIQUES DE L'ANONYMAT EN LIGNE

> « Il n'y a que deux industries qui nomment leurs clients « utilisateurs » : l'industrie des drogues illicites et l'industrie informatique. »[2310]

831. Définition du terme « anonymat » en ligne. Au fil du temps, plusieurs variantes ont été proposées pour définir le concept d'anonymat dans le cyberespace. Craig R. Scott a déclaré dans son article que l'anonymat est représenté par *«* la mesure dans laquelle un interlocuteur perçoit que la source du message est inconnue et non spécifique ». [2311] D'autres auteurs[2312] définissent l'anonymat ou l'absence de nom comme l'incapacité de déterminer l'identité d'une personne dans un contexte particulier.

Quant à l'étymologie du terme *anonyme,* elle vient de la langue grecque, où *"an"* signifie *sans*, et *"onyma"* signifie *nom.* Le pseudonyme est étroitement lié à l'anonymat, qui consiste à

[2307] Recommandation CM/Rec(2014)6 du Comité des Ministres aux Etats membres sur le Guide des droits de l'homme pour les internautes et l'exposé des motifs adopté par le Comité des Ministres le 16 avril 2014
[2308] J.-C. Saint-Pau, op. cit. pg 833
[2309] M. Untersinger, B. Bayart, *Anonymat sur Internet: protéger sa vie privée*, 2e édition, Eyrolles, 2014.
[2310] Edward Tufte, renommé statisticien américain et professeur.
[2311] C. R. Scott, *To reveal or not to reveal : A theoretical model of anonymous communication,* revue Teoria Comunicării, vol. VIII, n° 4, 1998, pp. 387.
[2312] E. Caliskan, T. Minarik, A.-M. Osula, *Technical and Legal Overview of the Tor Anonymous Network*, magazine Tallinn, 2015, disponible sur www.ccdcoe.org, consulté le 02.09.2024.

identifier une personne sous un faux nom.[2313] Ainsi, en principe, l'anonymat en ligne se concentre sur le masquage de l'identité réelle sous un pseudonyme, empêchant la détection de la personne derrière l'appareil.[2314]

832. Concept d'actualité. L'anonymat en ligne est un concept d'actualité qui permet aux navigateurs de déguiser leur véritable identité lorsqu'ils accèdent à des pages Web ou interagissent avec d'autres personnes. « L'anonymat est traditionnellement perçu comme l'incapacité d'autrui à identifier un individu. Il peut être vu dans un contexte social large, comme une foule, ou dans un contexte social étroit, comme la communication entre deux personnes sur Internet. »[2315]

L'anonymat en ligne fait l'objet d'une réglementation internationale, étant reconnu par la Déclaration[2316] du Conseil de l'Europe sur la liberté de communication sur Internet et le « rapport du Rapporteur spécial pour la promotion et la protection du droit à la liberté d'opinion et d'expression[2317] » des Nations Unies.

833. Le concept de « désinhibition en ligne ». En cette ère numérique, l'anonymat s'est accru, avec l'augmentation du nombre de personnes utilisant un faux nom ou une fausse identité pour s'exprimer sur Internet. Ce nouveau concept a été défini dans la doctrine spécialisée comme « l'effet de désinhibition en ligne »[2318], qui a provoqué un changement dans le comportement des utilisateurs, qui ont tendance à s'exprimer librement, sans censure morale, fréquemment et « plus intensément » qu'il ne l'aurait fait en association avec lui-même.

L'anonymat offre un certain nombre d'avantages dans l'idée de protéger l'intimité, d'encourager la libre expression des pensées et des concepts, l'autonomie, au-delà de la peur des répercussions sociales.[2319] Le droit à la vie privée est considéré comme l'un des droits fondamentaux les plus importants garantis par la Convention Européenne des Droits de

---

[2313] *Ibidem*.

[2314]Exploring Online Anonymity, *A brief introduction of online anonymity*, Medium, 2018. https ://medium.com/@shannonwilkins_93340/blog-post-1-a-brief-introduction-of-online-anonymity-1d091f536d26, consulté le 08.09.2024.

[2315] K. Christopherson, *The Positive and negative implications of anonymity in Internet social interactions : „On the Internet, Nobody Knows You're a Dog",* Computers in Human Behavior, 2007, p.3040.

[2316] Le Conseil de l'Europe, La *Déclaration sur la liberté de communication sur Internet* a été adoptée par le Comité des Ministres le 28 mai 2003, lors de la 840e réunion des Vice-Ministres.
Le principe 7, intitulé *Anonymat*, stipule : « Afin d'assurer la protection contre la surveillance en ligne et d'accroître la libre expression des informations et des idées, les États membres doivent respecter la volonté des internautes de ne pas faire connaître leur identité. Cela n'empêche pas les États membres d'agir et de travailler ensemble pour trouver les responsables de crimes, conformément au droit national, à la CEDH et à d'autres accords internationaux dans les domaines de la justice et de la police. »

[2317] Assemblée Générale des Nations, *Rapport quant au Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression,* disponible sur https ://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf, consulté le 03.09.2024.

[2318] J. Suler, *The online dysinhibition effect*, PubMed, 2024, https ://pubmed.ncbi.nlm.nih.gov/15257832/#full-view-affiliation-1, consulté le 10.12.2024

[2319] Ș. Boncu, *Psychologie sociale, Cours 16 – Désindividualisation* référence à T. Postmes & R. Spears, *Deindividuation and Antinormative Behavior*: *A Meta-Analysis*, Psychological Bulletin, 1998, p. 238

l'Homme, comme le prévoit l'article 8 de ce traité international. Il est tenu compte du fait que sous la protection de l'anonymat, l'individu estime qu'il n'y a plus de censure et de différenciation selon l'appartenance politique, le statut social, l'aspect, l'ethnicité, la religion, la religion, race, etc.

834. L'anonymat, la nécessité d'une réglementation distincte. Cependant, nous ne pouvons pas apprécier que l'anonymat s'impose être réglementé comme un droit distinct, parce que l'anonymat doit être traité en fonction de chaque contexte. Toutefois, il est juste de considérer l'anonymat comme un élément essentiel de plusieurs droits de l'homme, tels que le droit à la liberté d'expression, le droit de vote, le droit à la vie privée ou le droit à la liberté d'association.[2320]

835. Lacunes législatives. Si l'anonymat sur Internet est sans aucun doute un moyen précieux de protéger la vie privée et la liberté d'expression, c'est aussi un outil capable de contourner les normes juridiques.[2321] À cet égard, l'anonymat met en lumière et accentue les lacunes législatives, à la lumière des défis juridiques qu'il soulève, notamment dans le contexte de la cybercriminalité et de la protection des données personnelles. Toutefois, l'anonymat en ligne ne garantit pas la protection des contrevenants et ne constitue pas un moyen de contourner la loi et de les exonérer de leur responsabilité pénale, car il existe de nouvelles méthodes d'identification des auteurs, d'autant plus que la même méthode d'utilisation du compte anonyme à partir des mêmes serveurs ou ordinateurs est utilisée à plusieurs reprises.

836. Évolution au fil des années. En regardant le contexte historique, il est facile de voir que l'anonymat en ligne est apparu et s'est développé avec l'évolution d'Internet, au cours de la période des années '90, lorsque principalement des forums, des *chat rooms* et d'autres plateformes sociales ont été utilisés. À cette époque, l'anonymat était utilisé avec les plus pures intentions, pour protéger l'identité et encourager la liberté d'expression. Cependant, avec la popularité d'Internet, l'anonymat en ligne a gagné une valeur différente, imposant une analyse de la sécurité, de la vie privée[2322] et de la responsabilité dans l'environnement en ligne.

L'Université Carnegie Mellon aux États-Unis a compilé des statistiques sur plus de 1000 utilisateurs adultes. En ce qui concerne la protection de la vie privée, le rapport statistique conclut qu'un nombre notable d'utilisateurs ont rencontré des problèmes de vol ou de

[2320] E. Caliskan, T. Minarik, A.-M. Osula, *Technical and Legal Overview of the Tor Anonymous Network*, Tallinn, 2015.

[2321] IP2World, *Navigating the Ethical Dilemmas of Online Anonymity*, blog IP2World,2023. https://www.ip2world.com/blog/navigating-the-ethical-dilemmas-of-online-anonymity.html, consulté le 31.08.2024.

[2322] R. van den Hoven van Genderen, *Cybercrime investigation and the protection of personal data and privacy,* Project on Cybercrime of the Council of Europe, 2008. https ://rm.coe.int/16802fa3a3 consulté le 10.12.2024.

harcèlement de données personnelles, de perte de réputation, de fraude ou de vol d'informations bancaires.[2323]

La cybercriminalité est devenue l'un des problèmes les plus répandus et les plus graves dans la société d'aujourd'hui, généré par l'utilisation excessive de gadgets et de plateformes dans le dark web, la « consommation d'informations » en ligne, qui a généré de nombreuses situations de vulnérabilité dans le cyberespace. Au fil des ans, la définition du concept de cybercriminalité a posé et continue de poser des défis. Bien que les Nations Unies[2324] et le Conseil de l'Europe[2325] aient accepté et reconnu l'existence de ce phénomène[2326], cette notion n'est pas encore réglementée par la loi.[2327]

837. Armes législatives contre la cybercriminalité. L'outil le plus précieux dans le domaine de la *cybercriminalité* au niveau européen est la Convention du Conseil de l'Europe sur la cybercriminalité[2328], il est essentiel de transposer ce thème et de le réglementer au niveau international. Reconnue comme la Convention de Budapest contre la cybercriminalité, elle a été adoptée le 23 novembre 2001 par le Conseil de l'Europe et vise à « renforcer une politique pénale commune visant à protéger la société contre la cybercriminalité [...] en adoptant une législation appropriée et en encourageant la coopération internationale »[2329]

À la lumière de la cybercriminalité*, la cybercriminalité* et l'anonymat travaillent ensemble et développent une relation symbiotique.

La montée de la cybercriminalité à travers le filtre de l'anonymat remet en question l'autorité de la loi dans l'environnement virtuel et oblige à réévaluer les normes juridiques en ligne, car la capacité de dissimuler l'identité offre un degré élevé de protection aux utilisateurs contre les accusations pénales qui peuvent leur être portées, générant de nouvelles formes de cybercriminalité.[2330]

[2323] L. Rainie, S. Kiesler, R. Kang, M. Madde, *Anonymity, Privacy, and Security Online*, Pew Research Center, 2013.

[2324] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime, 2013*. https ://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf), consulté le 03.09.2024.

[2325] Convention sur la cybercriminalité - https ://rm.coe.int/1680081561 - consulté le 10.02.2023.

[2326] S. Broadhead, *The contemporary cybercrime ecosystem* : *A multi-disciplinary overview of the state of affairs and developments*, Computer Law & Security Review, vol. 34, 2018, p.1181.

[2327]*La cybersécurité dans l'UE et ses États membres, Comité de contact des institutions supérieures de contrôle de l'Union européenne, 2020*. https ://www.eca.europa.eu/sites/cc/Lists/CCDocuments/Compendium_Cybersecurity/CC_Compendium_Cybersecurity_RO.pdf, consulté le 14.09.2024.

[2328]Conseil de l'Europe, *Convention on Cybercrime*, Budapest, 2001 https ://rm.coe.int/1680081561, consulté le 08.09.2024.

[2329] *Ibidem*.

[2330] V. Hardeveld G., C. Webber, K. O'Hara, *Deviating from the cybercriminal cript: exploring tools of anonymity (mis)used by carders on cryptomarkets*, American Behavior Scientist, 2017.

838. Obligation de coopération transfrontalière. Ces dernières années, les autorités ont déployé des efforts considérables pour prévenir et combattre la cybercriminalité. Il convient de souligner que la cybercriminalité ne connaît pas de frontières géopolitiques et que les états doivent donc améliorer la collaboration et la coopération entre leurs propres organes et repenser la législation numérique.[2331]

Internet n'est plus seulement un moyen de communication, mais a acquis la valeur d'une « plateforme pour lancer des cyberattaques, fournissant des moyens sophistiqués pour enfreindre la loi ». À ce titre, « la diversité et la spécificité des délits dans l'environnement informatique ont imposé une approche spécialisée dans leur enquête, à travers la formation d'équipes d'enquête spécialisées, l'implication de spécialistes, le suivi attentif des suspects et de leurs activités, l'analyse détaillée du lieu du crime, la collecte et l'archivage des preuves, tous sont des éléments essentiels pour une enquête informatique efficace[2332]. »

839. L'importance d'Europol. Europol joue un rôle majeur dans la lutte contre la cybercriminalité et sa prévention. Les difficultés et les défis rencontrés par les services répressifs dans le contexte de la garantie de la cybersécurité et du fonctionnement juridique du dark web sont évidents.[2333] Afin d'améliorer la justice pénale dans l'espace en ligne, il est nécessaire d'harmoniser les procédures nationales permettant d'obtenir des preuves électroniques. Cela impliquerait « une approche commune en coopération avec les FAI (fournisseurs de services en ligne), une simplification des procédures d'entraide judiciaire (MLA) [2334] et une éventuelle refonte de la manière de déterminer la compétence dans l'espace virtuel ».[2335]

840. Application de la Convention de Budapest dans les pays membres. Pour entrer dans des zones sûres pour les criminels, où ils se cachent des enquêteurs, il est nécessaire de réglementer la criminalisation de certains secteurs.[2336] À cet égard, la mise en œuvre de la Convention de Budapest devrait être effectuée dans tous les états signataires, étant donné que les dernières vérifications effectuées par le Comité de la Convention sur la Cybercriminalité

[2331] F. Hare, *Borders in Cyberspace : Can Sovereignty Adapt to the Challenges of Cyber Security ?,* Annales de l'Université George Mason, 2009.
[2332]*Cybercriminalité,* DIICOT Romania. https ://www.diicot.ro/prezentare/ce-investig%C4%83m/5089-criminalitatea-informatic%C4%83
, consulté le 10.12.2024.
[2333]Internet Organised Crime Threat Assessment (IOCTA) European Police Office, 2016. https ://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf .
[2334]Modernizing International Procedures against Cyber-enabled Crimes, https ://www.eastwest.ngo/info/modernizing-international-procedures-against-cyber-enabled-crimes, consulté le 06.09.2024.
[2335] *Ibidem*.
[2336] *Ibidem*.

[2337] ont révélé de nombreuses irrégularités : certains états n'ont pas appliqué la Convention ou le cadre juridique est incomplet ou incompatible avec les dispositions de la Convention.[2338]

Une autre question qui doit être traitée à travers le filtre de cybersécurité est la sécurité des données personnelles. À l'heure actuelle, les données personnelles ont une valeur incontestable et peuvent être considérées comme une « source d'argent sécurisée »[2339]. La réaction naturelle de la société est de rechercher des solutions pour protéger au mieux les données privées, y compris par l'utilisation de logiciels qui empêchent la surveillance sur Internet « dans un avenir où les grandes entreprises continuent de collecter des données de manière non réglementée », indique le rapport. De plus en plus de gens se soucieront de la sécurité de leurs renseignements personnels et migreront vers des logiciels comme Tor. »[2340]

841. Évaluation des menaces dans l'environnement en ligne. Europol rend compte chaque année de ces questions, appelé IOCTA (évaluation des menaces du crime organisé en ligne), qui examine les tendances et les préoccupations en matière de cybercriminalité et fournit des données sur la manière dont la protection des données personnelles est affectée. En outre, ce rapport comprend également des analyses d'autres actions illicites, telles que la fraude en ligne, les cyberattaques ou les délits sur le dark web[2341]. Dans le même temps, des études montrent qu'il n'y a plus de différences très grandes entre le délit classique, celui qui fonctionne hors ligne, et celui qui fonctionne exclusivement dans l'environnement virtuel, en commettant des délits informatiques, les deux types de délit vivant ensemble dans une parfaite symbiose.

842. La lutte des autorités contre la cybercriminalité. Nous assistons à l'évolution d'un nouveau type de crime organisé. À cet égard, il existe actuellement deux tendances : l'introduction de la criminalité organisée traditionnelle dans l'espace numérique et le développement d'une nouvelle forme de criminalité organisée.[2342] L'anonymat continue d'être le moyen le plus simple de commettre une cybercriminalité, compte tenu des avantages qu'il procure aux maléfiques en ligne, raison pour laquelle le crime organisé traditionnel voulait entrer dans le monde numérique.

[2337] Assessing the Implementation of the Budapest Convention, 2016, http ://www.coe.int/en/web/cybercrime/assessments, consulté le 07.09.2024.

[2338] Internet Organised Crime Threat Assessment (IOCTA) European Police Office, 2016. https ://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf, consulté le 07.09.2024.

[2339] F. Hare, *Borders in Cyberspace : Can Sovereignty Adapt to the challenges of Cyber Security ?,* Annales de l'Université George Mason, 2009.

[2340] Localization Lab*, Comprendre et éviter la censure sur Internet*, 2020. https ://www.localizationlab.org/understanding-and-circumventing-network-censorship-ro, consulté le 10.12.2024.

[2341] Europol, *L'évaluation de la menace de la criminalité organisée sur Internet (IOCTA), mises à jour stratégiques, politiques et tactiques sur la lutte contre la cybercriminalité*, disponible sur L'évaluation des menaces de la criminalité organisée sur Internet (IOCTA) | Europol (Europa.eu), consulté le 09.09.2024.

[2342] T. Tropina, *La structure évolutive de la criminalité en ligne. Comment organiser la cybercriminalité*, Eucrim, no. 4, 2012, p.158-165.

Enfin, l'anonymat dans le cyberespace n'est pas une question technique, ni une question juridique naturelle. Pour les pays sous régime totalitaire, la relation entre anonymat et la possibilité d'être identifié est sans entrave. En Corée du Nord, seuls quelques milliers de personnes ont accès au World Web. Cela accentue la vulnérabilité du domaine virtuel aux réglementations nationales.[2343] En Chine, les autorités s'efforcent d'interdire l'anonymisation et la censure des contenus étrangers en ligne[2344]. La mise en place d'un cadre législatif mieux défini pour les conséquences négatives de l'anonymat en ligne ne résout pas le problème en soi, et la société en général doit être impliquée[2345]. Toutefois, dans les états démocratiques, tels que les États membres de l'Union Européenne, l'anonymat reste l'un des plus grands défis pour la société, car les autorités sont en lutte permanente contre le monde de la cybercriminalité[2346].

A. Anonymat en ligne versus identité numérique

843. Identité réelle vs identité numérique. Partant d'une définition de l'identité numérique, il est facile de voir qu'elle englobe en elle-même un ensemble d'informations représentant une personne particulière dans l'espace numérique et consiste, en principe, en nom, adresse, date de naissance, et la façon dont il se comporte en tant qu'utilisateur sur internet.[2347] L'identité numérique est la représentation électronique d'une personne, qu'elle utilise pour accéder à des services sur Internet, pour effectuer des achats en ligne et pour établir des liens avec d'autres personnes.[2348]

[2343] M. Kuhn, *Le droit à l'anonymat dans l'espace numérique*, Humanistische Union, 2019, https ://www.humanistische-union.de/publikationen/vorgaenge/225-226/publikation/das-recht-auf-anonymitaet-im-digitalen-raum-1/?fbclid=IwY2xjawFFSrNleHRuA2FlbQIxMAABHWEEyFIZrE4PDbHU0Lj652UNV0HVwbsbuSjv6h-6O8UqtdrHJa8K0VwhpA_aem_dDRvfufn48NUpjg4PpRNPg, ?, consulté le 10.09.2024.

[2344] J.A. Lee, C.Y. Liu, *Real-Name Registration Rules and the Fading Digital Anonymity in China*, Washington International Law Journal, vol.25, no.1, 2016. https ://digitalcommons.law.uw.edu/wilj/vol25/iss1/3/, consulté le 10.09.2024.

[2345]M. Kuhn, *Le droit à l'anonymat dans l'espace numérique*, Humanistische Union, 2019. « *Faire face aux conséquences négatives de l'anonymat est une tâche de la société dans son ensemble, en particulier en termes de manières, et non un problème qui peut être résolu en éliminant le vide juridique »,* consulté le 10.09.2024.

[2346] T Tropina, *La structure évolutive de la criminalité en ligne, Comment organiser la cybercriminalité*, Eucrim, no. 4, 2012, p.158-165, disponible sur La structure évolutive de la criminalité en ligne - Eucrim, " *Alors que la société de l'information est confrontée au problème de l'harmonisation de la législation sur la cybercriminalité et de la coopération opérationnelle pour les enquêtes sur les infractions et la poursuite des cybercriminels et des groupes criminels organisés dans le cyberespace, les modèles traditionnels et ceux qui ne sont accessibles qu'en ligne restent – et continueront probablement de le rester – quelques pas en avance sur les législateurs et les organismes chargés de l'application de la loi* »*,* consulté le 10.09.2024.

[2347] *Understanding digital identity*, Imprivata, s.d. https ://www.imprivata.com/uk/understanding-digital-identity, consulté le 12.09.2024.

[2348] *Digital identity: The Complete Guide to Digital Identification*, Adnovum.https ://www.adnovum.com/blog/digital-identity, consulté le 13.09.2024.

Il y a une différence majeure entre l'identité d'une personne dans la réalité et celle dans le monde numérique[2349]. Un internaute est un individu qui accède régulièrement à un site Web ou à une plateforme particulière, et un seul utilisateur peut avoir une multitude d'identités numériques.[2350]

844. Le domaine étendu des données et des informations. La notion d'*identité numérique* est souvent confondue avec l'*identité du compte*, comme c'est le cas avec le terme *utilisateur.* L'identité numérique couvre un champ plus large de données et d'informations, tandis que la notion de compte concerne l'action d'authentification pour recevoir l'accès à une plateforme particulière.[2351]

Dans la même note, *l'empreinte digitale numérique* est étroitement liée à l'identité numérique, représentant les « traces » qu'un utilisateur laisse en ligne. Ainsi, chaque fois qu'une personne accède à un site web, publie sur les réseaux sociaux, envoie des e-mails ou ajoute des commentaires, tout cela contribue à façonner une *empreinte digitale.*[2352] Il prend en charge le processus de personnalisation de l'expérience en ligne, car les moteurs de recherche adaptent les résultats à leurs préférences de navigation.[2353]

Les services en ligne et les applications de médias sociaux « partagent constamment des données générées par les utilisateurs sous forme d'informations sur les lieux, les habitudes de navigation, les dossiers de communication, les informations de santé, les informations financières et les préférences générées concernant les activités en ligne et hors ligne de l'utilisateur[2354] ». Ces données sont généralement partagées avec des services tiers afin de fournir au consommateur une expérience personnalisée.[2355]

845. Recommandations législatives. Depuis mars 2009, le Parlement Européen signale dans une recommandation que « *l'identité numérique fait de plus en plus partie intégrante de nous-*

[2349] *Understanding digital identity*, Imprivata, s.d.https ://www.imprivata.com/uk/understanding-digital-identity, « *L'identité personnelle d'un individu est l'ensemble unique de caractéristiques qui définissent cette personne dans le monde physique. En échange, l'identité numérique d'une personne fait référence à son empreinte numérique sur un réseau* », consulté le 12.09.2024.

[2350] *Online user definition*, Law Insider. https ://www.lawinsider.com/dictionary/online-user, consulté le 12.09.2024.

[2351] *What is a digital identity?,* One Identity.https ://www.oneidentity.com/learn/what-is-a-digital-identity.aspx, consulté le 13.09.2024.

[2352] *Managing your digital footprint*, Office of the executive vice chancellor. https ://executivevc.unl.edu/tipsheets/managing-your-digital-footprint, consulté le 14.09.2024.

[2353] *Digital footprint: definition, examples and ways reduce*, Verizon. https ://www.verizon.com/about/blog/digital-footprint-definition-examples-and-ways-reduce, consulté le 14.09.2024.

[2354] S. Puglisi, D. Rebollo-Monedero, J. Forne, *On the Anonymity Risk of Time-Changing User Profiles*, Entropy 2017. https ://doi.org/10.3390/e19050190, consulté le 14.09.2024.

[2355] *Ibidem*.

mêmes » et mérite dans ce contexte la protection la plus efficace en cas d'intrusion extérieure, qu'il s'agisse de gouvernements ou d'organismes privés[2356].

Les données relatives à l'identité numérique devraient bénéficier d'une protection et d'une sécurité, ce qui exige qu'elles soient considérées comme *des droits personnels inaliénables, inaliénables et non économiques*.[2357] Ceci est pertinent pour l'anonymat, les pseudonymes et la protection de la vie privée.

À cet égard, il convient de noter qu'il n'existe pas de reconnaissance juridique de l'identité numérique, mais que les droits de l'homme en tant qu'identité physique s'appliquent *in extenso* à ce profil.[2358] Ainsi, parmi les droits inhérents de l'homme, avec une application directe dans l'espace virtuel, il y a le droit à l'honneur, à la dignité, à la réputation, à la vie privée et à l'image propre, droits reconnus à la fois par la Déclaration Universelle des Droits de l'Homme et par la Convention Européenne des Droits de l'Homme.

846. Identité vs anonymat en ligne. Quant à la différence entre identité numérique et anonymat en ligne, elle est mise en évidence au niveau de l'identification des personnes. Ainsi, l'authentification implique que l'utilisateur accepte que son identité soit divulguée, à l'aide d'une adresse e-mail, d'une adresse IP ou d'un numéro de téléphone.[2359] En revanche, l'anonymat donne au consommateur l'avantage de ne pas être déterminé par les applications ou les plateformes auxquelles il accède.[2360]

Un aspect intéressant est la liberté d'expression, transposée à travers le filtre de l'identité numérique vs l'anonymat en ligne. En ce qui concerne ce dernier, j'ai traité de la discussion dans la sous-section consacrée à l'anonymat en ligne, dans laquelle j'ai capturé « la désinhibition de l'homme dans un contexte où son identité n'est pas connue ». Cette désinhibition concerne non seulement la liberté d'expression et d'opinion, mais encourage également le harcèlement, *le trolling* et les discours haineux.[2361]

[2356] Parlement Européen, *Recommandation du Parlement Européen du 26 mars 2009 au Conseil relative au renforcement de la sécurité et des libertés fondamentales sur l'internet*, disponible à l'adresse https ://www.europarl.europa.eu/doceo/document/TA-6-2009-0194_EN.html, consultée le 14.09.2024.

[2357] Parlement Européen, *Recommandation du Parlement Européen du 26 mars 2009 au Conseil relative au renforcement de la sécurité et des libertés fondamentales sur l'internet*, disponible à l'adresse suivante : https ://www.europarl.europa.eu/doceo/document/TA-6-2009-0194_EN.html.

[2358] *What defines your digitall identity and what legal rights are associated with it*?, Signaturit Group, 2024. https ://www.signaturit.com/blog/what-defines-your-digital-identity-and-what-legal-rights-are-associated-with-it/?fbclid=IwY2xjawFOqrhleHRuA2FlbQIxMAABHevl72a-Xxjoe2Wb_3r0i_-m_HpkKnZB-wx-nuyftKsGGk3GEJkxUHJsMA_aem_BpwwzCX92GCWSWbySXZltw, consulté le 14.09.2024.

[2359] I. Ciobotaru, *Anonyme et authentifié: identité numérique sur internet ouvert*, Medium, 2020.

[2360] *Ibidem*.

[2361] S. Kisters, *Ethical Dilemma of Online Anonymity: Impact, Challenges, and Solutions*, 2023, disponible sur https ://originstamp.com/blog/the-ethical-dilemma-of-online-anonymity/, consulté le 13.09.2024.

En termes d'identité numérique, la liberté d'expression est plus censurée, impliquant un certain degré de responsabilité et d'assumation, ce qui est compréhensible étant donné que l'auteur peut être identifié et tenu responsable[2362].

847. L'identité en ligne, une arme contre la cybercriminalité. Dans le contexte de la cybersécurité, l'identité numérique soutient la lutte contre la criminalité[2363], tandis que l'anonymat prolifère les activités illicites, représentant l'un des ennemis les plus puissants des autorités. Les discussions juridiques sur la création d'une plateforme nationale d'identité numérique ont soulevé des inquiétudes[2364] quant à d'éventuelles attaques visant la confidentialité des données.

848. Non-conformités entre l'identité réelle et l'identité numérique. Les plateformes de médias sociaux telles que Facebook, Instagram ou Twitter[2365] ont des politiques et des règles strictes, et ne peuvent être utilisées qu'en créant un compte. Bien que la sécurité sur ces sites Web ait été développée, l'inconvénient est que n'importe qui peut générer un compte avec de fausses informations sur des noms, des études, des adresses,[2366] qui ne sont pas passés par une analyse préalable.[2367] Ainsi, l'anonymat est masqué par des données irréelles, générant une identité numérique qui n'est pas conforme à l'identité réelle.

À cet égard, les plateformes de services en ligne ont mis en place une stratégie de vérification de la véracité des informations. Ainsi, les utilisateurs qui ont des identités différentes sur différentes applications utiliseront ces données pour confirmer l'identité sur une troisième plate-forme.[2368] Par exemple, les utilisateurs de Facebook utiliseront souvent cette interface pour accéder à Instagram, d'autant plus que les deux sites Web appartiennent à Meta.

[2362] N. Dutta, S. Mojtahedi, *Navigating the Risks and Rewards of Digital ID Systems*, Open Government partnership, 2024. https ://www.opengovpartnership.org/stories/navigating-the-risks-and-rewards-of-digital-id-systems/, consulté le 14.09.2024.

[2363] M.-J. Sule, M. Zendaro, G. Thomas, *Cybersecurity through the lens of Digital Identity and Data Protection : Issues and Trends,* Technology in Society, vol. 67, 2021, https ://doi.org/10.1016/j.techsoc.2021.101734, consulté le 14.09.2024.

[2364] B. Scaria, *L'importance d'un système national d'identité numérique, ISACA, 2022. «* Une plateforme nationale d'identité numérique comporte un risque important pour la cybersécurité et la vie privée. Pour atténuer les risques, une approche robuste et globale doit être adoptée pour identifier une personne dans un cadre réel et pour s'assurer que les risques en ligne sont effectivement réduits ». https ://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/the-importance-of-a-national-digital-identity-system?gad_source=1&gclid=CjwKCAjwxY-3BhAuEiwAu7Y6swLHm3dxytGE6l-tOgeLQJpjgkdEAj226OK9j0NniUBcS4Eo5E6XKRoCmz4QAvD_BwE, consulté le 14.09.2024.

[2365] Gilad Edelman, *Facebook and Twitter Want to Keep the Justice System Stacked Against Defendants*, juin 2020, disponible sur https ://www.wired.com/story/facebook-twitter-criminal-justice-stored-communications-act/, consulté le 14.09.2024.

[2366] Martin Moore, *Fake accounts on social media, epistemic uncertainty and the need for an independent auditing of accounts,* février 2023, disponible sur https ://doi.org/10.14763/2023.1.1680, consulté le 13.09.2024.

[2367] https ://www.juridice.ro/692759/atestarea-identitatii-digitale-acum-si-in-blockchain.html, consulté le 15.09.2024.

[2368] Jain P., Ponnurangam K., Anupam J, *Identifying users across multiple online social networks,* à la XXe Conférence Internationale sur le World Wibe Web, mai 2013, pp. 1259-1268.

Dans ce cas, « la demande de données personnelles par une application renforce la crédibilité pour la deuxième plateforme que les données initialement saisies sont correctes ».[2369]

Ainsi, l'activité d'une personne sur un site Web particulier peut révéler son identité sur une autre page, en utilisant également les emplacements des publications téléchargées sur ces plateformes.[2370] Par conséquent, un individu qui crée un faux profil aura de la difficulté à accéder à d'autres applications, l'anonymat gagnant de moins en moins de terrain dans le Web de surface.

849. Mécanismes de protection. La prévalence accrue des cybermenaces et des violations de la vie privée a nécessité la mise en place de mécanismes de protection de l'identité numérique.[2371] Comprendre la cybersécurité part d'une hypothèse de base : nous sommes tous des cibles d'intérêt pour les attaques de pirates informatiques.[2372]

L'Union Européenne dispose déjà d'un ensemble assez complet de règles de protection de l'identité[2373]. À cet égard, l'instrument de base est le RGPD[2374] – *le Règlement sur la protection des données à caractère personnel*, étant un acte normatif universellement contraignant avec les résultats les plus efficaces dans le domaine.[2375]

Le RGPD donne aux utilisateurs le droit d'exiger des organisations qu'elles suppriment les données personnelles lorsqu'elles considèrent qu'elles ne sont plus nécessaires pour l'objectif initial ou qu'elles ne s'identifient plus à elles.[2376] Ainsi, l'identité et l'empreinte numérique peuvent subir des changements, s'adaptant au comportement de l'utilisateur dans l'environnement en ligne et hors ligne.

[2369] S. Puglisi, D. Rebollo-Monedero, J. Forne, *On the Anonymity Risk of Time-Varying User Profiles*, mars 2017, « *Une information demandée par un service pourrait en fait ajouter de la crédibilité aux informations fournies par l'utilisateur pour une deuxième application, démontrer que certaines données personnelles se chevauchent et ajouter d'autres informations* », disponible sur https ://doi.org/10.3390/e19050190, consulté le 14.09.2024.

[2370] S. Puglisi, D. Rebollo-Monedero, J. Forne, *On the Anonymity Risk of Time-Varying User Profiles*, mars 2017, disponible sur https ://doi.org/10.3390/e19050190, consulté le 15.09.2024.

[2371] S. Kisters, *Protecting Digital Identity : Ensure Human Rights Online – Practical Strategies and Cybersecurity Measures*, juillet 2023, disponible sur https ://originstamp.com/blog/protecting-digital-identity-ensuring-human-rights-online/, consulté le 15.09.2024.

[2372] M.-J. Sule, M. Zendaro, G. Thomas, *Cybersecurity through the lens of Digital Identity and Data Protection : Issues and Trends,* Technology in Society, vol. 67*,* 2021, disponible sur https ://doi.org/10.1016/j.techsoc.2021.101734, consulté le 15.09.2024.

[2373] E. Michalkiewicz-Kadziela, E. Milczarek, *Legal boundaries of digital identity creation*, Internal Policy Review, vol.11, 2022. « En ce qui concerne la législation en vigueur au niveau de l'Union Européenne, la protection de l'identité la plus complète est assurée par des dispositions relatives à la protection des données à caractère personnel », disponible sur https ://doi.org/10.14763/2022.1.1614, consulté le 14.09.2024.

[2374] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la directive 95/46/CE (Règlement général sur la protection des données) .

[2375] E. Michalkiewicz-Kadziela, E. Milczarek, *Legal boundaries of digital identity creation*, Internal Policy Review, vol.11, 2022.

[2376] *Le droit à la vie privée à l'ère numérique*, blog.eset.ro, 2017. https ://blog.eset.ro/confidentialitate/dreptul-la-viata-privata-in-era-digitala/, consulté le 15.09.2024.

850. L'anonymat, préféré des criminels. Avec une vue comparative, il est évident que certaines personnes aspirent à l'anonymat en ligne. Étant donné que l'approche de l'identité numérique implique le stockage centralisé des données personnelles par le système national[2377], les criminels seront toujours enclins à l'anonymat ou aux pseudonymes. Cependant, cela n'est pas interdit par la loi, du moins pas dans les États membres de l'UE, mais au contraire, c'est un droit garanti aux citoyens de l'Union Européenne.[2378]

a). Dark web/deep web

851. Réseaux numériques. Grâce à l'anonymat qu'Internet offre aux utilisateurs, en particulier grâce à l'utilisation de systèmes tels que TOR, *dark web* et *deep web* environnements impliquent plusieurs problèmes qui ont un effet sur la vie privée. Une brève distinction entre les deux types de réseaux doit être exposée[2379].

Deep Web fait référence à tout ce qui sur Internet n'est pas indexé par les moteurs de recherche comme Google. Le contenu *deep web* inclut tout ce qui se trouve derrière un pare-feu de paiement ou qui nécessite des identifiants de connexion. Il inclut également tout contenu dont ses propriétaires ont bloqué l'indexation des *web crawler*[2380]. Les dossiers médicaux, le contenu fiscal et les pages web confidentielles de l'entreprise ne sont que quelques exemples qui composent *le deep web.* Les estimations placent la taille du *deep web* entre 90% et 95% de l'Internet[2381]. Sur ce réseau peuvent être trouvés même du contenu tels que des publications ou d'autres études de nature académique et scientifique. Seule une petite partie d'Internet est accessible via un navigateur Web standard – généralement connu sous le nom de « web clair ».

852. Internet, catalyseur des activités et de la qualité de vie. Sans aucun doute, à l'ère de la technologie, Internet a grandement facilité les activités et le niveau de vie de la société. Cependant, l'évolution de la technologie a créé un environnement propice à l'émergence de

---

[2377] B. Scaria, *The Importance of a National Digital Identity System*, ISACA, 2022. disponible sur https ://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/the-importance-of-a-national-digital-identity-system?gad_source=1&gclid=CjwKCAjwxY-3BhAuEiwAu7Y6swLHm3dxytGE6l-tOgeLQJpjgkdEAj226OK9j0NniUBcS4Eo5E6XKRoCmz4QAvD_BwE?utm_source=isaca_internal&utm_medium=share_link, consulté le 30.08.2024.

[2378] M. Kuhn, *Das Recht auf Anonymitat im digitalen Raum*, Humanistische Union, n° 225/226, 2019, pp. 43-56.

[2379]D. Guccione, *What is the dark web? How to access it and what you'll find*, CSO, 2024. https ://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html consulté à 25.08.2020

[2380] Crawler Web = Logiciel qui navigue systématiquement sur les pages Web pour les indexer pour la formation de liens

[2381] *23 Dark Web Statistics to Investigate in 2023*, Web tribunal, 2023. https ://webtribunal.net/blog/dark-web-statistics

nouvelles menaces. L'innovation à l'ère numérique est certainement une arme à double tranchant, selon la personne derrière l'anonymat.[2382]

Internet ne pouvant être utilisé qu'à des fins pacifiques, les criminels ont tiré le meilleur parti des possibilités offertes par l'évolution et la mondialisation, en concentrant toute leur attention sur le développement de réseaux générant d'énormes profits. La grande majorité des consommateurs en ligne naviguent sur ce qu'on appelle le *Web de surface (Surface Web)*, sans même savoir que cette plateforme apparemment riche et encombrante ne représente que 5 à 10 % du contenu sur Internet. On pourrait comparer la *Surface Web* à la pointe d'un iceberg, dont les dimensions se cachent dans les profondeurs (d'où le nom *DeepWeb*).[2383]

Ainsi, *Surface Web* est l'Internet connu de tous les utilisateurs, utilisé à des fins diverses, de la conduite des affaires et de la participation à des cours spécialisés, à la connexion avec la famille et les amis. En dehors du *Surface Web,* mais aussi au sein du World Wide Web (WWW), se cachent le *Deep Web* et le *Dark Web*, deux arènes d'Internet, souvent mal comprises par la population et même confuses.[2384]

853. Réseaux cachés. Le *Deep Web* héberge principalement des sites bénins, tels que des bases de données, des pages Web protégées par mot de passe ou des intranets.[2385] L'essence de ce portail est que le Deep Web n'est pas indexé par les moteurs de recherche classiques comme Google ou Yahoo, c'est pourquoi il est souvent associé à des activités illicites. Cependant, la plupart de ses contenus sont légitimes et comprennent des données qui nécessitent un certain degré de sécurité et de confidentialité.[2386]

Dark Web est un sous-ensemble du *deep web* qui est intentionnellement caché, nécessitant l'accès à un navigateur spécifique - TOR. Ce navigateur utilise un système de navigation qui nécessite une multitude d'adresses IP, ce qui donne à l'utilisateur l'anonymat. D'où le nom « oignon », se référant aux couches protectrices sous lesquelles se trouve celui qui navigue dans TOR. Personne ne connaît vraiment la taille du dark web, mais la plupart des estimations le placent à environ 5% de l'internet total. En outre, le *réseau sombre* tout entier n'est pas utilisé à des fins illicites, malgré son nom péjoratif.

[2382] V.C. Voinea, *Les ténébres du réseau. Deep Web et Dark Web,* Intelligence*,* 2022.

[2383] *Everything you should know about the Dark Web,* Tulane University, s.d. https ://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web, consulté le 31.08.2024.

[2384]P. Hoelscher, *What is the difference between the surface web, the deep web and the dark web*?, Infosec, 2018. https ://www.infosecinstitute.com/resources/general-security/what-is-the-difference-between-the-surface-web-the-deep-web-and-the-dark-web/, consulté le 04.09.2024.

[2385] C. Grannan, *What's the Difference between Deep Web and Dark Web?,* Britannica, https ://www.britannica.com/story/whats-the-difference-between-the-deep-web-and-the-dark-web, consulté le 04.09.2024.

[2386] K. Baker, Deep Web vs Dark Web: what's the difference?, Cybersecurity 101, 2024. https ://www.crowdstrike.com/cybersecurity-101/the-dark-web-explained/deep-web-vs-dark-web/, consulté le 04.09.2024.

854. Dark web, énigmes juridiques. En ce qui concerne le concept de *dark web*, un certain nombre de questions juridiques se posent. Il convient de noter d'emblée que les règles en vigueur ne font pas de distinction entre l'internet de surface et l'internet le moins connu. Ces réseaux privés rendent manifestement difficile l'identification de l'auteur en cas de délits informatiques. La plupart des problèmes découlant de l'utilisation du réseau *dark web* sont liés à la portée du droit pénal. Ainsi, il peut s'agir de cybercriminalité financière (utilisation de crypto-monnaies), de délits contre la vie privée ou de délits contre les actifs informatiques. Comme la première catégorie est de plus en plus préoccupée par les infractions de blanchiment d'argent par le biais de crypto-monnaies, nous concentrerons notre attention sur les délits contre la vie privée et, implicitement, les données personnelles qui sont menacées par l'utilisation de ces réseaux Internet.

Le *Dark Web* est la partie orageuse, sombre et anonyme de l'Internet, régie par le principe de la protection de la vie privée, contexte favorable à la perpétration des délits les plus sombres, y compris le trafic de drogue, la prostitution, la traite des êtres humains, la pornographie enfantine, la torture, les assassinats sur commande, les armes, mais aussi les cyberattaques.[2387] Dans la même note, cette interface fournit un réel soutien aux enquêteurs pour la découverte de nombreuses activités illicites et la prévention des tragédies.

855. Réseaux cachés, mode d'accès. L'accès aux deux plateformes, deep web et dark web, se fait via le navigateur TOR – le routeur Onion, dont la configuration permet la connexion au réseau Onion. TOR est un logiciel open-source et open-access, un réseau de tunnels virtuels qui garantissent la confidentialité et la sécurité sur Internet, ce qui rend difficile le suivi de la source.[2388]

856. Aide gouvernementale au développement du Dark Web. Quant aux débuts du Dark Web, malgré les apparences, l'histoire de ce courant a une influence gouvernementale. Au milieu des années 1990, ce qui est connu sous le nom d'« Onion Routing » a été développé et financé par le gouvernement fédéral des États-Unis, ce qui a permis au navigateur Tor de protéger l'identité des utilisateurs.[2389]

857. Le logiciel TOR. *The Onion Routing* ou « le routage de l'oignon » est un logiciel ou un réseau qui prend en charge le mode perfectionné de communication anonyme sur la plate-forme Internet par cryptage « en couches », qui transmet « des paquets de données à travers plusieurs nœuds de réseau, éliminant une couche de cryptage à chaque nœud ». Ce mode de fonctionnement est destiné à assurer à l'utilisateur que les données restent cryptées, tandis que

[2387] S. Kaur, S. Randhawa *Dark Web : A Web of Crimes*, Springer Nature, 2020.
[2388] *Despre TOR Browser*, TOR-manual. https ://tb-manual.torproject.org/ro/about/, consulté le 07.09.2024.
[2389]B. Acton, *The origins and history of the Dark Web*, IdentityIQ, 2024. https ://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/, consulté le 05.09.2024.

l'identité de l'expéditeur reste protégée. L'essence de ce processus est d'ouvrir des messages et des réponses avec des clés différentes, avec une clé unique pour chaque serveur. L'utilisateur a accès à toutes ces clés, mais les serveurs n'ont accès qu'à leur clé de chiffrement/déchiffrement spécifique. Par conséquent, puisque chaque message est enveloppé sous des couches de chiffrement et doit être déchiffré couche par couche, ce processus est similaire aux feuilles d'oignon.[2390]

Il existe également une deuxième variante pour l'étymologie du nom *« oignon ».* Selon elle, le navigateur a été créé et développé pour être utilisé par les forces armées américaines pour sécuriser les secrets lors de missions à l'étranger, représentant une stratégie de codage multicouche. Le principe de fonctionnement est l'existence de plusieurs structures multicouches, qui permettent à l'utilisateur de connaître la source précédente et suivante, mais pas la source d'origine ou de destination.[2391]

858. Quand TOR est remplacé par VPN. Dans certains cas, TOR semble inefficace pour accéder à certains sites sur le Dark Web, et d'autres outils sont nécessaires, tels que VPN – réseaux privés virtuels ou autres programmes sécurisés. Un VPN est un réseau privé qui utilise des réseaux publics, développant un « tunnel » virtuel à travers lequel l'information « voyage » pour transmettre des données d'une structure à une autre.[2392] Selon Europol[2393], après les proxys, les VPN et les TOR comptent parmi les technologies les plus utilisées par les cybercriminels. L'exploitation de zones beaucoup plus sombres est souvent réalisée en utilisant simultanément plusieurs VPN, proxys et le navigateur TOR, précisément pour obtenir une protection avancée de l'identité.

b). Développement de marchés noirs virtuels

859. Le développement des marchés noirs, l'aide des cryptomonnaies. Bien que TOR dispose d'un certain nombre d'outils ou de fonctionnalités qui assurent la sécurité des gens, l'anonymat qu'il offre est exploité principalement avec une intention illicite. Le dark web a certainement facilité le développement de marchés noirs virtuels, et les criminels ont profité de cette opportunité, d'autant plus que les paiements sont effectués dans un système crypté, en

[2390] R. Dingledine, N. Mathewson, P. Syverson, « *Tor: The Second-Generation Onion Router* », USENIX Security, 2004 (spec. tehnic Tor). https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.pdf
[2391] D. Yadav, S. Saxena, B. Bhushan, *The Dark Web : A dive into the darkest side of the Internet.* International Conference on Innovative Computing & Communications *ICICC, 2020*, Disponible sur SSRN : https ://ssrn.com/abstract=3598902 ou *http ://dx.doi.org/10.2139/ssrn.3598902*, consulté le 02.09.2024.
[2392] *What is a VPN? How it works, types, and benefits*, Kaspersky. https ://kaspersky.com/resource-center/definitions/what-is-a-vpn, consulté le 07.09.2024.
[2393] Site-ul Europol, https ://www.europol.europa.eu/, consulté le 07.09.2024.

utilisant des monnaies numériques (telles que Bitcoin ou d'autres crypto-monnaies) non réglementées et difficiles à suivre.[2394]

Mais avant l'invention de la crypto-monnaie, la réalisation de transactions illicites sur le dark web se heurtait à de nombreux obstacles, car la localisation des consommateurs se faisait facilement à des milliers de kilomètres, et aucune des parties impliquées dans l'opération ne voulait s'exposer au risque d'utiliser des cartes de crédit ou PayPal.[2395] La crypto-monnaie était la solution à ce problème, et avec elle, les ventes illégales sur le dark web ont explosé.[2396]

Afin de lutter contre le phénomène criminel, « l'enquête et l'abolition des sites illégaux seraient plus efficaces que l'enquête sur leurs utilisateurs ». [2397]

860. Exemples de marchés noirs. Dans le paradigme de l'application de la réglementation sur la protection de la vie privée, le dark web est devenu la principale source d'attaques criminelles, étant le principal moyen de mener des activités criminelles. Parmi les connaisseurs, la plate-forme dark web est appréciée comme étant adaptée « au commerce illégal le plus sûr de substances illicites et dangereuses, où la monnaie est la crypto-monnaie (Bitcoin, Ripple, Ethereum, etc.) ».[2398] Les marchés noirs tels que Silk Road, Agora, Alpha Bay et Dream Market jouissent depuis longtemps d'une notoriété parmi les trafiquants et les usagers de drogue, mais malgré l'anonymat, les agents du FBI ont réussi à identifier et à fermer certains d'entre eux.

861. Trafic illégal, y compris le trafic d'êtres humains. Sur une note négative, le dark web est également connu pour la traite des êtres humains. La traite des êtres humains a souvent été promue sur le Web de surface, sur des plateformes telles que Facebook ou Craiglist, mais le côté obscur d'Internet a été utilisé pour recruter des individus.[2399] La monnaie numérique, VPN et TOR ont soutenu l'expansion de la traite des êtres humains[2400], une forme d'esclavage moderne.[2401]

[2394] B. Acton, *The origins and history of the dark web*, IdentityIQ, 2024 sur https ://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/, consulté le 02.09.2024.
[2395] E. Kastner, *History of the Dark Web (timeline),* History of the Dark Web, 2020. consulté le 02.09.2024.
[2396] *Ibidem*.
[2397] V.C. Voinea, *Les ténébres du réseau. Le Deep Web et le Dark Web* Intelligence, 2022. disponible sur https ://intelligence.sri.ro/tenebrele-retelei-deep-web-si-dark-web/, « en raison du haut anonymat qu'il procure, le Dark Web est un environnement favorable à toutes sortes d'activités, qu'elles soient légales ou illégales. Réglementer ce domaine pour les autorités est un processus extrêmement difficile et laborieux, mais nécessaire pour assurer la sécurité des utilisateurs ordinaires et lutter contre les phénomènes criminels qui se sont répandus dans cet espace », consulté le 03.09.2024
[2398]*Business on the dark web : deals and regulatory mechanisms,* SecureList, 2023. https ://securelist.com/dark-web-deals-and-regulations/109034/ consulté le 10.11.2024.
[2399] R.S. Portnoff, *The Dark Net : De-anonymization, classification and analysis*, UC Berkeley, 2018. disponible sur https ://escholarship.org/uc/item/50c7k0cr, consulté le 03.09.2024.
[2400] T. Felipe, *The digital and physical footprint of dark net markets*, Journal of International Marketing, no. 28(1), 2020. pp. 66-80, disponible à l'adresse suivante : https ://doi.org/10.1177/1069031X19898678, consulté le 03.09.2024.
[2401] J. K. Graham, *The Dark Web and Human Trafficking*, Liberty University, 2022, p. 17.

La fuite d'informations implique que des données telles que des secrets personnels, financiers ou gouvernementaux sont divulguées de manière erronée sans autorisation. Le dark web encourage de telles activités, étant le paradis des pirates informatiques, qui profitent des vulnérabilités logicielles, des infrastructures défectueuses ou des politiques faibles.[2402]

862. Programmes contre la pornographie infantile. La pornographie mettant en scène des enfants est une autre activité qui entre dans le cadre de la traite et de l'exploitation des personnes vulnérables. En 2011, Europol s'est associé à pas moins de 13 pays dans le cadre de l'opération Rescue, qui s'est concentrée sur le matériel pédopornographique téléchargé sur le dark web.[2403] Actuellement, les États membres ont lancé un programme global de lutte contre la criminalité internationale sous le nom d'EMPACT (European Multidisciplinary Platform Against Crimimal Threats - plateforme européenne multidisciplinaire contre les menaces criminelles), une initiative en matière de sécurité dont l'un des principaux objectifs[2404] est la dissuasion de la cybercriminalité à l'encontre des mineurs.

863. Activités illégales possibles sur le dark web. Nous mentionnons également le concept de « red rooms » du dark web, une plateforme adjacente où les utilisateurs sont censés regarder en direct des actes de criminalité, d'agression, de suicide ou de pornographie juvénile.

Pour des raisons pratiques, il est également nécessaire de présenter la méthode illicite de *proxying*, utilisée pour déformer la réalité des informations présentées sur différentes plateformes. Fondamentalement, les criminels poussent les consommateurs dans les éros en présentant des informations irréelles sur une page qui semble légitime afin de les rediriger vers ce site Web « fantôme » créé pour effectuer des paiements. Ainsi, lorsque le paiement est effectué, l'argent est redirigé vers le compte des criminels, bien qu'apparemment les clients reçoivent la confirmation de paiement du site copié, semblable au site légitime.

Tout aussi inquiétant est le trafic d'armes sur la « plate-forme sombre », un problème mondial qui menace le respect des normes, les missions de police et la sécurité de la population.[2405] Europol soutient étroitement les États membres dans la lutte contre les organisations criminelles dont l'activité est le trafic illicite d'armes et d'explosifs. Dans le même

---

[2402] Abnormal AI, *What is a Data Leak? How they happen and how top revent them*, Glossary, s.d. https ://abnormalsecurity.com/glossary/data-leak, consulté le 12.09.2024.

[2403] C. Gannon, A. Blokland, S. Huikuri, K. M. Babchishin, R. Lehmann, *Child sexual abuse material on the darknet*, Forens Psychiatr Psychol Kriminol, 2023. disponible sur https ://doi.org/10.1007/s11757-023-00790-8 , consulté le 12.09.2024.

[2404] Europol, *Child sexual exploitation*. https ://www.europol.europa.eu/crime-areas/child-sexual-exploitation, « En tant que forme de cybercriminalité, l'exploitation sexuelle des enfants est l'une des priorités de l'UE dans la lutte contre la criminalité grave et organisée dans le cadre d'EMPACT 2022-2025 » - consulté le 12.09.2024.

[2405] R. Broadhurst, J. Foye, C. Jiang, M. Ball, *Illicit firearms and other weapons on darknet markets*, l'Institut Australien de Criminologie, 2021. disponible sur https ://www.aic.gov.au/sites/default/files/2021-03/ti622_illicit_firearms_and_other_weapons_on_darknet_markets.pdf, consulté le 09.09.2024.

temps, Europol s'occupe de la lutte contre le terrorisme en collaboration directe avec les autorités judiciaires nationales[2406].

Ainsi, le dark web est le centre principal pour l'exécution de diverses activités criminelles. Bien sûr, le nombre de délits est beaucoup plus élevé, y compris, parmi ceux déjà mentionnés, le clonage de sites web, la fraude bancaire, la falsification, les assassinats, l'espionnage, chantage et autres.

864. Évolution des instruments de lutte. L'avenir du dark web est incertain, car il continue de progresser et de s'adapter aux nouvelles technologies et aux nouvelles formes de répression. L'ingéniosité des criminels facilite la création d'autres moyens de chiffrement et d'anonymisation pour contrer l'évolution des outils d'application de la loi et de surveillance gouvernementale.[2407]

Dans la même note, les organismes compétents continueront de lutter contre la cybercriminalité sur le dark web en investissant dans des ressources et des technologies pour les soutenir dans le processus de surveillance et de lutte contre la criminalité en ligne, ainsi qu'en renforçant la coopération transfrontalière.[2408]

En ce qui concerne les délits contre la vie privée, nous pouvons mener l'analyse dans deux directions principales : violation de la correspondance et violation du respect de la vie privée[2409].

c). Silk Road, « supermarché » en ligne pour les délits

865. Le dark web et la responsabilité pénale. L'article 323-3 le Code pénal français criminalise l'introduction frauduleuse de données dans un système de traitement automatisé[2410], l'extraction, la conservation, la reproduction, la transmission, la transmission, la transmission de données, suppression ou modification frauduleuse de ces données. La question d'intérêt est

[2406] Europol, *Le trafic illicite d'armes à feu*, disponible à l'adresse https ://www.europol.europa.eu/crime-areas/illicit-firearms-trafficking, « Dans le cadre d'une stratégie plus large visant à identifier les réseaux criminels fournissant des armes à feu et des munitions aux groupes terroristes, les experts d'Europol travaillent en étroite collaboration avec des experts de la lutte contre le terrorisme dans le domaine des investissements internationaux *»,* consulté le 09.09.2024.

[2407]B. Acton, *The origins and history of the Dark Web*, IdentityIQ, 2024. https ://www.identityiq.com/digital-security/the-origins-and-history-of-the-dark-web/, consulté le 10.09.2024.

[2408] *Ibidem*.

[2409] O. de Maison Rouge, *Les cyberisques. La gestion juridique des risques à l'ère immatérielle*, LexisNexis, 2018. p. 155-165.

[2410] M.-C. Sordino, « Les collectivités territoriales face au risque pénal en cas d'atteinte à la cybersécurité », La Semaine juridique – Administrations et collectivités territoriales, n° 21, 27 mai 2024, étude 2150 : „connaître les fondements de l'engagement de la responsabilité pénale liée, soit aux systèmes de traitement automatisé des données, soit aux infractions pénales classiques, peut permettre de prévenir certains comportements, avant le déclenchement de la répression"

étroitement liée à la façon dont les criminels opèrent à travers le réseau *du dark web*. Lorsqu'une personne est victime de cyberattaques, les auteurs cryptent les données de la personne concernée et demandent une rançon. Après le transfert demandé, la partie lésée reçoit un code pour déverrouiller les données personnelles bloquées par les pirates. Un premier cas de condamnation pour délits commis par le biais du *dark web* a eu lieu en 2017, lorsque l'administrateur d'un site Web de ce réseau a été condamné à une peine de prison.

Nous nous référons, dans ce cas, à Silk Road, le « supermarché » en ligne pour les crimes. La sentence prononcée contre son fondateur, Ross William Ulbricht, connu sous le nom de Dread Pirate Roberts, a été confirmée par la Cour d'appel de New York le 31 mai 2017. Il a été condamné à la prison à perpétuité sans possibilité de libération. Cet arrêt soulève des questions sur les moyens juridiques dont dispose la France (et la Roumanie) pour faire face à ce type d'infractions[2411].

Le site Web *Silk Road (route de la soie)* a été fermé pour la première fois en 2013 et a été considéré comme « eBay of crime ». Elle a généré un chiffre d'affaires de 1,2 milliards, dont 80 millions ont été perçus par ses administrateurs. Les utilisateurs du site pourraient obtenir des drogues, des faux documents, des armes ou même des « kits de logiciels malveillants » pour pirater divers ordinateurs. Le site fonctionnait via le réseau TOR, ce qui lui permettait de crypter et d'anonymiser les flux d'informations grâce à un réseau de serveurs actif dans le monde entier. Le site a agi en tant que tiers intermédiaire, agissant comme « escrow », qui a facturé des commissions entre 8% et 15% pour chaque transaction effectuée[2412]. Le paiement se fait en Bitcoin, une crypto-monnaie basée sur la technologie blockchain et qui garantit la discrétion des transactions. Pour Silk Road, les administrateurs eux-mêmes ont joué ce rôle. Ainsi, ils s'assuraient que le vendeur recevait son argent et que l'acheteur recevait ce qu'il avait commandé. Une fois la transaction terminée, un système d'évaluation a été mis en place pour évaluer la confiance du vendeur et de l'acheteur. Ce processus est très courant sur *le Dark Web* car la confiance n'est pas la règle, seulement l'exception.

866. Peine d'une sévérité exceptionnelle. Le premier signe qui a donné une trace aux enquêteurs était un utilisateur (sous le pseudonyme d'Altoid) qui a mentionné plusieurs fois sur d'autres plateformes le nom du site et les possibilités que ceux qui y accèdent peuvent avoir. L'accusé de 33 ans a été condamné à la prison à perpétuité le 29 mai 2015, après un procès de treize jours. La principale qualification adoptée par la Cour d'appel est le trafic de drogues et

[2411] É. Caprioli, *Droit pénal et Dark Web,* LexisNexis Jurislasseur, 2017.
[2412] A. Petit, *Guided tour of the cybercriminal Dark Web*, éd. Dalloz IP/IT, n°2, 2017, p. 91.

les infractions connexes découlant de la création et de l'utilisation d'une plateforme de commerce électronique[2413].

Si les actions de l'accusé avaient été jugées en droit français, la solution correcte aurait été d'invoquer l'article 323-3 du Code pénal. Par conséquent, considérant que l'article pénalise l'introduction frauduleuse de données dans un système automatisé de traitement de données, ainsi que l'extraction, la possession, la reproduction, la transmission, la suppression frauduleuse et la modification de ces données, la règle d'incrimination aurait été fortuite. La modification des données aurait été opérable, car ces données sont cryptées (dans notre cas) par une tierce personne de sorte qu'elles sont inutilisables. Si le délit est commis en groupe organisé, ce qui est très courant pour les délits commis sur le *dark web*, les peines sont plus sévères, selon les articles 323-4 et 323-4-1 du Code pénal[2414].

d). Groupes organisés démantelés par la justice française

867. En 2018, les autorités françaises ont ordonné la fermeture d'un site Internet fonctionnant sur *le Dark Web,* à travers lequel les utilisateurs avaient facilement accès, entre autres, aux stupéfiants, aux armes, aux faux documents et aux données bancaires. Il s'agit du site « Black Hand » (la main Noire), qui était géré par une personne utilisant le système de cryptage TOR. Dans l'affaire ont été détenus plusieurs personnes, l'administrateur du site et d'autres personnes directement liées à l'activité criminelle menée à travers la plate-forme[2415].

Un autre groupe criminel organisé opérant en France a été démantelé par des agents de la Direction nationale du renseignement et des Enquêtes douanières (DNRED) à la suite d'une action le 17 mai 2021[2416]. A cette occasion, la plateforme connue sous le nom du *monde parallèle* a été fermée[2417], où des drogues, des armes, des cartes, des faux documents ou des

---

[2413] Pour plus de détails, *US v. Ulbricht, no. 13-06919,* US District Court, Southern District of New York, , disponible à https ://www.courtlistener.com/docket/4352774/united-states-v-ulbricht/

[2414] É. A. Caprioli, *op. cit.*

[2415] Selon le communiqué de presse publié par le Ministère français de l'Économie le 16 juin 2018, disponible sur https ://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=D134C754-EDAC-4F18-B26E-295147EEE2FE&filename=304%20-%20G%C3%A9rald%20DARMANIN%20f%C3%A9licite%20la%20douane%20pour%20le%20d%C3%A9mant%C3%A8lement%20du%20forum%20%C2%AB%20Black%20Hand%20%C2%BB%20(ou%20La%20main%20noire)%2C%20l%27une%20des%20plus%20importantes%20places%20de%20march%C3%A9%20ill%C3%A9gales%20du%20darkweb%20fran%C3%A7ais.pdf</s> ?

[2416]Direction générale des douanes et droits indirects (DGDDI), «*Démantèlement du forum "Le Monde Parallèle" sur le Darknet*», Actualités – douane.gouv.fr, 2021, https://www.douane.gouv.fr/actualites/demantelement-du-forum-le-monde-parallele-sur-le-darknet?

[2417] Franceinfo, *Stupéfiants, faux documents, armes: la plateforme "Le Monde Parallèle" qui proposait ses activités illégales sur le Darknet démantelée par les douaniers,* 2021. https ://www.francetvinfo.fr/societe/justice/stupefiants-faux-documents-armes-la-plateforme-le-monde-parallele-qui-proposait-ses-activites-illegales-sur-le-darknet-demantelee-par-les-douaniers_4632893.html

bases de données liées à la vie privée des internautes ont été vendus. Il s'agit de la troisième action majeure des autorités *françaises*, après la fermeture de *la Main Noire* en 2018 et la fermeture *du marché français du Deep Web* en 2019[2418].

En 2022 et 2024, le dark web a reçu certains de ses plus grands succès en fermant et en confisquant les serveurs supportant la plateforme Hydra[2419] et ceux derrière les plateformes Nemesis[2420], Incognito et[2421] Breach Forums[2422]. Par exemple, les chiffres derrière Hydra sont remarquables en tant que marché noir le plus important et le plus ancien au monde, couvrant plus de 80% des transactions illégales de crypto-monnaie, avec une valeur nominale de plus de 5,2 milliards de dollars entre 2015 et 2024.

e). Séquestration de données (ransomware)

868. Formes courantes de cybercriminalité. Il convient également de mentionner le concept de « séquestration de données », la méthode utilisée par les pirates opérant au sein du *Dark Web*. Cette opération est appelée ***ransomware*** et est parmi les dernières nouvelles en matière de violations de la vie privée. Le ransomware est l'un des plus grands problèmes de sécurité sur Internet et l'une des formes les plus courantes de cybercriminalité. Un ransomware est une forme de logiciel malveillant (malware) qui crypte des fichiers et des documents à partir d'un seul ordinateur ou même d'un réseau entier, y compris des serveurs. Les victimes peuvent souvent se retrouver avec peu d'options. Ils peuvent soit récupérer l'accès à leurs données saisies en payant une rançon aux auteurs, soit restaurer les données à l'aide de sauvegardes, soit espérer qu'une clé de décryptage sera disponible gratuitement. Certaines attaques de ransomware commencent par quelqu'un qui clique sur ce qui semble être un document joint à un courriel non suspect qui, une fois ouvert, télécharge le logiciel utilisé dans une activité criminelle, et les données de la victime deviennent inaccessibles[2423].

[2418] C. Cimpanu, *French authorities seize their third dark web marketplace,* The Record, 2021. https ://therecord.media/french-authorities-seize-their-third-dark-web-marketplace

[2419]U.S. Department of Justice, *Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace,* 2022. https ://www.justice.gov/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace

[2420]F.Truta, *German Authorities Take Down Darknet Marketplace 'Nemesis Market',* Bitdefender, 2024. https://www.bitdefender.com/en-us/blog/hotforsecurity/german-authorities-take-down-darknet-marketplace-nemesis-market

[2421]U.S. Attorney's Office, *"Incognito Market" Owner Arrested For Operating One Of The Largest Illegal Narcotics Marketplaces On The Internet,*2024. https://www.justice.gov/usao-sdny/pr/incognito-market-owner-arrested-operating-one-largest-illegal-narcotics-marketplaces

[2422]P. Arntz*, Notorious data leak site BreachForums seized by law enforcement*, Malwarebytes labs,2024. https ://www.malwarebytes.com/blog/news/2024/05/notorious-data-leak-site-breachforums-seized-by-law-enforcement

[2423] É. A. Caprioli, *Régime juridique du Ransomware ou prise d'otage numérique,* Revue de la Gendarmerie Nationale, 4e trimestre, 2016. p. 179

Un cas notoire de ransomware qui a suivi la mort d'une personne s'est produit à Düsseldorf, en Allemagne. Plus précisément, le 11 septembre 2020, un hôpital de la ville allemande a été la cible d'une attaque de ransomware, ce qui a empêché un patient souffrant de conditions graves d'être admis dans l'établissement médical. En accédant à distance et en bloquant l'accès aux données médicales, le personnel médical a été contraint de rediriger le patient vers une autre unité hospitalière, mais il est mort dans l'ambulance. L'ancien chef du National Cyber Security Centre du Royaume-Uni a déclaré que si l'incident pouvait s'avérer avoir été causé par une cyberattaque, on pourrait sans aucun doute parler du premier cas de décès d'une personne à la suite d'une cybercriminalité[2424].

869. La criminalisation des ransomwares en Roumanie. L'activité de ransomware est également soumise au droit pénal en Roumanie. Ainsi, en cas d'acte de ce type, la responsabilité de l'auteur de l'attaque serait engagée en vertu de l'article 360 du Code pénal roumain (accès illégal à un système informatique), de l'article 362 (altération de l'intégrité des données informatiques) et même de l'article 364 (transfert non autorisé de données informatiques), dans le cas où un transfert de données réel est également effectué et pas seulement une simple copie. En outre, dans le cas où il y aurait également des activités de vente de logiciels destinées à commettre une infraction informatique, la loi pénale roumaine prévoit (similaire à la loi française) le délit d'opérations illégales avec des appareils informatiques ou des logiciels (article 365 du Code pénal).

B. Atteintes à la sécurité des données privées

a). La conception du Code pénal français.

870. Au chapitre VI, article 5 du Code pénal français (226-16 – 226-24) sont prévus les actes criminels relatifs *aux atteintes aux droits de la personne physique des fichiers ou des traitements informatiques*. Les éléments matériels criminalisés par la règle pénale sont l'interception, le détournement, l'utilisation ou la divulgation de renseignements contenus dans la correspondance. Ensuite, nous décrirons brièvement chaque délit afin de dresser un tableau clair de la façon de criminaliser les actes commis sur la protection de la vie privée par le biais des systèmes d'information[2425].

[2424]F.Truta, *Patient Dies After Ransomware Attack on Düsseldorf Hospital*, Security Boulevard, 2020. https ://securityboulevard.com/2020/09/patient-dies-after-ransomware-attack-on-dusseldorf-hospital/ consulté le 20.09.2020

[2425] J.-C. Saint-Pau, *Droits de la personnalité,* LexisNexis, 2013, pp. 645-660.

L'article 226-16 prévoit le non-respect des formalités préalables. Cet acte implique de réaliser, même par négligence, l'activité de traitement de données personnelles sans respecter les formalités prévues par la loi préalablement à leur mise en œuvre. L'article 226-17 incrimine l'acte de traitement de données personnelles sans respect des dispositions du RGPD (articles 24, 25, 30, 32). En outre, l'article 226-18 prévoit l'acte de collecte de données personnelles par des moyens frauduleux, déloyaux ou illégaux. En ce qui concerne ce crime, l'élément matériel est exécuté de diverses manières. Par exemple, nous pouvons nous référer à la situation dans laquelle une entreprise qui gère un cybercafé collecte les données des clients après leur connexion via les ordinateurs mis à disposition. Nous proposons également, à titre d'exemple, une affaire dans laquelle des employés d'EDF-GDF[2426] ont été condamnés sur cette base parce qu'ils avaient vendu les adresses de nouveaux souscripteurs à un assureur, chacun commettant également des infractions de corruption active et passive[2427] (corruption, selon la législation roumaine).

L'article 226-19 érige en infraction pénale le fait de stocker ou de stocker dans la mémoire de l'ordinateur, sans le consentement exprès de la personne concernée, des données personnelles qui révèlent directement ou indirectement des origines raciales ou ethniques, des opinions, des affiliations politiques, philosophiques, sociales ou politiques, religieux ou syndicaux de personnes ou liés à leur santé, à leur orientation sexuelle ou à leur identité de genre. Est également érigé en infraction pénale le fait, sauf dans les cas prévus par la loi, de stocker ou de conserver dans la mémoire de l'ordinateur des données personnelles relatives à des infractions, des condamnations ou des mesures de sécurité. Dans la pratique, il a ordonné la condamnation d'un homme qui a stocké dans son ordinateur et partagé des photos de son ex-maîtresse dans des poses intimes, ainsi qu'un texte décrivant ses habitudes sexuelles[2428].

Ensuite, les articles 226-19-1 prévoient l'acte de traitement de données à caractère personnel à des fins de recherche en santé, lorsque : 1. Sans préavis aux personnes pour le compte desquelles les données personnelles sont collectées ou transmises sur leur droit d'accès, de rectification et d'opposition, sur la nature des données transmises et sur leurs destinataires ; 2. En violant l'opposition de la personne concernée ou, lorsque la loi le prévoit, en l'absence de consentement éclairé et exprès de la personne ou, dans le cas d'une personne décédée, en ignorant le refus exprimé par celle-ci au cours de sa vie.

L'article 226-20 criminalise la conservation de données personnelles au-delà de la période prévue par la loi ou la réglementation (RGPD), en demandant l'autorisation ou l'avis

[2426] Une société de fourniture d'électricité et de gaz en France.
[2427] Trib. Commercial Paris, n° 181 de mars 1995, Expertises, p. 120.
[2428] Trib. Corr. de Privas, Science criminelle, 1998, p. 574.

ou en faisant une déclaration préalable adressée à la Commission nationale de l'informatique et des libertés, à moins que cette conservation ne soit effectuée à des fins historiques, statistique ou scientifique dans les conditions prévues par la loi. Il est également incriminé par le même article et la loi, sauf dans les cas prévus par la loi, le traitement à des fins autres que les données historiques, statistiques ou scientifiques personnelles conservées pendant la période prévue par la loi. En d'autres termes, la règle d'incrimination se réfère à la situation dans laquelle des données personnelles ont été conservées au-delà de la période prévue par la loi et il est nécessaire que le sujet actif sollicite un avis ou une autorisation de la CNIL pour l'utilisation de ces données[2429].

L'article 226-21 : L'acte commis par toute personne qui détient des données personnelles au moment de l'enregistrement, de la classification, de la transmission ou de toute autre forme de traitement, et qui a dévié ces informations de leur finalité telle que définie par la loi, Règlement ou décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé. Article 226-22 de la loi de toute personne qui a recueilli, lors de l'enregistrement, du classement, de la transmission ou de toute autre forme de traitement, des données à caractère personnel dont la divulgation aurait un effet non patrimonial sur la personne concernée ou sa vie privée et qui apporte, sans le consentement de la personne concernée, ces données sont connues d'un tiers qui n'a pas l'autorisation de les recevoir. La punition est aussi l'acte de culpabilité. Un exemple de ce délit peut être le fait pour le fonctionnaire de divulguer le secret professionnel à une autre personne qui n'a pas l'autorisation de prendre connaissance des données[2430].

871. Création de nouvelles infractions. En 2018, deux nouveaux articles ont été introduits qui prévoient les infractions relevant de cette catégorie. L'article 226-22-1, qui criminalise le transfert ou l'établissement d'un transfert de données personnelles ou qui doit être traité vers un État n'appartenant pas à l'Union Européenne ou à une organisation internationale, en violation des dispositions du RGPD. Enfin, l'article 226-22-2 prévoit l'acte commis par une personne qui empêche les agents de la Commission nationale de l'informatique et des libertés de remplir leur mission, de leur communiquer les informations qu'ils demandent ou de communiquer de fausses informations.

Au moyen de l'article 226-23, il est offert la possibilité que les données qui ont fait l'objet des infractions prévues aux articles 226-16 – 226-22-2, soient supprimées, et les membres de la CNIL sont habilités à vérifier cet aspect. Enfin, l'article 226-24 prévoit la possibilité de sanctionner les personnes morales qui commettent les actes décrits ci-dessus. Les

[2429] V. Malabat*, Droit pénal spécial*, 7e édition, Ed. Dalloz, Paris, 2015, pp. 347-349
[2430] M. Bénéjat*,* J.-C. Saint-Pau(coord.)*, La responsabilité pénale professionnelle,* éd. Dalloz, 2012, pp. 42-44.

peines prévues dans ce groupe d'infractions consistent en une peine d'emprisonnement pouvant aller jusqu'à 5 ans et une amende pouvant aller jusqu'à 300.000 euros.

b). La conception du Code pénal roumain

872. Protection des données privées – Code pénal roumain. En ce qui concerne les implications pénales dans le domaine de la cybersécurité, la législation pénale roumaine contient des règles d'incrimination destinées à protéger ce domaine technique. Ainsi, comme je l'ai déjà souligné, le Code pénal contient au titre VII des atteintes à la sécurité publique le chapitre sur les atteintes à la sécurité et à l'intégrité des systèmes et données informatiques. Ainsi, les articles 360 à 366 du Code pénal contiennent les infractions pénales sanctionnées en relation avec les atteintes à l'intégrité des systèmes informatiques et des données. Incriminés en vertu de l'état de droit n° 161/2003 sur certaines mesures visant à assurer la transparence dans l'exercice des dignitaires publics, les fonctions publiques et l'environnement des affaires, la prévention et la répression de la corruption, les actes correspondants ont été inclus dans le règlement pénal précisément en raison de l'importance des valeurs sociales protégées. Par le biais de la criminalité informatique, le législateur défend ces relations sociales en ce qui concerne la protection des données trouvées dans les systèmes d'information et les systèmes d'information eux-mêmes. Il est donc aisé de constater que les valeurs sociales indirectement protégées par l'incrimination des faits en cause se rapportent également à la vie privée et à la vie privée de l'individu. Même la tentative est incriminée à l'égard de ces faits. D'une manière générale, les infractions contenues dans ce titre sont similaires à celles que l'on retrouve en droit français.

§2. LA VIE PRIVÉE DANS LE MÉTAVERS

873. L'extension de la réalité en ligne. Introduit relativement récemment dans le dictionnaire, le terme métavers a été utilisé pour la première fois par l'écrivain Neal Stephenson dans son roman de fiction Snow Crash[2431], un roman qui explore l'anxiété de la société face à

[2431] Le roman a été publié en juin 1992 aux États-Unis par Bantam Books Publishing House, proposant non seulement une histoire de science-fiction mais aussi des sujets liés à l'anthropologie, l'informatique, la politique, la cryptographie, la ligvistique ou la philosophie. Pour Stephenson, *le métavers* était un successeur d'Internet (comme on l'appelait à l'époque), un univers à travers lequel les gens pouvaient passer du monde réel à un monde de réalité virtuelle. L'identité en *métaverse* est acquise par un avatar qui a des préoccupations similaires à celles de la nature

la numérisation et aux technologies de l'information[2432]. Difficile à définir, le métavers est perçue comme une extension de la réalité, une fusion du réel et du virtuel, avec de nouvelles opportunités, mais sociales, économiques ou de divertissement[2433].

Le Meta verse, réalité numérique expansive et immersive, pose des défis importants en termes de protection de la vie privée, d'autant plus que les interactions, les activités et les comportements des utilisateurs sont collectés, stockés et analysés à une échelle sans précédent. Regis Chatellier, de la Commission nationale de l'informatique et des libertés (CNIL), caractérise la Meta verse comme une promesse incertaine, estimant que son succès dépend de l'innovation, de la régulation et de l'inclusion sociale[2434].

Lancée en 2003, la plateforme Second Life est la création la plus proche de ce qu'exige un métavers. Dans cet univers virtuel, les utilisateurs peuvent créer et posséder des propriétés, développer des entreprises, interagir socialement, sans les restrictions imposées par la réalité physique[2435]. Philip Rosedale, l'un des créateurs de second Life, met en garde contre le risque de monopoliser cet espace numérique, ainsi que les problèmes de confidentialité et de contrôle qu'il peut soulever[2436].

874. Atteindre l'immortalité dans l'univers parallèle. Connu pour la justesse de ses prédictions technologiques, en particulier sur l'intelligence artificielle, Raymond Kurzweil a parlé en 2007 de l'incorporation de l'homme dans la technologie, dans le but d'atteindre l'immortalité, et comment ce processus prend le dessus sur toute la personnalité humaine, la mémoire, les talents et l'histoire[2437]. Nous parlons de plus que de violations de la vie privée.

875. La popularité du métaverse. Actuellement, la métavers est tombée dans l'ombre, comme toute technologie, face à l'intelligence artificielle (IA), vue avec scepticisme et ironie par les grands investisseurs dans le domaine[2438]. Mais ceux qui vivent dans l'univers parallèle

---

[2432] J, Jashua*, Information Bodies : Computational Anxiety in Neal Stephenson's Snow Crash,* Interdisciplinaire Literary Studies, 2017. https ://doi.org/10.5325/intelitestud.19.1.0017

[2433] M. Damar, „*Metaverse Shape of Your Life for future : A bibliometric snapshot*", Journal of Metaverse, arXiv, 2021. https ://arxiv.org/abs/2112.12068

[2434] R. Chatellier, *Metavers : ce jeu dont qui sera le heros ?,* CNIL, 2022. https ://linc.cnil.fr/metavers-ce-jeu-dont-qui-sera-le-heros

[2435] P. Ludlow, M. Wallace, *The second Life Herald : The Virtual tabloid that a refusé l'aube de la le metaverse,* MIT press, 2007.

[2436] E. Gent, "*Lessons from a second Life > Before Meta, Philip Rosedale created an Online Universe*", in *IEEE Spectrum*, vol. 59, no. 1, pp. 9-19, 2022. Doi : 10.1109/MSPEC.2022.9676346.

[2437] R. Kurzweil (trad. de l'anglais par Adeline Mesmin*), Humanité 2.0 : La Bible du changement* ("*The Singularity is near : When Humans Transcend Biology")*, Paris, M21, 2007, p.647.

[2438] E. Gent, *What Can the Metaverse Learn from Second Life ? Creator Philip Rosedale says a virtual reality internet is still some way off*, IEEE Spectrum, 2021.

de « second Life » jouissent d'une communauté stable et de la liberté offerte par cet espace et ne sont pas intéressés par l'expansion de l'IA[2439].

En 2022, Metaverse a été considérée par Forbes comme l'une des 10 principales tendances auxquelles nous devrions nous préparer en 2023[2440]. En termes de popularité de la métavers à l'heure actuelle, les statistiques montrent qu'elle compte environ 400 millions d'utilisateurs actifs chaque mois, la plupart d'entre eux étant des adolescents mineurs[2441]. Il devrait atteindre 700 millions d'utilisateurs d'ici 2030. Gartner prédit que d'ici 2026, un quart de la population mondiale passera au moins une heure par jour en métavers. [2442]Bien que le chiffre semble élevé, les données sur le nombre d'utilisateurs de la plateforme Meta Horizon Worlds étaient en 2022 d'environ 200 000 dans le monde, bien en dessous des attentes de l'entreprise, qui s'était fixé comme objectif de 50 000 utilisateurs actifs mensuels[2443].

A. Délits possibles en métavers

876. Infractions possibles dans le métaverse. Le rapport sur les dangers de la métavers, publié en 2022, a révélé que près de la moitié des utilisateurs considèrent la dépendance à la réalité virtuelle comme le plus grand risque. D'autres préoccupations sont liées à l'intrusion dans la vie privée et aux effets négatifs sur la santé mentale. La privation de vie privée peut être secondaire à la collecte massive de données et à la surveillance continue de l'activité. En conclusion, les auteurs évoquent la nécessité d'adopter des réglementations et des mesures de protection pour prévenir les conséquences négatives pour les usagers et la société[2444]. Après un examen complet de la méta-averse, les principales préoccupations décrites étaient, en plus de celles liées à la confidentialité et à la sécurité des données, des questions éthiques et juridiques, par exemple comment protéger les utilisateurs contre les comportements abusifs ou illégaux

[2439] S. Parkin, *Who needs the Metaverse? Meet the people still living on Second Life*, The Guardian, 2023. https ://www.theguardian.com/technology/2023/jun/10/who-needs-the-le métavers-meet-the-people-still-living-on-second-life

[2440] B. Marr, *The Top 10 Tech Trends In 2023 Everyone Must Be Ready For*, Forbes, 2022. https ://www.forbes.com/sites/bernardmarr/2022/11/21/the-top-10-tech-trends-in-2023-everyone-must-be-ready-for/?sh=5a8cd8537df0

[2441] M. Geri, *48 Metaverse Statistics | Market Size & Growth,* Influencer marketing Hub, 2023. https://influencermarketinghub.com/metaverse-stats/

[2442]Stamford, Conn., *Gartner predicts 25% of people will spend at least one hour per day in the Metavers by 2026*, Gartner, 2022.https ://www.gartner.com/en/newsroom/press-releases/2022-02-07-gartner-predicts-25-percent-of-people-will-spend-at-least-one-hour-per-day-in-the-le métavers-by-2026

[2443] Statistica Research Department, *Nombre d'utilisateurs actifs de Meta Horizon Worlds dans le monde en octobre 2022*, Statistica, 2025. https://www.statista.com/statistics/1362347/meta-horizon-worlds-users/

[2444] A. Petrosyan, *Dangers of the metaverse according to internet users worldwide in 2021*, Statista, 2022. https ://www.statista.com/statistics/1288822/le métavers-dangers/

dans les métavers. Il met également en évidence l'impact sur l'identité et l'autonomie et la façon dont les utilisateurs risquent de perdre le contrôle d'eux-mêmes[2445].

877. Fréquence des infractions dans le métaverse. En examinant plus en détail les délits potentiels réalisables dans les métavers, nous pouvons analyser le rapport fait par l'American Enterprise Institute (AEI) en 2022[2446]. Selon les données, un incident d'abus ou de harcèlement (harcèlement sexuel, pornographie, menaces, racisme, y compris à l'encontre de mineurs) a lieu dans l'environnement virtuel Metaverse toutes les 7 minutes, avec l'absence de règlements clairs et de mécanismes de protection conduisant à ce taux accru de comportements antisociaux[2447]. Une étude de 2021 s'est penchée sur ces comportements, montrant que l'environnement immersif de la réalité virtuelle amplifie le harcèlement, le trolling ou l'invasion de l'espace personnel[2448]. On attire de plus en plus l'attention sur les questions du harcèlement sexuel dans les métavers, considéré comme traumatisant et grave comme le monde réel, et beaucoup soulignent que les mesures mises en œuvre pour prévenir ces incidents ne sont pas suffisantes[2449]. En 2016, un utilisateur de Metaverse a décrit son expérience de harcèlement sexuel. Bien que virtuel, il a eu un réel impact émotionnel, générant des sentiments de vulnérabilité et d'inconfort[2450].

a). Interpol a ouvert son bureau en métavers pour enquêter sur les délits

878. Les efforts d'Interpol pour s'adapter à l'évolution technologique. Au début de 2024, la police britannique enquêtait pour la première fois sur un cas de harcèlement sexuel dans des métavers sur l'avatar d'un mineur. Les autorités soulignent que cette affaire ouvre des discussions sur les défis législatifs générés par l'application de la loi dans des environnements virtuels[2451]. INTERPOL s'efforce également de développer des moyens de surveillance et

[2445] L. Lik-Hang, T. Braud et all., *All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda*, arXiv, 2021. https ://arxiv.org/abs/2110.05352

[2446] M. Jamison, M. Glavish, *The Dark Side of the Metaverse, Part I*, AEIdeas, 2022. https ://www.aei.org/technology-and-innovation/the-dark-side-of-the-le métavers-part-i/

[2447] *Facebook's Metaverse One incident of abuse and harassment every 7 minutes*, Center for Countering Digital Hate, 2021. https ://counterhate.com/research/facebooks-le métavers/#about

[2448] F. Yasaman, *Breaking the Virtual Ice: Antisocial Behaviors in Social Virtual Reality and How Developers Cope with Them*, thèse sous la direction de Roland Klemle, TH Köln, University of Applied Sciences, 2021. https ://www.researchgate.net/publication/349212255_Breaking_the_Virtual_Ice_Antisocial_Behaviors_in_Social_Virtual_Reality_and_How_Developers_Cope_with_Them

[2449] T. Basu, *The metaverse has a groping problem already*, MIT Technology Review, 2021 https ://www.technologyreview.com/2021/12/16/1042516/the-metavers-has-a-groping-problem/

[2450] J. Belamire, *My First Virtual reality Groping,* Medium 2016. https ://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee

[2451] C. Vallance, *Police investigate virtual sex assault on girl's avatar*, BBC News, 2024. https ://www.bbc.com/news/technology-67865327

d'application de la loi dans les métavers[2452]. Dans une tentative de s'adapter à l'évolution de la technologie, il crée en 2022 le premier bureau virtuel en métavers, reflétant ainsi la nécessité de la présence des autorités dans les environnements virtuels[2453].

b). Vide législatif pour les casinos du métavers

879. Le jeu est un domaine très rentable dans les métavers, générant environ 3 millions par mois[2454]. Ils sont également très accessibles aux mineurs. Cependant, les casinos en Metaverse sont dans un vide juridique parce que les joueurs n'utilisent pas de l'argent réel, mais des jetons, qui ne sont pas considérés comme des biens de valeur[2455]. Dans *Soto v Sky Union*, les juges ont rejeté l'affaire concernant l'illégalité du jeu virtuel « Castle Clash », arguant que les objets virtuels utilisés dans le jeu avec sont des biens de valeur, n'ont pas de valeur monétaire réelle au sens de[2456] la législation sur les jeux d'argent.

880. Infractions liées à la manipulation des consommateurs. Les infractions à la sécurité de l'information sont un autre sujet sensible, puisque les métavers peuvent collecter et utiliser une grande variété de données personnelles. Nous pouvons collecter des données d'identification personnelle, des données comportementales (activités, habitudes, interactions sociales diverses), des données biométriques (mouvements corporels, expressions faciales, gestes, regard, fréquence cardiaque, état émotionnel ou même conditions médicales), messages et communications entre utilisateurs[2457]. Des études ont montré qu'en utilisant la réalité virtuelle (VR) pendant 20 minutes, jusqu'à 2 millions de données biométriques peuvent être collectées[2458]. Cette quantité de données personnelles est nécessaire pour le métavers afin de créer un monde captivant et personnalisé[2459] pour les utilisateurs. Compte tenu de la quantité

[2452] M. Cieslak, T. Gerken, *Interpol working out how to police the metaverse*, BBC Click, 2023. https ://www.bbc.com/news/technology-64501726

[2453] Interpol*, Interpol launches first global police Metaverse*, 2022. https ://www.interpol.int/en/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metavers

[2454] P. Rosen, *This metaverse casino raked in $7,5 million in last 3 months and accounts for a third of Decentraland's daily users,* Business Insider, 2022. https ://markets.businessinsider.com/news/currencies/decentraland-metavers-casino-crypto-gambling-poker-2022-2

[2455] S. Mullin, J. Gatto, *The Game Goes On: Sheppard Mullin Obtains Dismissal With Prejudice of Class Action Alleging Social Gaming Micro-transactions Constitute Illegal Gambling*, Gambling, Virtual Currency, 2018. https ://www.mygamecounsel.com/2018/05/articles/gambling/micro-transactions-castle-clash/

[2456] *Soto v. Sky Union*, LLC, United States District court, N.D. Illinois, Eastern Division, 2016. https ://casetext.com/case/soto-v-sky-union-llc-1

[2457] P.Zhigeng, Y. Jiaqi et all., *Data- and management-driven metavers*, Research, Data Science and Management, vol.7, issue2, 2024. p.75-78, https ://doi.org/10.1016/j.dsm.2023.11.003.

[2458] J. Bailenson, „*Protecting non-verbal data tracked in virtual reality"*, JAMA Pediatrics, 2018. jamanetwork.com/journals/jamapediatrics/article-abstract/2694803

[2459] Y. Huang, Y.J. Li, Z.Cai, *Security and privacy in metaverse: A comprehensive survey*, Big Data Mining and Analytics,vol.6(2), 2023. p.234–247.https ://doi.org/10.26599/BDMA.2022.9020047

colossale de données, il y a des préoccupations au sujet de la vie privée et du risque d'utilisation abusive des renseignements personnels, d'autant plus que la protection des données dans les métavers est difficile compte tenu de sa nature mondiale[2460]. Dans sa lettre au fondateur en 2021, Mark Zuckerberg insiste sur l'importance de respecter les principes de confidentialité et de travailler avec les experts de l'industrie pour créer un environnement sûr pour le développement d'une économie virtuelle robuste, diversifiée et dynamique dans les métavers[2461]. Compte tenu de la grande diversité des données stockées, elles peuvent être utilisées pour comprendre les réactions émotionnelles et le comportement des utilisateurs, adaptant ensuite la publicité à ces caractéristiques. Cela peut conduire à une manipulation accrue des consommateurs[2462].

L'AEI présente également quelques propositions en termes de réponse aux défis des métavers. Il s'agit notamment de : développer un cadre législatif adaptable à la dynamique rapide de la technologie, responsabiliser les plateformes qui développent métavers, adopter des mesures pour protéger la vie privée des utilisateurs, grâce à des technologies de cryptage avancées et à l'anonymisation des données, améliorer la coopération internationale, éduquer et sensibiliser aux risques auxquels ils sont confrontés dans ces environnements virtuels[2463].

c). Impact du métavers dans la vie réelle

881. L'influence du métaverse sur l'économie. Bien que le métavers soit un concept 100% virtuel, son impact sur la vie réelle n'est pas négligeable, de nombreuses études mettant en évidence l'influence qu'elle peut avoir sur de nombreux aspects de la société, de l'économie et de la vie privée[2464].

Économiquement, plus de 120 milliards ont été investis dans les métavers en 2022[2465]. Compte tenu des investissements à grande échelle dans les métavers, le Parlement Européen prévoit que le marché des métavers atteindra environ 600 milliards d'euros d'ici 2030[2466]. Les

[2460] T. Parlar, *Data Privacy and Security in the Metaverse*, in F.S. Esen, H. Tinmaz, M. Singh(eds), *Metaverse. Studies in Big Data*, vol.133. Springer, Singapore, 2023. https ://doi.org/10.1007/978-981-99-4641-9_8
[2461] Fcaebook, *Founder's Letter*, Meta, 2021. https ://about.fb.com/news/2021/10/founders-letter/
[2462] T. Mega, P. Car, M. Niestadt, L Van de Pol, *Metaverse opportunities, risks and policy implications*, EPRS, 2022, https ://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf
[2463] M. Jamison , M. Glavish, *The Dark Side of the Metaverse, Part II : Potential Solutions*, AEIdeas, 2022. https ://www.aei.org/technology-and-innovation/the-dark-side-of-the-le métavers-part-ii-potential-solutions/
[2464] Facebook, *The Metaverse May Be Virtual, But the Impact Will Be Real,* Meta, 2022 https ://about.fb.com/news/2022/09/the-le métavers-may-be-virtual-but-the-impact-will-be-real/
[2465] McKinsey & Company, *Value creation in the metaverse, the metaverse does actually impact the environment*, 2022. https ://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/value-creation-in-the-Metaverse
[2466] Ibidem réf. 28

utilisateurs investissent également dans les métavers. Un participant a investi 450 000 pour devenir le voisin virtuel de Snoop Dogg[2467], et un autre a acheté un terrain pour 3,7 millions (ce qui est également la transaction la plus précieuse[2468] de Metaverse).

882. Des études montrent que les utilisateurs renoncent à la confidentialité pour de petits avantages. La vie privée et la vie privée sont parmi les droits les plus opprimés dans l'environnement virtuel. Selon certains auteurs, cette tendance semble également secondaire au désintérêt des utilisateurs pour la vie privée numérique. Une étude de 2022 a montré que les gens étaient prêts à renoncer à la vie privée pour des montants relativement modestes ou pour des récompenses et des avantages immédiats[2469]. De plus en plus, la nécessité d'un cadre juridique international coordonné pour la protection de la vie privée dans les espaces numériques est discutée. Des organisations telles que les Nations Unies ou l'Organisation de coopération et de développement économiques (OCDE) ont entamé des discussions sur les réglementations transnationales en matière de protection des données et de confidentialité[2470]. Le métavers, par sa nature mondiale, rend ces réglementations internationales encore plus urgentes, et la collaboration entre les pays et les régions sera essentielle pour assurer une protection adéquate de la vie privée des utilisateurs.

d). Mécanismes permettant d'identifier le délinquant

883. Il est clairement nécessaire de mettre en place des politiques plus strictes, des mécanismes de signalement plus efficaces et des réglementations pénales plus accessibles pour maintenir la sécurité des utilisateurs et la commodité des métavers. La législation et les mécanismes de protection existants ne sont pas toujours suffisants pour assurer la protection attendue dans l'environnement virtuel. Pour soutenir cette idée, nous pouvons illustrer le cas de *K.U. c. Finlande*, où l'identité d'un mineur a été utilisée à mauvais escient pour créer des publicités illégales sur une plateforme de rencontres en ligne. La CEDH a constaté que la législation finlandaise ne prévoyait pas de mécanisme efficace pour identifier l'auteur de

[2467] W.Lavin, *NFT Collector spends $450,000 to live as snoop doggs virtual neighbor*, NME, 2022. https ://www.nme.com/news/music/nft-collector-spends-450000-to-live-as-snoop-doggs-virtual-neighbor-3114160

[2468] C. Polona, M. André, N. Maria,. *Metaverse: Opportunities, Risks and Policy implications*, EPRS: European Parliamentary Research Service. Belgium, 2022. retrieved from https ://coilink.org/20.500.12592/gjscr8

[2469] T.J. Prince, S. Wallsten, *How much is privacy worth around the world and across platforms?,* Journal of Economics & Management Strategy, vol.31, issu4, 2022. p.841-861 https ://onlinelibrary.wiley.com/doi/10.1111/jems.12481

[2470] United Nation, General Assembly, *Road map for digital cooperation: implementation of the recommendation of the High-level Panel on Digital Cooperation*, 2020. https ://documents.un.org/doc/undoc/gen/n20/102/51/pdf/n2010251.pdf

l'infraction, étant dépassée dans le contexte de la criminalité en ligne[2471]. Une affaire de violence domestique qui a été étendue dans l'environnement en ligne qui a atteint la CEDH est *Buturugă c. Roumanie,* la Cour soulignant dans cette affaire que les autorités roumaines n'ont pas enquêté et n'ont pas traité correctement les questions liées à la violence numérique, limité aux aspects physiques de la violence domestique[2472]. L'affaire révèle la vulnérabilité des femmes dans l'environnement virtuel, soulignant la nécessité de mieux reconnaître les risques et les dommages causés par la violence numérique et la nécessité de mesures de protection efficaces.

B. Perspectives juridiques actuelles

884. Défis législatifs. Le métavers opère à l'intersection de plusieurs branches juridiques, telles que le droit de la protection des données, le droit de la propriété intellectuelle, les droits des consommateurs et les règles de cybersécurité. Les principaux défis juridiques sont liés à la propriété intellectuelle, à la confidentialité des données et à la juridiction[2473].

885. Situation actuelle. Toutefois, la législation en vigueur sur les questions ci-dessus peut également être appliquée dans un environnement virtuel, bien qu'elle n'ait pas été initialement conçue pour des environnements virtuels interactifs à l'échelle des métavers. Nous pouvons mentionner ici le Règlement général sur la protection des données (RGPD)[2474] et la directive sur le commerce électronique[2475] dans l'Union Européenne. En 2022, le règlement (UE) 2022/2065, également appelé loi sur les services numériques, est adopté, qui vise à créer un marché unique des services numériques et à faire de l'espace virtuel un environnement sûr, transparent et responsable[2476]. Vu comme une avancée timide dans la lutte « contre le Far West dans lequel le monde numérique s'est transformé », la principale conclusion du règlement est

[2471]CEDH, *K.U. v. Finland* - 2872/02, 2008. https ://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa42a

[2472]CEDH, *Buturugă v. Romania – 56867/15*, 2020. https ://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-6635916-8811383%22]}

[2473] M. Kalyvaki, *Navigating the Metaverse Business and Legal Challenges: Intellectual Property, Privacy, and Jurisdiction*, Journal of Metaverse. Vol.3, 2023. https://doi.org/10.57019/jmv.1238344

[2474] General Data Protection Regulation, *What is GDPR, the EU's new data protection law?*. https ://gdpr.eu/what-is-gdpr/

[2475] European Union law, *e-Commerce Directive,* 2024. https ://digital-strategy.ec.europa.eu/en/policies/e-commerce-directive

[2476] European Union law, *Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC*. https ://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A277%3ATOC&uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG

que « ce qui est interdit hors ligne doit aussi l'être en ligne »[2477]. Par ailleurs, en France, l'organisation CNIL a publié de nombreuses lignes directrices sur la protection des données personnelles dans l'environnement en ligne. En ce qui concerne la réglementation de la compétence judiciaire, le Parlement Européen a élaboré le règlement (UE) n° 1215/2012 qui vise à faciliter l'application uniforme de la justice dans les États membres[2478].

Outre-mer, nous pouvons nous référer à la *Digital Millennium Copyright Act* (DMCA)[2479] ou à la *California Privacy Protection Act* (CCPA)[2480]. Bien entendu, ces réglementations doivent être adaptées pour répondre aux nouvelles réalités technologiques, dans lesquelles les identités numériques des utilisateurs et leurs comportements en ligne sont beaucoup plus complexes, variés et infiniment plus exposés.

a). Juridiction dans le métaverse.

886. Compétence. Un exemple de compétence en métavers est l'affaire *Bragg vs, Linden Research Inc* de 2007. Dans cette affaire, le plaignant accuse Linden d'abus après avoir bloqué l'accès à son compte et confisqué ses actifs virtuels, acquis du point de vue du défendeur, en utilisant une monnaie non autorisée. La Cour considère que le recours de Linden ainsi que les conditions d'utilisation des plateformes sont injustes, et cette décision aboutit finalement à un règlement amiable en dehors du tribunal[2481]. Cette affaire met en évidence un des problèmes juridiques liés au métavers, à savoir l'application et le respect du droit de la propriété. Sur le même sujet, à la suite d'un procès collectif, Linden indemnisera à la fois de l'argent virtuel et de l'argent réel pour un groupe d'utilisateurs qui ont été violés sur leurs droits de propriété[2482].

D'un point de vue criminel, la difficulté vient de démontrer l'existence de l'élément matériel, c'est-à-dire la composante physique des délits dans les métavers. En reprenant la discussion sur les cas de harcèlement sexuel dans l'environnement virtuel, puisque le délit n'est

---

[2477] J. Dupriez, *GAFAM , le Parlement Européen s'attaque au « Far-West » du numérique,* Public Senat, 2022.https ://www.publicsenat.fr/actualites/non-classe/gafam-le-parlement-europeen-s-attaque-au-far-west-du-numerique-191984

[2478] Regulation (EU) n° 1215/2012 of the European Parliament and of the Counsil of 12 december 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) https ://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32012R1215

[2479] G. Stobbs, *18 - The Digital Millennium Copyright Act*, Multimedia Security technologies for Digital Rights Management, Academic Press, 2006. p. 457-482, https ://doi.org/10.1016/B978-012369476-8/50020-8

[2480] State of California Department of Justice, « *California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General »,* State of California Department of Justice, 2018. https ://oag.ca.gov/privacy/ccpa

[2481] *Bragg v. Linden Research, Inc.* https ://casetext.com/case/bragg-v-linden-research

[2482] *Evans v. Linden Research, Inc,* No. C-11-01078 DMR (N.D. Cal. Apr. 29, 2014) https ://casetext.com/case/evans-v-linden-research-12

pas isolé, il y a de plus en plus de cas[2483], d'un point de vue juridique ils ne peuvent pas être qualifiés de crime de viol, selon les dispositions légales en vigueur, parce que l'élément matériel ne peut pas être défini. Dans le Code pénal français, le crime de viol est défini à l'article 222-23 qui définit le viol comme « tout acte de pénétration sexuelle de quelque nature que ce soit commis sur une personne par la violence, la contrainte, la menace »[2484]. L'agression sexuelle est également définie à l'article 222-22 du Code pénal. Dans le Code pénal roumain (article 218), le viol est défini de la même manière, nécessitant un rapport physique, effectué par la contrainte[2485].

b). Vol d'objets virtuels.

887. Un autre délit qui peut être commis dans les métavers est le vol. Elle est régie par l'article 311-2 du Code pénal français[2486] et par l'article 228 du Code pénal roumain[2487]. Dans les deux cadres législatifs, la notion de « bien » englobe non seulement les biens matériels, mais tout mobile ayant une valeur économique. Il existe déjà des décisions de justice qui établissent que même des données ou des actifs virtuels peuvent être volés[2488]. Nous pouvons donc conclure que dans ce cas, la législation actuelle peut également être adaptée et utilisée dans le contexte du métavers. Dans certains états, comme les Pays-Bas, le délit de vol virtuel était déjà réglementé d'un point de vue pénal, par la décision de la Cour suprême néerlandaise du 31 janvier 2012, lorsque deux jeunes ont été reconnus coupables de vol d'un objet virtuel[2489]. L'arrêt a un impact considérable sur le droit pénal, créant un précédent pour la reconnaissance de la valeur et de la protection législative des biens numériques dans l'environnement virtuel, soulignant que le droit actuel doit s'adapter aux évolutions technologiques[2490].

[2483] Voir le cas de Nina Patel, qui a été insultée et abusée en 2022 dans le métavers Horizon World https ://www.telegraph.co.uk/news/2024/01/03/raped-in-virtual-reality-metavers-victim-blaming/
Regardez le cas choquant de 1993 sur la plateforme LambdaMOO quand un avatar a agressé sexuellement d'autres utilisateurs de https ://www.villagevoice.com/a-rape-in-cyberspace/

[2484] Code pénal français, *section 3 : du viol, de l'inceste et des autres agressions sexuelles (articles 222-22 à 222-33-1)*

[2485] Code pénal roumain (LOI no 286/2009) *article 218*

[2486] Code pénal français, *Livre III : des crimes et délits contre les biens (articles 311-1 à 324-9), Chapitre Ier : du vol (articles 311-1 à 311-16), section 1 : du vol simple et des vols aggravés (articles 311-1 à 311-11)*

[2487] Ibidem Réf. 47, article 228.

[2488]Cour de Cassation, Chambre criminelle, du 9 septembre 2003, *02-87.098*, Inédit https ://www.legifrance.gouv.fr/juri/id/JURITEXT000007599163/

[2489] Dutch Supreme Court, *J. 10/00101,* Criminal Chamber, January 31, 2012.

[2490] H. Wolswijk, *Theft: Taking a Virtual Object in RuneScape: Judgment of 31 January 2012, Case No. 10/00101 J,* The Journal of Criminal Law, vol.76(6), 2012. p.459-462. https ://doi.org/10.1350/1740-5580-76.6.459

c). Héritage de l'identité numérique après le décès du titulaire

888. Le droit de « se déconnecter » du métaverse. Une autre situation sensible est l'application, la mise en pratique de la loi sur l'héritage des données ou des actifs dans les métavers. Les articles sur ce sujet soulignent la nécessité d'adapter la législation nationale et européenne pour une gestion adéquate de « l'héritage numérique » après[2491] le décès/retrait du titulaire. Ici, nous devons discuter du droit, qui est plus juste pour des raisons éthiques, de « déconnecter » des métavers. Il existe déjà des analyses du besoin des utilisateurs de se déconnecter de l'environnement virtuel, en identifiant les avantages tels que la réduction du stress, l'amélioration de la vie privée et de la santé mentale[2492].

Compte tenu de la possibilité de rassembler des biens de valeur économique et de la nature encore mortelle des utilisateurs du Métavers, afin de mieux gérer les droits fondamentaux de l'homme tels que la vie privée, les droits de propriété ou de succession, les créateurs discutent de la création d'une identité numérique, Une empreinte digitale unique et non communicable, que j'appelle des « jetons liés par le son (SBT) »[2493]. Les SMS stockeront les réalisations, les expériences et tout autre élément déterminant de la vie en ligne d'un individu, même après la mort. Cela permet de réaliser un patrimoine numérique, et les questions concernant qui peut accéder à l'identité virtuelle d'une personne nécessitent une réglementation rigoureuse[2494].

d). Droit européen et français, intérêt pour les métavers.

889. En conclusion, nous pouvons souligner l'attention accrue des autorités sur ce sujet. En 2023, le Conseil de l'Europe et l'IEEE (Institute of Electrical and Electronics Engineers)[2495] ont produit un rapport sur les effets des métavers sur l'homme. Il met en évidence l'effet direct de cette réalité en ligne sur les droits de l'homme, la vie privée, la liberté d'expression et

---

[2491] A. Favreau, *Mort numérique. Quel sort juridique pour nos informations personnelles ?,* Revue Lamy droit civil, vol.125, 2015. p.66-68. « hal-01452467 »

[2492] J. Hopkins, „*Managing the right to Disconnect—A Scoping Review",* Sustainability, MDPI, vol. 16(12), 2021.p.1-14.

[2493] M. À Cabot-Nadal, B. Playford, M. Payeres-Capellà, S. Gerske, M. Mut-Puigserver, R. Pericas-Gornals, „*Private Identity-related attributes verification Protocol using SoulBound tokens and Zero-Knowledge Proofs",* 7th Cyber Security in Networking Conference (CSNet*)* Montréal, QC, Canada, 2023. p.153-156, doi: 10.1109/CSNet59123.2023.10339754.

[2494] P.Ohlhaven, E.G. Weyl, V. Buterin, *Decentralized Society: Finding Web3's Soul*, SSRN, 2022. available at: https ://ssrn.com/abstract=4105763 or http ://dx.doi.org/10.2139/ssrn.4105763

[2495] IEEE est l'une des plus grandes organisations au monde dédiée à l'avancement de la technologie au profit de l'humanité. Il est impliqué dans les domaines du génie électrique, de l'électronique, des télécommunications, de l'informatique, de la robotique, promouvoir en permanence la recherche scientifique. https ://www.ieee.org/

l'égalité[2496]. La protection de la vie privée et des données personnelles est assurée par les articles 6 et 8 de la Convention 108 du Conseil de l'Europe[2497]. La liberté de pensée est régie par l'article 9 de la même Convention[2498].

À la lumière de ce qui précède, le Conseil de l'Europe élabore également des recommandations CM/Rec(2018)7 sur la protection des enfants dans l'espace numérique[2499]. Il recommande aux États membres d'imposer des mesures législatives pour protéger les enfants contre le harcèlement en ligne, l'exploitation ou les contenus préjudiciables.

De même, reconnaissant les opportunités du métavers dans les domaines de l'éducation, du divertissement et de l'innovation technologique, la France a produit en 2022 un rapport dans le but de comprendre et de préparer ses implications sociales, économiques et juridiques[2500].

Conclusions du chapitre 1

Le chapitre 1 met en évidence la manière dont l'interaction entre l'individu et la technologie a évolué, aboutissant à la construction d'un écosystème numérique dans lequel l'intelligence artificielle, l'apprentissage automatique et le profilage de masse conditionnent effectivement le contenu et les garanties du droit pénal. Il en résulte que les techniques de *Machine Learning* et de *Deep Learning*, les systèmes autonomes et les outils algorithmiques ne peuvent être considérés comme de simples moyens neutres : ils interviennent dans la génération de faits, dans l'amplification de la capacité criminelle et dans la dilution de la traçabilité de la décision, ce qui oblige à réexaminer les modèles de responsabilité pénale (humaine, des personnes morales, éventuellement des entités techniques) et les règles de compétence, d'incrimination et de sanction.

L'analyse des *deepfakes*, du profilage comportemental et de la manipulation de l'information montre que l'atteinte à la vie privée ne se limite plus à la divulgation non autorisée de données, mais inclut la fabrication d'identité, le détournement de la volonté, la restructuration de l'environnement informationnel et l'utilisation des données personnelles comme vecteur

[2496] *The metaverse and its impact on human rights, the rule of law and democracy*, Conseil de l'Europe and IEE SA, 2024. https ://rm.coe.int/the-le métavers-impact-on-and-its-impact-on-human-rights-the-rule-of-law/1680ae6bce

[2497] *Convention 108 and Protocols*, Conseil de l'Europe. https ://www.coe.int/en/web/data-protection/convention108-and-protocol

[2498] Ibidem

[2499] *Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment*, Conseil de l'Europe, 2018. https ://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808b79f7

[2500] A. Basdevant, C. François, R. Ronfard, *Mission exploratoire sur les metavers*, Vie-publique, 2022. https ://www.vie-publique.fr/files/rapport/pdf/286878.pdf

d'influence. Le Big Data, les réseaux sociaux et les techniques de désinformation créent des formes d'ingérence dans lesquelles le consentement devient formel, la liberté de choix est érodée et la distinction entre opinion, propagande et atteinte à la vie privée revêt une importance pénale.

La section consacrée à l'anonymat en ligne, aux marchés noirs virtuels, aux *ransomwares* et aux activités menées sur le *dark web*/*deep web* met en évidence le conflit structurel entre la nécessité d'identifier les auteurs et la protection des données. Elle décrit le rôle des réglementations françaises et roumaines actuelles en matière de sécurité informatique, mais aussi leurs limites face à la mobilité transnationale des faits. L'analyse du métaverse remet en question, dans la même logique, la qualification pénale des faits commis dans des environnements immersifs, la question de la localisation de l'illicite, la protection des biens et de l'identité numériques et la continuité de la responsabilité après le décès du titulaire.

Dans l'ensemble, ce chapitre montre que la relation entre le droit pénal et les nouvelles technologies ne peut plus se résumer à des adaptations marginales : la manière dont sont conçues la responsabilité, la typicité, la territorialité et la protection de la vie privée est directement affectée par l'intelligence artificielle, le profilage, l'anonymat et les univers numériques persistants. Les prémisses d'une reconstruction dogmatique se dessinent ainsi, dans laquelle la vie privée devient un critère central d'évaluation des nouvelles incriminations et des limites de l'intervention pénale.

Chapitre 2
EFFETS JURIDIQUES DE LA CRYPTOGRAPHIE DANS LES CONVERSATIONS NUMÉRIQUES

890. Collecte d'informations, historique. Les technologies modernes comme Internet et les appareils intelligents facilitent la surveillance de masse des individus, mettant ainsi en danger la vie privée et la vie privée.[2501] La technologie est également le principal facteur qui a mené à l'augmentation de la collecte de renseignements personnels.[2502] Bien sûr, l'enregistrement des informations personnelles est pratiqué depuis des siècles[2503], un effort des autorités à cet égard étant l'introduction du recensement, le premier ayant eu lieu en 1086 au Royaume-Uni (Domesday Book)[2504]. Au fil du temps, de plus en plus de questions sur la vie privée ont été incluses dans le recensement, ce qui a mené à de nombreuses protestations publiques, ce qui a nécessité un régime législatif strict et bien établi en matière de protection de la vie privée et de droits à la vie privée au début du XXe siècle.[2505]

Section 1. LA VIE PRIVÉE À L'ÈRE DE LA MONDIALISATION NUMÉRIQUE – LIMITER LES INTRUSIONS

891. Diverses définitions de l'intimité. À l'heure actuelle, la protection de la vie privée est l'un des concepts les plus importants de la protection de la vie privée, sa définition étant vraiment difficile, surtout à l'ère actuelle de la mondialisation.[2506] Dans son analyse, Salove définit l'intimité comme un équilibre entre les intérêts et les besoins sociaux de l'individu. En 1890, Warren et Brandeis ont défini le droit à la vie privée comme le « droit d'être laissé seul », c'est-à-dire le droit de vivre sans intrusion dans l'espace personnel, sans divulgation d'informations personnelles ou dénigrantes.[2507] Depuis lors, ils ont souligné que les progrès de

[2501] A. Nishnianidze, *Surveillance in the Digital Era*, European Scientific Journal. vol.20, 2024, p.1-25. https ://www.researchgate.net/deref/https%3A%2F%2Fdoi.org%2F10.19044%2Fesj.2024.v20n37p1?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19
[2502] D.J. Solove, *The Digital Person: Technology and Privacy in the Information Age*, NYU Press, 2004. https ://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=2501&context=faculty_publications
[2503] P.M.Regan, *Légiférer sur la protection de la vie privée : technologie, valeurs sociales et politiques publiques*, University of North Carolina Press, 1995. Par exemple, au XIe siècle, Guillaume le Conquérant recueille des informations sur ses sujets en matière de fiscalité. http ://www.jstor.org/stable/10.5149/9780807864050_regan. Consulté le 24 septembre. 2024.
[2504] Archives nationales, *Domesday Book*. https ://cdn.nationalarchives.gov.uk/documents/education/domesday.pdf
[2505] R. Ellis Smith, *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet,* Harvard Law Review, vol. 94, 1981. p.1906–07.
[2506] D. J. Solove, *Understanding Privacy*, Harvard University Press, 2008.
[2507] S. Warren, L. Brandeis. « *The Right to Privacy* », Harvard Law Review, vol.IV, no.5, 1890.

la technologie (l'apparence de la photographie étant le meilleur exemple de la météo à cet égard) peuvent affecter la vie privée, supprimant la liberté et la créativité.

§1. CRYPTOGRAPHIE ENCOURAGÉE PAR LES LÉGISLATIONS

892. Protection pénale de la vie privée en Roumanie. Le Code pénal roumain criminalise en son article 302[2508] la violation du secret de la correspondance, ainsi que l'interception, sans droit, d'un appel ou d'une communication faite par des moyens électroniques. Et l'article 226[2509] réglemente la surveillance et l'enregistrement sans consentement, la divulgation d'images et de sons sans le consentement de la personne sanctionnée. Selon l'article 28 de la Constitution roumaine, « le secret des lettres, télégrammes, autres envois postaux, appels téléphoniques et autres moyens légaux de communication est inviolable »[2510].

893. Justifications: sécurité nationale et terrorisme. Sous certaines conditions, les interceptions sont autorisées, pour la protection de la sécurité nationale ou la lutte contre le terrorisme. L'article 13 de la loi 51/1991[2511] stipule que les organes chargés de la sécurité nationale, y compris le Service roumain de renseignement (Sri), ne peuvent intercepter des communications qu'avec l'autorisation d'un juge. Ensuite, l'article 14 oblige les fournisseurs de services de télécommunications à coopérer avec les autorités et à leur permettre d'accéder aux données faisant l'objet d'une interception. Le Code de procédure pénale réglemente également l'interception des communications comme moyen de preuve dans les enquêtes pénales. L'article 138 inclut l'interception des communications dans les mesures techniques de surveillance pour les enquêtes sur les infractions pénales, et l'article 139 définit les conditions dans lesquelles les communications peuvent être interceptées. L'interception ne peut être utilisée que s'il existe des motifs raisonnables de soupçonner une infraction grave et que la mesure doit être proportionnée à l'objectif visé. Toute interception doit être préalablement autorisée par un juge, conformément à l'article 142 du Code de procédure pénale[2512].

894. Protection pénale de la vie privée en France. En France, l'interception des communications est réglementée par le Code de procédure pénale. L'article 100 dispose que

https ://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

[2508] *Le Code Pénal du 17 juillet 2009, Chapitre II - infractions de service - article 295-309*

[2509] *Le Code Pénal du 17 juillet 2009, Chapitre IX - infractions affectant le domicile et la vie privée - articles 224 à 227.* https ://legislatie.just.ro/Public/DetaliiDocument/185905

[2510] *Le Code Pénal, Art. 302 Violation du secret de correspondance* | https ://lege5.ro/gratuit/gezdmnrzgi/art-302-violarea-secretului-corespondentei-codul-penal?dp=gqytsojvgq3tc

[2511] *Loi no 51 du 29 juillet 1991* (**republiée**), publiée au Journal Officiel, no190, du 18 mars 2014 https ://legislatie.just.ro/Public/DetaliiDocument/1517

[2512] *Code de procédure pénale* du 1er juillet 2010. (*actualisé*) https ://legislatie.just.ro/Public/DetaliiDocument/185907

l'écoute électronique des communications téléphoniques n'est autorisée que dans le cadre d'une enquête judiciaire. Leur autorisation par une autorité judiciaire compétente est obligatoire.[2513] Les infractions pour lesquelles ces mesures peuvent être utilisées (criminalité organisée, terrorisme, trafic de stupéfiants) sont précisées à l'article 100-1. En outre, les articles 100-2 à 100-8 décrivent la procédure dans laquelle les interceptions sont effectuées, leur durée maximale, les possibilités de prolongation, les moyens de suppression et la manière dont elles peuvent être utilisées dans un processus.[2514]

895. Nécessité d'une autorisation. En son article 66, la Constitution française impose au juge d'autoriser les interceptions, afin de protéger au mieux la vie privée des citoyens.[2515]Le droit à la vie privée dans ce cadre est également protégé par la Commission nationale de l'informatique[2516] et des libertés (CNIL) et la Déclaration des droits de l'homme et du citoyen de 1789.[2517] La CNIL surveille la mise en œuvre des mesures de surveillance des communications, en veillant à ce qu'elles respectent les droits fondamentaux et soient limitées dans le temps et dans l'objectif.[2518] Dans sa délibération n° 2015-078 du 5 mars 2015,[2519] la CNIL émet un avis sur la loi sur l'information, soulignant la nécessité d'un contrôle rigoureux et du respect de règles strictes puisque ces activités de surveillance et de collecte d'informations interfèrent massivement dans la vie privée et les données personnelles de l'individu[2520].

La cryptographie, science qui protège les informations en les chiffrant, est essentielle pour assurer la sécurité, la confidentialité et l'intégrité des communications et des transactions.[2521] Les applications de messagerie les plus populaires, WhatsApp, Telegram, signal, utilisent le cryptage pour protéger leurs informations.[2522] Il existe plusieurs types de chiffrement : la cryptographie intégrale et la cryptographie de bout en bout. La cryptographie

---

[2513] P. Dourneau-Josette,. *Interceptions de correspondances émises par la voie des télécommunications électroniques*, Dalloz, 2016. (actualisation: 2020) https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ENCY/PEN/RUB000386/2016-07/PLAN017

[2514] *Code de procédure pénale*, Sous-section 2 : des interceptions de correspondances émises par la voie des communications électroniques (articles 100 à 100-8) https ://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000006182887/2020-03-24/#LEGISCTA000032655289

[2515] *Constitution du 4 octobre 1958*. https ://www.legifrance.gouv.fr/loda/id/LEGISCTA000042418213

[2516] V. Gautron, *Fichiers de police, art.2, § 1: Missions et pouvoirs de la Commission nationale de l'informatique et des libertés (CNIL)*, pf 29-32, Dallo, 2015. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ENCY/PEN/RUB000374/2015-04/PLAN010

[2517] *Déclaration universelle des droits de l'homme.* https ://www.ohchr.org/en/human-rights/universal-declaration/translations/romanian-romana

[2518] *Décret no 2019-536 du 29 mai 2019*, Pris pour l'application de la *loi no 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Art. 141*. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=DATA195466

[2519] *Délibération 2015-078 du 5 mars 2015.* https ://www.legifrance.gouv.fr/cnil/id/CNILTEXT000030395106/

[2520] C. Lazerges, *Hervé Henrion-Stoffel*, Chronique de politique criminelle, 2015. politique-criminelle-renseignent-et-droits-de-lhomme.pdf

[2521] CNIL, *Comprendre les grands principes de la cryptologie et du chiffrement*, 2016. https ://www.cnil.fr/fr/cybersecurite/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement

[2522] W. Stallings, *Cryptography and Network Security : Principles and Pratice,* 7th Global Edition, Pearson, 2017.

de bout en bout est une méthode par laquelle une conversation privée entre deux personnes ne peut pas être interceptée par une tierce personne.[2523]

A. Reconnaissance de la cryptographie dans le cadre réglementaire

896. La législation française et roumaine reconnaît l'importance du cryptage et encourage son utilisation pour la protection des données personnelles, la confidentialité, la vie privée et l'intégrité des informations.

L'article 32, paragraphe 1, du RGPD sur la « sécurité des traitements » (applicable en France et en Roumanie) préconise l'utilisation de la pseudonymisation préserver la confidentialité et l'intégrité des données personnelles face aux progrès technologiques rapides.[2524]

En France, la loi n° 2018-133, également appelée loi sur la cybersécurité, promeut l'utilisation du chiffrement pour renforcer la protection des données.[2525] Actuellement, le projet de loi n° 659 pour les années 2019-2025 contient diverses dispositions sur la défense. En ce qui concerne la cybersécurité, elle propose d'autoriser différents systèmes de détection de fuites potentielles, systèmes conçus pour alerter les abonnés de la vulnérabilité.[2526]

a). Règlement ePrivacy

897. L'importance du cryptage pour garantir la confidentialité numérique. Le comité européen de la protection des données (EDPB) a adopté en 2021 une déclaration soulignant la nécessité du cryptage pour garantir la confidentialité des communications électroniques, soulignant l'importance d'adopter le règlement ePrivacy en tant que règlement complémentaire du RGPD visant à garantir un cadre cohérent et complet pour la protection des données et la vie privée dans l'environnement numérique.[2527] Bien que le document ci-dessus ne traite pas

---

[2523] S. Bradner, "*The end of end-to-end security ? [Internet Security] »*, in IEEE Security & Privacy, vol.4, no.2, p.76-79, 2006. Mots clés : services Web et Internet ; réseaux IP ;TCPIP ;protocoles ;sécurité du système de communication ;partage de vidéos ;cybercriminalité ;sites Web ;Terre ;réseaux neuronaux cellulaires ;sécurité Internet ;conception de système de bout en bout ;sécurité de bout en bout.

[2524] *Article 32 - Règlement général de l'UE sur la protection des données "sécurité du traitement"* https ://www.privacy-regulation.eu/ro/32.htm

[2525] *Loi n° 2018-133 du 26 février 2018 portant diverses d'adaptation au droit de l'Union Européenne dans le domaine de la sécurité*. https ://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036644772

[2526] Projet de *loi n°659*, Chapitre III - Dispositions relatives à la cyber-défense, Article 19 .-https ://www.assemblee-nationale.fr/dyn/15/textes/l15b0659_projet-loi#D_Chapitre_III_30

[2527] *Statement 03/2021 on the ePrivacy Regulation*, adopted on 9 March 2021 https ://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2021/03/edpb_statement_032021_eprivacy_regulation_en.pdf

directement des limites du chiffrement dans le contexte de[2528] la sécurité nationale, il n'appuie pas les tentatives visant à limiter le chiffrement pour des raisons de sécurité nationale et souligne que cela devrait être soigneusement réglementé.

898. Conservation généralisée et accès illimité, incompatibles avec le droit européen. En adoptant la déclaration susmentionnée, EDPB s'est également fondée sur la jurisprudence de la Cour de justice de l'Union Européenne (CJUE) de 2020 – affaires jointes C-511/18, C-512/18 et C-520/18,[2529] qui examinait la légalité de la législation nationale sur la collecte et la conservation de données de masse, impliquant des états tels que la France, la Belgique et le Royaume-Uni. La CJUE confirme que les lois nationales prévoyant une conservation généralisée et un accès illimité aux données personnelles ou la localisation des utilisateurs d'internet et de téléphone ne sont pas compatibles avec le droit de l'UE.[2530] Dans le même temps, la Cour rappelle que, dans les situations où la sécurité nationale est gravement menacée, ou pour lutter contre les formes graves de criminalité, des mesures peuvent être imposées pour accéder à ces données, mais dans le respect du principe de proportionnalité.[2531]

À la suite de la décision de la CJUE dans les affaires C-520/18, C-512/18 et C-511/18, le Conseil d'État constate que les articles L. 851-1, L. 851-2, L. 851-3 (alinéa IV) et L. 851-4 du Code de sécurité intérieure[2532] (SID) ne sont pas conformes aux règles de l'Union Européenne. En analysant les deux lois, les principales incompatibilités concernent la collecte et l'accès aux données personnelles, la surveillance massive des communications à des fins de sécurité nationale.[2533]

En 2022, la Cour de cassation française aligne le droit national sur le droit européen, en ce qui concerne les restrictions de conservation et d'accès aux données de communication (internet et téléphone). Il réaffirme que la conservation de ces données ne peut se faire de manière générale et indifférenciée et que l'accès par les autorités doit être proportionné à la raison et soumis à des critères clairs, tels qu'une autorisation légale préalable.[2534]L'engagement

---

[2528] S. Landau, *Surveillance or Security ? The Risks Posed by New Wiretapping Technologies*, MIT press, 2011.

[2529] Judgment of the Court (Grand Chamber) of 6 October 2020, affaires no *C-511/18, C-512/18* and *C-520/18*. https ://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CJ0511

[2530] *Données personnelles : interdiction des collectes générales des services de sécurité — Cour de justice de l'Union Européenne*, Dalloz, 2021. p.406 https ://www.dalloz.fr/lien?famille=revues&dochype=RECUEIL%2FJURIS%2F2021%2F0352

[2531] *Protection des données : la CJEU inléchit sa jurisprudence — Cour de justice de l'Union Européenne,* AJDA 2020. p.1880 https ://www.dalloz.fr/lien?famille=revues&dochype=AJDA%2FJURIS%2F2020%2F2083

[2532] *Code de la sécurité intérieure* , Titre V : des techniques de recueil de renseignement soumises à autorisation (articles L851-1 à L855-1 C), Chapitre Ier : des accès administratifs aux données de connexion (articles L851-1-7)

[2533] *Code de la communication, Code de la sécurité intérieure* https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=COMI021430

[2534] B. Nicaud, *Restrictions à la conservation des données de connections et à leur accès : la Cour de cassation tire les conséquences de la jurisprudence de la CJUE,* Dalloz, 2022. https ://www.dalloz-

juridique des fournisseurs à protéger les données de leurs utilisateurs est également inscrit dans la Charte des droits fondamentaux de l'UE, articles 7 (« respect de la vie privée »[2535]) et 8 (« protection des données à caractère personnel »), qui régit également la mesure dans laquelle l'autorité publique peut intervenir dans ce droit.[2536] De son côté, la Convention européenne des droits de l'homme, en son article 8, consacre le droit au respect de la vie privée, y compris la correspondance.[2537]

b). Résolution du Conseil de l'Europe « Sécurité par cryptage et sécurité malgré le cryptage »

899. Le 14 décembre 2020, le Conseil de l'Europe a adopté la résolution « sécurité par le cryptage et sécurité malgré le cryptage »[2538]. Dans ce document, deux aspects quelque peu contradictoires sont mis en évidence : D'une part, le cryptage doit être encouragé, développé et nécessaire pour fournir un cadre sûr pour la protection des données numériques, et d'autre part, le cryptage « rend l'accès aux preuves et leur analyse extrêmement difficiles, voire impossibles, à réaliser dans la pratique ». Il est également démontré qu'un équilibre entre les deux est nécessaire dans un contexte où la preuve des délits par les organes judiciaires est rendue beaucoup plus facile par l'accès aux informations trouvées dans les conversations cryptées ou dans les environnements informatiques cryptés. Il souligne l'importance du cryptage comme outil essentiel de protection des données personnelles, en encourageant son utilisation mais aussi en attirant l'attention sur les obstacles qu'il peut faire peser sur la justice et la sécurité. Il est nécessaire de trouver un équilibre entre la protection de l'individualité et l'autorisation d'un accès légal aux données lorsque cela est nécessaire.[2539]

900. Solutions techniques relatives à la sécurité par cryptage. La proposition concrète du Conseil est d'ouvrir un dialogue actif avec les représentants de l'industrie informatique, associant à la fois les milieux universitaires, les autorités judiciaires et même la société civile, afin d'identifier des solutions techniques pour l'accès aux données cryptées. Évidemment,

actualite.fr/flash/restrictions-conservation-des-donnees-de-connections-et-leur-acces-cour-de-cassation-tire-conse

[2535] *Charte des droits fondamentaux de l'Union Européenne Titre II – libertés, article 7.* https ://fra.europa.eu/ro/eu-charter/article/7-respectarea-vietii-private-si-de-familie

[2536] *Charte des droits fondamentaux de l'Union Européenne Titre II – libertés, article 8.* https ://fra.europa.eu/ro/eu-charter/article/8-protectia-datelor-cu-caracter-personal

[2537] *Convention européenne des droits de l'homme*. https ://www.echr.coe.int/documents/d/echr/Convention_RON

[2538] *Encryption: Council adopts resolution on security through encryption and security despite encryption,* Council of the EU, Press release, 2020. https ://www.consilium.europa.eu/ro/press/press-releases/2020/12/14/encryption-council-adopts-resolution-on-security-through-encryption-and-security-despite-encryption/

[2539] *Résolution du Conseil sur le cryptage Sécurité par le cryptage et sécurité malgré le cryptage, Conseil de l'Union européenne*, 2020. https ://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/ro/pdf

l'objectif est de lutter contre la criminalité. Dans le même temps, il est proposé d'élaborer un ensemble de règles qui permettraient aux organes judiciaires de jouer leur rôle actif dans la détection des délits « tout en protégeant la vie privée, les droits fondamentaux et la sécurité des communications ».

Après l'adoption de la résolution sur la « sécurité par le cryptage » le 23 juin 2021, la « communication de la Commission au Parlement Européen et au Conseil sur le deuxième rapport d'étape sur la stratégie de l'UE pour une union de la sécurité » a été publiée. Dans ce document[2540], nous trouvons une définition du terme cryptage[2541] mais aussi une série d'actions ciblées concernant la mise en œuvre de[2542] la stratégie de l'UE en matière de sécurité, la sensibilisation aux risques actuels et la manière de répondre de toute urgence aux menaces extérieures. L'attitude des criminels à utiliser des applications de cryptage suscite des inquiétudes et, dans le même temps, « les autorités répressives de l'UE doivent continuellement développer leur capacité à traiter des informations cryptées dans le cadre d'enquêtes criminelles ». Il appartient aux États membres d'utiliser le nouvel outil de décryptage d'Europol[2543], une plateforme développée en partenariat avec le Centre commun de recherche de la Commission européenne et bénéficiant d'un ordinateur de grande puissance situé dans un centre de recherche à Ispra, en Italie. Les capacités de ce supercalculateur ont été mises gratuitement à la disposition des états pour décrypter légalement des informations provenant de réseaux terroristes ou criminels organisés, sans compromettre le cryptage lui-même et implicitement la vie privée des utilisateurs.

901. La cryptographie post-quantique met-elle en danger votre vie privée ? Afin de mettre en œuvre la « stratégie de l'union de la sécurité », une première étape a consisté à réaliser une « cartographie détaillée de la manière dont les États membres gèrent le cryptage, ainsi qu'un processus multipartite d'exploration et d'évaluation des options juridiques, éthiques et techniques ». Progressivement, ces dernières années, les débats ont évolué jusqu'à la publication au Journal officiel de l'Union Européenne le 11.04.2024 de la Recommandation (UE) 2024/1101 de la Commission sur la feuille de route pour la mise en œuvre coordonnée de

---

[2540] *Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions relative au plan d'action pour la démocratie européenne*, Commission européenne, 2020. https ://eur-lex.europa.eu/resource.html?uri=cellar:37e1dec3-0745-11ec-b5d3-01aa75ed71a1.0006.02/DOC_1&format=PDF

[2541] « *Le cryptage est une technologie clé dans le domaine de la sécurité, pour sécuriser les systèmes et les transactions numériques, ainsi que pour protéger les droits fondamentaux, y compris la liberté d'expression, la vie privée et la protection des données*. »

[2542] *Stratégie de l'Union européenne pour l'union de la sécurité* https ://eur-lex.europa.eu/RO/legal-content/summary/eu-security-union-strategy.html

[2543] A. Vitard, *Pourquoi la nouvelle plateforme de déchiffrement d'Europol inquiète des députés européens?,* l'Usine Dgitale, 2021. https ://www.usine-digitale.fr/article/pourquoi-la-nouvelle-plateforme-de-dechiffrement-d-europol-inquiete-des-deputes-europeens.N1074809

la transition vers la cryptographie post-quantique[2544]. Une opinion ferme est exprimée en ce sens que les États membres doivent modifier radicalement les « algorithmes, protocoles et systèmes cryptographiques » pour passer à la « cryptographie post-quantique ». Cette recommandation intervient après que 11 états membres ont signé la « Déclaration européenne sur les technologies quantiques » le 6 décembre 2023, une déclaration initiée pendant la présidence espagnole du Conseil de l'Union Européenne[2545], mais considérée avec scepticisme[2546]. Parmi les signataires initiaux figurent la France, mais l'Allemagne ne l'est pas, cette dernière arguant qu'il n'est pas encore temps d'entreprendre une telle initiative[2547]. Enfin, 26 états membres ont signé la déclaration exprimant un idéal difficile : l'UE doit être la nouvelle « vallée quantique » du monde[2548], un formidable concurrent pour la Chine et les États-Unis. À ce stade, l'ordinateur quantique[2549], un système informatique bien supérieur à celui d'aujourd'hui, est au niveau du projet[2550], étant au stade de la recherche. Tant les gouvernements des états les plus puissants[2551] que les géants de l'informatique[2552] poursuivent le supercalculateur, et la législature des états qui ont déjà compris la menace se prépare à la réponse. La réalisation de ce projet conduira automatiquement à un véritable problème[2553] qui mettrait en danger à la fois les données privées des individus et la sécurité nationale des états : le système de cryptage actuel sera inutile. Bref, c'est dans ce contexte que la Commission

---

[2544] *Recommandation (UE) 2024/1101 de la Commission sur la feuille de route pour la mise en œuvre coordonnée de la transition vers la cryptographie post-quantique*, Journal officiel de l'Union européenne, 2024. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:L_202401101

[2545] G. Fleureau, *Onze pays membres de l'Union européenne, dont la France, renforcent leur collaboration en informatique quantique,* Siecle digital, 2023. https://siecledigital.fr/2023/12/08/onze-pays-membres-de-lunion-europeenne-dont-la-france-renforcent-leur-collaboration-en-informatique-quantique/

[2546] « *Bien que le pacte soit un pas dans la bonne direction, le manque de soutien démontre que l'Europe ne perçoit toujours pas les technologies quantiques comme une priorité stratégique* », a déclaré Andrea Rodríguez, représentante du Centre de Politique Européenne, spécialiste des questions numériques

[2547]A. Clasen, *L'Espagne présente un nouveau « pacte quantique » européen,* Euractiv, 2023. https ://www.euractiv.fr/section/strategie-industrielle/news/lespagne-presente-un-nouveau-pacte-quantique-europeen/

[2548] *Façonner l'avenir numérique de l'Europe,* Commission européenne, 2025. https ://digital-strategy.ec.europa.eu/fr/policies/quantum

[2549] « *Les ordinateurs quantiques sont des calculateurs reposant sur des principes physiques fondamentalement différents des ordinateurs classiques actuels. Si de tels ordinateurs de grande taille sont un jour construits, ils pourraient effectuer certaines tâches beaucoup plus rapidement que ces derniers* », définition trouvée dans *« Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique, 14/04/2022* »

[2550] *L'ordinateur quantique : tout comprendre en 15 minutes* Polytechnique insights, 2023. https ://www.polytechnique-insights.com/tribunes/science/lordinateur-quantique-tout-comprendre-en-15-minutes/

[2551] *President Biden Signs Memo to Combat Quantum Computing Threat,* NSA/CSS news, 2022. https ://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3020175/president-biden-signs-memo-to-combat-quantum-computing-threat/

[2552]*IBM quantum case studies*, IBM. https ://www.ibm.com/quantum/case-studies

[2553] M. Kop, V. Wadhwa, "*How to Prevent Quantum-A.I. Hybrids from Taking Over the World*", Fortune, 2023 ; Intelligence Report on the Multilateral Governance of Quantum Computing for the SDGs, Genève, Oct. 2023

européenne a présenté sa recommandation sur la transition vers la cryptographie post-[2554]quantique, bien que concrètement l'ordinateur quantique n'ait pas encore été lancé.

c). La France a déjà introduit dans sa législation la notion de cryptographie post-quantique

902. La France, acteur majeur de la découverte de l'ordinateur quantique[2555], a déjà introduit la notion de cryptographie post-quantique dans une législation récente. Il s'agit d'une loi sur la stratégie militaire[2556] pour la période 2024-2030, et de l'ordonnance[2557] émise en février 2024 par le ministère de l'économie, des Finances et de la souveraineté industrielle et numérique, qui concerne l'exportation de technologies associées à l'ordinateur quantique. Les juristes français regardent déjà avec intérêt le terrain et comment une question simple : « Comment réguler ce qui n'existe pas encore et dont l'existence même et les effets potentiels sont sujets à débats ? »[2558]. L'Agence française de cybersécurité (ANSSI) a déclaré : "La menace quantique doit être prise en compte avant de savoir si elle deviendra un jour réalisable. Ainsi, un changement profond de la cryptographie à clé publique doit être globalement initié pour anticiper un éventuel effondrement de la sécurité des infrastructures cryptographiques actuelles"[2559]. Dans le même temps, d'autres avocats attendent une réglementation législative claire sur la cybersécurité à l'ère de la cryptographie post-quantique[2560]. Tous ces débats tournent autour de la notion de sécurité de l'information gouvernementale et de protection de la vie privée.

B. Cryptage : protection de la vie privée ou protection contre la criminalité

[2554] *Qu'est-ce que la cryptographie post-quantique ?,* IBM. https://www.ibm.com/fr-fr/topics/quantum-safe-cryptography

[2555] *France 2030 : Point d'étapes trois ans après le lancement de la stratégie nationale des technologies quantiques et lancement du programme Proqcima,* Ministère de l'Enseignement supérieur et de la Recherche, 2024. https://www.enseignementsup-recherche.gouv.fr/fr/france-2030-point-d-etapes-trois-ans-apres-le-lancement-de-la-strategie-nationale-des-technologies-95121

[2556] *Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressantes pour la défense*

[2557] *Arrêté du 2 février 2024 relatif aux exportations vers les pays tiers de biens et technologies asssociés à l'ordinateur quantique et à ses technologies habilitantes et d'équipements de conception, développement, production, test et inspection de composants électroniques avancés*

[2558] J. Charpenet, M. Teller, *La régulation des technologies quantiques : un cas d'école pour la régulation des innovations « totales »*, Dalloz IP/IT, 2024. pg 459

[2559] Agence nationale de la sécurité des systèmes d'information (ANSSI), *Avis scientifique et technique de l'ANSSI sur la migration vers la cryptographie post-quantique,* 2022. https ://cyber.gouv.fr/sites/default/files/2022/04/anssi-avis-migration-vers-la-cryptographie-post-quantique.pdf

[2560] A. Latil, *A quand le Quantum Act?,* Recueil Dalloz no.43, 2023, p. 2185

903. Il est généralement admis que le cryptage est une solution indispensable pour protéger la vie privée et la sécurité en ligne[2561], mais en même temps il est également un obstacle important dans la lutte contre le crime organisé et le terrorisme, avec de nombreuses analyses indiquant que cette technologie est préférée non seulement par les citoyens pour protéger leur vie privée, mais aussi par le fait qu'elle ne l'est pas seulement par les citoyens, mais aussi des criminels et des organisations terroristes pour masquer leurs activités illégales.[2562] Par exemple, des groupes comme ISIS ont utilisé des applications comme Telegram et WhatsApp pour coordonner les attaques et les organiser sans être détectés[2563]. Ces plateformes sont utilisées pour distribuer du matériel de propagande et recruter de nouveaux membres.[2564] Selon un rapport publié par The Guardian, l'Etat islamique a utilisé Telegram pour communiquer avec des cellules terroristes dans différentes parties du monde et pour organiser des attaques majeures, y compris en Europe.[2565]

a). Conflit entre Apple et FBI au sujet de l'accès aux informations privées

904. La CJCE reste inébranlable, s'opposant à la préservation et à l'accès généralisés et indifférenciés des communications électroniques, même dans le but de lutter contre la criminalité, quelle que soit sa gravité.[2566] L'Union Européenne considère cette mesure comme un véritable piège pour le droit à la vie privée.[2567] Dans ce contexte, il est compréhensible que les autorités soient sceptiques quant à la difficulté d'accéder à des informations cryptées.[2568] Le chiffrement rend l'accès aux données et aux messages d'une conversation inaccessible à quiconque n'a pas la clé. Un conflit célèbre sur le sujet vient d'outre-mer, impliquant Apple et le FBI. En 2016, le FBI a demandé l'accès à l'iPhone d'un suspect terroriste, mais le cryptage

[2561] F. G'sell, *Le chiffrement est-il un droit fondamental ? Une étude de cas sur la réglementation du CSAM dans l'UE,* 2023 https ://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2023/07/Chiffrement-comme-droit-fondamental.pdf
[2562] B. Schneier, *Data and Goliath : The Hidden Battles to Collect Your Data and Control Your World*. W.W. Norton & Company, 2015.
[2563] G. Greenwald, *No Place to Hide: Edward Snowden, the NSA and the U.S. Surveillance State*, Metropolitan Books, 2014.
[2564] *ISIS militants usong encrypted apps to evade detection*, BBC News, 2020.
[2565] *Telegram : the app of choice for ISIS*, The Guardian, 2017
[2566] M.C. de Montecler, *Conservation des données : la Cour de justice de l'Union Européenne persiste et signe*. Dalloz actualité, 2022. https ://www.dalloz-actualite.fr/flash/conservation-des-donnees-cour-de-justice-de-l-union-europeenne-persiste-et-signe
[2567] B. Nicaud, *Restrictions à la conservation des données de connections et à leur accès : la Cour de cassation tire les conséquences de la jurisprudence de la CJUE,* Dalloz actualité, 2022. > https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ACTU0213973
[2568] S. Levy, *Crypto : How the Code Rebels Beat the Gorvenment Saving Privacy in the Digital Age*, Penguin, 2001. Discute de la cryptographie avancée et de la façon dont les gouvernements tentent d'accéder à l'information cryptée.

avancé de l'appareil a empêché les autorités d'obtenir les informations nécessaires à l'enquête.[2569] Bien que le FBI ait un mandat légal, Apple a refusé de développer une version du logiciel qui permettrait l'accès, arguant qu'il devait protéger la vie privée de tous ses utilisateurs[2570]. Cet incident a mis en lumière la tension entre le droit à la vie privée et la nécessité pour les autorités d'accéder à des informations essentielles à la sécurité publique.[2571]

b). Telegram bloquée sur le territoire de la Russie

905. Une affaire plus récente est Podchasov c. Russie (demande n° 33696/19),[2572] où l'obligation légale des applications de messagerie (en l'occurrence Telegram) de stocker et de fournir aux autorités russes les données de communication, ainsi que les informations nécessaires pour décrypter les messages, est analysée. Parce qu'il ne se conforme pas, Telegram est condamnée à une amende et bloquée sur le territoire russe. La Cour européenne des droits de l'homme a condamné la Russie pour violation de son droit à la correspondance. La Cour européenne des droits de l'homme conclut dans cette affaire que l'attaque contre la sécurité du cryptage « est incompatible avec une société démocratique ».[2573] Bien qu'il s'agisse d'une victoire importante pour la protection de la vie privée, il s'agit peut-être de la dernière condamnation de la Russie depuis son retrait de la Convention européenne des droits de l'homme.[2574]

c). Propriétaire de Telegram arrêté en France

906. L'arrestation de Durov, le chef de Telegram, illustre la manière dont les états européens vont traiter le refus des opérateurs de services de donner aux autorités accès au contenu de leurs

[2569] C. Baily, W. Garland, L. Nitchals, J. O'Rourke, James, *Apple, Inc : Data Privacy and a Request from the FBI*, Eugene D. Fanning Center for Business Communication, University of Notre Dame, publié sur SAGE Business Cases, 2017.
[2570] K. Zetter, *Apple vs. FBI : à Inside the Battle Ober Encryption*, Wired, 2016.
[2571] A. Parienty, *Apple contre le FBI : les dessous d'un bras de fer*, Alternatives économiques, n° 356, 2016. p.73-73. https ://shs-cairn-info.docelec.u-bordeaux.fr/magazine-alternatives-economiques-2016-4-page-73?lang=fr.
[2572] ECHR, Case of *Podchasov c. Russia, no. 33696/19*, 2024. https ://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2024/03/case_of_podchasov_v._russia.pdf
[2573] C. Béchade, *Les portes dérobées dans le chiffrement sont "incompatibles avec une société démocratique", juge la Cour européenne des droits de l'homme,* Clubic, 2024. https ://www.clubic.com/actualite-518911-les-portes-derobees-dans-le-chiffrement-sont-incompatibles-avec-une-societe-democratique-juge-la-cour-europeenne-des-droits-de-l-homme.html
[2574] C. Zorn, *Le chiffrement des communications protège les droits de l'homme, en Russie et ailleurs,* Dalloz actualité, 2024. https ://www.dalloz-actualite.fr/flash/chiffrement-des-communications-protege-droits-de-l-homme-en-russie-et-ailleurs

plateformes informatiques.[2575] Le 24 août 2024, Pavel Durov a été arrêté en France pour activités illégales (trafic de drogue, abus sexuels) sur son application de messagerie[2576]. Il est également accusé de refuser de coopérer avec les autorités françaises pour décrypter les communications privées, ce qui est illégal en France en vertu de la loi sur la lutte contre le terrorisme et le crime organisé[2577].

d). Les effets négatifs du chiffrement : une source d'inquiétude pour le droit

907. Offrir aux autorités nationales un accès illimité aux données numériques. En 2016, à la lumière des nombreux attentats terroristes perpétrés contre des pays européens, un premier débat au sein de l'Union Européenne sur le cryptage portait sur la lutte contre le terrorisme.[2578] La France, l'un des pays les plus touchés, propose une loi qui permet aux applications de communication en ligne de donner aux autorités nationales un accès complet aux données demandées[2579]. Depuis 2015, en réponse aux attentats terroristes en France[2580], la loi 2015-912 sur les services de renseignement est en vigueur. Elle légalise les activités des services de renseignement et de surveillance. Ces derniers peuvent surveiller les conversations en les écoutant, surveiller l'activité en ligne, accéder aux données GPS,[2581] ou utiliser des techniques plus avancées, comme l'utilisation d'algorithmes d'intelligence artificielle pour détecter le comportement humain (boîte noire) ou le piratage légal (infiltration d'ordinateurs, de serveurs, de réseaux)[2582].En élargissant considérablement la capacité de l'État à surveiller et contrôler la vie privée des citoyens, cette loi a généré de multiples plaintes suscitant la suspicion de faire de

[2575] G. Stargardter, *Behind the arrest of Telegram boss, a small Paris cybercrime unit with big ambitions*, Reuters, 2024.
[2576] *Arrestation de Pavel Durov, patron de Telegram*, Doc du Juriste, blog juridique, 2024. https ://www.doc-du-juriste.com/blog/actualites-droit/arrestation-pavel-durov-patron-telegram-27-08-2024.html
[2577] *Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale* https ://www.legifrance.gouv.fr/jorf/id/JORFSCTA000032627246
[2578] *Communication de la Commission au Parlement européen et au Conseil relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme*, 2016. https ://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52016DC0050
[2579] *Rapport d'information n°1833*, déposé en application de l'article 145 du règlement, par la commission des affaires étrangères, en conclusion des travaux d'une mission d'information sur la lutte contre le financement du terrorisme international https ://www.assemblee-nationale.fr/dyn/15/rapports/cion_afetr/l15b1833_rapport-information
[2580] *Loi n° 2015-912 du 24 juillet 2015 relative au renseignement*. https ://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899/2015-07-27/
[2581] O. de Maison Rouge, *Le droit français du renseignement, Section 2 - Techniques de < renseignement > prévues par la loi*, Dalloz, pf.24-25, 2019. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ENCY/IPIT/RUB000427/2019-09/PLAN/0011
[2582] *La Loi sur le renseignement : présentation générale* https ://actu.dalloz-etudiant.fr/a-la-une/article/la-loi-sur-le-renseignement-presentation-generale/h/38e9460b1970b18b4906ca73415c4352.html

la France un « État de surveillance ».[2583] Face à ces préoccupations, le Conseil constitutionnel a censuré certains dispositifs initialement prévus par la loi, dans le cadre de la décision 2015-713 DC[2584]. Par conséquent, le Conseil constitutionnel détermine ce qui est impératif que toute mesure de contrôle respecte le principe de proportionnalité et soit soumise à un contrôle judiciaire strict afin d'éviter les abus.[2585] Suite à cette censure, la loi n° 2015-1556 du 30 novembre 2015 est née.[2586]

908. Plus récemment, afin de renforcer la surveillance et l'interception des communications en tant que mesure antiterroriste, la France a adopté en juillet 2021 la loi 2021-998, qui élargit les capacités des services de surveillance et d'interception de renseignements dans la lutte contre le terrorisme.[2587] Cela a rapidement fait l'objet de l'attention de la CNIL, dès lors que la loi était en phase de projet, notamment les articles 13 et 13 bis qui autorisent une nouvelle technique d'interception par satellite, qui devait être expérimentée pendant 4 ans Ainsi, dans la délibération n° 2021-045 d'avril 2021, la CNIL avertit que la loi peut gravement affecter les droits fondamentaux, le droit à la vie privée, et que cette collecte de données de masse peut également atteindre des personnes non impliquées dans des activités illégales. La CNIL exige l'introduction de filtres de tri avant l'utilisation de telles interceptions.[2588]

909. Critique de la décision de conserver les adresses IP. En 2024, la France s'est adressée à la Cour de justice de l'Union Européenne (CJUE) sur les mesures d'accès des autorités publiques aux données personnelles des citoyens. Ainsi, dans sa décision C-470/21[2589], rendue le 30 avril 2024, la Cour constate que la conservation générale des adresses IP (conformément à la directive 2002/58/ce[2590]) est incompatible avec le droit de l'Union. Toutefois, la Cour

---

[2583] X. Latour, *La loi relative au renseignement : un État de surveillance ?*, La semaine juridique administrations et collectivités territoriales, n° 40, 2015. p.2286 https ://fad4.u-bordeaux.fr/pluginfile.php/188796/mod_folder/content/0/XLatou%20la%20loi%20sur%20le%20renseignement%202015.pdf

[2584] Conseil constitutionnel, *23 juillet 2015*, *n° 2015-713 DC du* https ://www.conseil-constitutionnel.fr/decision/2015/2015713DC.htm

[2585] Conseil constitutionnel*, 23 juillet 2015 n° 2015-713*, Jurisprudence, Dalloz, 2015. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CONSCONST_LIEUVIDE_2015-07-23_2015713&FromId=IPIT_RUB000427_DOC_1

[2586] *Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales*. https ://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031549747

[2587] *Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement* https ://www.legifrance.gouv.fr/loda/id/LEGIARTI000043880740/2021-07-31/

[2588] CNIL, *Délibération n° 2021-045 du 15 avril 2021 portant avis sur les articles 13 bis et 13 ter du projet de loi relatif à la prévention d'actes de terrorisme et au renseignement (demande d'avis n° 21007082),* Dalloz, 2021. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CNIL_LIEUVIDE_2021-04-15_2021045

[2589] CJUE, *C-470/21*, Judgment https ://fra.europa.eu/en/caselaw-reference/cjeu-c-47021-judgment

[2590] *Directive 2002/58/CE du Parlement Européen et du Conseil du 12 juillet 2002 relative au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des communications publiques (Directive sur la vie privée et les communications électroniques*) https ://eur-lex.europa.eu/legal-content/RO/ALL/?uri=celex:32002L0058

autorise les autorités publiques à accéder à ces données, mais souligne la nécessité d'un contrôle par une autorité indépendante pour protéger les droits des citoyens.[2591]

910. Autres infractions facilitées par le cryptage. En ce qui concerne le chiffrement, il n'est pas seulement pertinent dans le contexte du terrorisme, mais aussi dans d'autres activités criminelles, telles que le trafic de drogue et le piratage. Par exemple, un article de Wired souligne comment WhatsApp est devenu une plateforme privilégiée pour les réseaux mondiaux de trafic de drogue.[2592]

Un autre exemple pertinent de l'utilisation de la cryptographie à des fins criminelles est le ransomware. Les attaquants de ransomware chiffrent les fichiers des victimes et demandent une rançon pour les déchiffrer.[2593] Le chiffrement de ces fichiers garantit que les autorités et les victimes ne peuvent pas accéder aux données sans la clé de déchiffrement, ce qui rend difficile leur récupération et l'identification des criminels.[2594]

Un autre domaine notable est celui des marchés en ligne illégaux, appelés « dark net », comme « Silk Road », une plateforme en ligne apparue en 2011, protégée par cryptographie, où les drogues et les marchandises illégales étaient échangées.[2595] Il a été fermé par le FBI en 2013 avec l'arrestation de son fondateur, Ross Ulbricht, 28 ans[2596]. Ces menaces peuvent être qualifiées de cybercriminalité, ce qui nécessite également l'émergence d'un moyen de défense, appelé cybersécurité[2597]. Lors de sa réunion annuelle de 2017, la Commission européenne présente un projet de lutte contre la cybercriminalité, dans lequel elle souligne l'importance du droit pénal dans la répression de ce crime[2598].

e). CEDH : les informations peuvent également être obtenues sans saboter le cryptage

[2591]CJUE, 30 avr. 2024, aff. C-470/21, *La CJUE précise les exigences concernant les modalités permettant à l'ARCOM, chargée de la lutte contre les contraçons commises en ligne, d'accéder à des données d'identification à partir d'une adresse IP*, Légipresse, Dalloz, p.278, 2024. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=LEGIPRESSE/CHRON/2024/0344

[2592] Wired, *Comment les criminels utilisent WhatsApp pour coordonner le commerce mondial de la drogue*.

[2593] The New York Times, *The Dark Side of Encryption : Comment les cybercriminels exploitent les mesures de sécurité ;*

[2594] BBC News, *Ransomware et cryptage : une menace croissante*.

[2595] The Investopedia team, *Qu'était la route de la soie en ligne ? Histoire et fermeture par le FBI, 2025.* https ://www.investopedia.com/terms/s/silk-road.asp

[2596] P. Ropartz, AFP agence, *États-Unis : qui est Ross Ulbricht, ce libertarien créateur du «eBay de la drogue», gracié par Donald Trump ?,* le Figaro, 2025. https://www.lefigaro.fr/international/etats-unis-qui-est-ross-ulbricht-ce-libertarien-createur-du-ebay-de-la-drogue-gracie-par-donald-trump-20250122

[2597] E. Autier, *Cybercriminalité : Bruxelles propose une nouvelle directive*, Dalloz 2017. https ://www.dalloz-actualite.fr/flash/cybercriminalite-bruxelles-propose-une-nouvelle-directive

[2598] État de l'Union, *Cybersécurité : la Commission dote l'UE de moyens supplémentaires pour répondre aux cyberattaques*, Dalloz, 2017. https ://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2017/09/ip-17-3193_fr

911. En discutant de l'équilibre entre la lutte contre la criminalité et la préservation des libertés, Fiona de Londras et Fergal Davis procèdent à une analyse détaillée des mesures de lutte contre ces crimes, en s'attachant à rendre plus efficaces les mesures traditionnelles de protection contre le terrorisme.[2599] Et la CEDH aborde ce sujet, dans les commentaires doctrinaux sur l'affaire Roman Zakharov[2600] c. Russie (2015), ou l'affaire Big Brother Watch et autres c. Royaume-Uni (requêtes nos 58170/2021, 62322/14 et 24960/15 – 13)[2601], soulignant qu'il existe d'autres moyens d'obtenir les informations nécessaires sans saboter le cryptage, comme les opérations secrètes, l'infiltration dans des groupes criminels, l'analyse des métadonnées ou la coopération efficace des services de renseignement internationaux.[2602] De plus, des études[2603] menées aux États-Unis ont montré que « *la surveillance de masse n'a pas contribué de manière significative à la lutte contre le terrorisme* »[2604].

§2. RÉGLEMENTATION LÉGALE CONCERNANT L'INTERCEPTION DES APPLICATIONS WHATSAPP, TELEGRAM, SIGNAL

912. Contrairement aux communications par réseau mobile, qui peuvent être facilement interceptées par la coopération des opérateurs, les communications via des applications mobiles, étant cryptées, ne peuvent pas être interceptées en mode classique. Au fil du temps, la perception de la cryptographie a changé, et la technologie est devenue de plus en plus accessible et largement utilisée par les citoyens, les entreprises et les organisations à but non lucratif.[2605] Dans ce contexte, les préoccupations des gouvernements augmentent, reflétant la crainte que l'utilisation généralisée de la cryptographie empêche les autorités de surveiller et d'intercepter les communications afin de prévenir les délits et les menaces à la sécurité publique.[2606] Leur interception nécessite un logiciel spécial, installé indétectable dans l'appareil mobile, tel que

---

[2599] F. de Londras, J. Doody, (eds.), *The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism,* 1st ed, Routledge, 2015. https ://doi.org/10.4324/9781315722320

[2600] Affaire *Roman Zakharov c. Russie*, requête no. 47143/06. https ://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159324%22]}

[2601] Affaire de *Big Brother Watch et autres v. Royaume-Uni*, requêtes nos. 58170/13, 62322/14 et 24960/15, https ://hudoc.echr.coe.int/fre#{"itemid":["001-210077"]}

[2602] Sur les enquêtes criminelles licites qui respectent la protection des données du XXIe siècle. *Déclaration commune d'Europol et de l'ENISA*, 2016. https ://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/on-lawful-criminal-investigation-that-respects-21st-century-data-protection

[2603] L. K. Donohue, *The future of Foreign Intelligence, Privacy and Surveillance in a Digital Age*, Oxford University Press, 2016.

[2604] R. Gallagher, *NSA Surveillance Played Little Role in Foiling Terror Plots, Experts Say*, The Guardian, 2013.

[2605] B. Schneier, *The Hidden Battles to Collect Your Data and Control Your World, Data et Goliath , (les batailles cachées pour collecter vos données et contrôler votre monde),* W.W. Norton & Company, 2015.

[2606] Cato Institute, *The Balance Between Encryption and National Security*

« cheval de Troie ».[2607] Il peut enregistrer des frappes au clavier, des sons, des captures d'écran, surveiller le trafic réseau, collecter des données confidentielles telles que des mots de passe, des données bancaires[2608]. L'utilisation de « chevaux de Troie » (ou de programmes similaires) pour lutter contre la criminalité soulève de nombreuses questions éthiques et juridiques, de sorte qu'ils ne sont autorisés que dans certains pays sous des réglementations strictes[2609].

913. Interception audio sans mandat, illégale même dans les lieux publics. En regardant l'histoire du dernier siècle des États-Unis, il convient de mentionner le cas de Katz v. [2610] En 1967, les États-Unis d'Amérique ont clarifié l'interprétation de l'amendement IV de[2611] la Constitution des États-Unis, qui protège les citoyens contre les perquisitions et les saisies injustifiées. La Cour suprême des États-Unis renforce l'amendement ci-dessus, remportant l'affaire Katz et déterminant qu'il est illégal d'intercepter une conversation téléphonique sans mandat, même dans des lieux publics (dans ce cas dans une cabine téléphonique)[2612]. Bien que la décision Katz ait assuré une protection importante de la vie privée, avec le développement de nouvelles technologies de communication, elle a paradoxalement réduit les attentes du public en matière de vie privée, créant ainsi de nouveaux défis pour la magistrature.[2613]

914. Interception sans mandat, uniquement dans les cas liés à la sécurité nationale. Immédiatement après les attentats du 11 septembre 2001, les États-Unis autorisent les agences du FBI et de la NSA à utiliser de tels logiciels de surveillance dans les enquêtes de sécurité nationale pour lutter contre la criminalité et le terrorisme [2614]en vertu du Patriot Act des États-Unis.[2615] La loi autorisait les autorités à effectuer des écoutes téléphoniques sans mandat dans le cadre d'enquêtes de sécurité nationale, ce qui compromettait les protections établies par l'arrêt Katz[2616]. Ainsi, bien que Katz demeure un précédent important dans le domaine de la protection de la vie privée, la réalité contemporaine marquée par les avancées technologiques

---

[2607] C.M. Steel, (2014) "*Technical Soddi Defenses : The Trojan Horse Defense Revisited*", Journal of Digital Forensics, Security and Law , vol.9 , no.4 , art.4, 2014. https ://doi.org/10.15394/jdfsl.2014.1192 disponible à l'adresse suivante : https ://commons.erau.edu/jdfsl/vol9/iss4/4

[2608] S. Brenner, B. Carrier, J. Henninger, *The Trojan Horse Defense in Cybercrime Cases*, Research Gate, 2004.

[2609] J. Daskal, *Law Enforcement access to Data Across Borders* : *The Evolving Security and Rights issues*, Journal of National Security Law and Policy, vol.8, 2016.
https ://digitalcommons.wcl.american.edu/facsch_lawrev/1100

[2610] *Katz c. États-Unis*, 389 U.S. 347, 1967. https ://supreme.justia.com/cases/federal/us/389/347/

[2611] A. A. Reed, "*Fourth Amendment first principles*", Harvard Law Review, vol.107, 1994. p.757-819.

[2612] *Katz c. Etats-Unis*, 389 U.S. 347 1967, Oyez. www.oyez.org/cases/1967/35. Consulté le 29 septembre 2024.

[2613] D. J. Solove, *Understanding Privacy*, Harvard University Press, 2008. https ://papers.ssrn.com/sol3/papers.cfm?abstract_id=1127888

[2614] *The USA Patriot Act : Preserving Life and Liberty*
https ://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf

[2615] *Public Law 107–56, OCT. 26, 2001*, Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (usa patriot act) act of 2001
https ://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf

[2616] *Katz c. États-Unis,* 389 US 347, 1967. https://www.oyez.org/cases/1967/35

et les nouvelles menaces à la sécurité nationale a apporté de nombreuses exceptions et limitations à son application.

915. Améliorer l'efficacité des enquêtes sur la cybercriminalité en Europe. La même année, le Conseil de l'Europe a adopté la Convention de Budapest[2617] sur la cybercriminalité. Elle vise à rendre les enquêtes sur la cybercriminalité plus efficaces en facilitant la coopération entre les États membres, notamment par l'utilisation de logiciels avancés pour surveiller ou prévenir le terrorisme. Un deuxième protocole, amélioré en termes d'échange rapide d'informations et de ressources, a été signé en 2023.[2618]

En 2016, le Royaume-Uni a adopté l'Investigatory Powers Act (IPA)[2619], une loi controversée[2620] qui permet la surveillance électronique et l'accès des autorités aux données privées des citoyens. Bien que les agences gouvernementales puissent avoir accès à ces données ou exiger un décryptage dans de mauvaises conditions législatives, seulement avec un mandat approuvé par les autorités compétentes, il existe de nombreuses critiques concernant la compromission de la sécurité des communications et la violation des droits à la vie privée.[2621] La dernière mise à jour de l'IAP a été effectuée en 2024 en vertu de la loi sur le pouvoir d'enquête (amendement) et a amélioré la capacité des autorités à accéder à des informations privées.[2622]

En 2017, l'Italie réglemente le[2623] terme « *captatore informatico* » par la loi 103 en tant que technique d'enquête qui permet aux autorités d'accéder aux appareils des suspects et de les surveiller, mais sous certaines conditions strictement stipulées dans la loi.[2624] Cette capture

---

[2617] *Convention sur la cybercriminalité Budapest*, Conseil de l'Europe, 23. nov 2001. https ://rm.coe.int/1680081561

[2618] *Deuxième Protocole additionnel à la Convention sur la cybercriminalité, relatif au renforcement de la coopération et à la divulgation de preuves électroniques* https ://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A22023A0228%2801%29

[2619] *Loi sur les pouvoirs d'enquête*, 2016. https ://www.legislation.gov.uk/ukpga/2016/25/contents[2620] E. MacAskill, O. Bowcott, "*Investigatory Powers Act : snooper's charter bill becomes law*", The Guardian, 2016.

[2620] E. MacAskill, O. Bowcott, "*Investigatory Powers Act : snooper's charter bill becomes law*", The Guardian, 2016.

[2621] Y. Akdeniz, N. Taylor, C. Walker, *Regulation of Investigatory Powers Act 2000* (1) : *BigBrother.gov.uk : State surveillance in the age of information and rights*, Criminal law review, 2001, p.73-90. https ://www.researchgate.net/publication/288154920_Regulation_of_Investigatory_Powers_Act_2000_1_BigBrothergovuk_State_surveillance_in_the_age_of_information_and_rights

[2622] J. Dawson, *Investigatory Powers (Amendment) Bill [HL]*, House of Commons, 2024. https ://commonslibrary.parliament.uk/research-briefings/cbp-9960/

[2623] *Legge del 23/06/2017 n. 103* - https ://def.finanze.it/DocTribFrontend/getAttoNormativoDetail.do?ACTION=getArticolo&id={59B004DE-3B39-42F5-B695-196E7CAD5896}&codiceOrdinamento=2

[2624] *Codice di Procedura penale*, Capo IV. Intercettazioni di conversazioni o comunicazioni https ://www.altalex.com/documents/news/2014/03/26/mezzi-di-ricerca-della-prova

informatique est en fait un virus de cheval de Troie et son utilisation est autorisée pour lutter contre la criminalité dans des situations soigneusement réglementées[2625].

En Roumanie, l'interception et l'enregistrement des communications électroniques de toute forme, l'extraction d'informations à partir de divers dispositifs, sont régis par le Code de procédure pénale - Loi n° 135/2010[2626] (articles 138 à 147). La loi no 51/1991[2627] autorise le Service roumain de renseignement, le Service de renseignement extérieur, le Service de protection et de garde à effectuer les actions susmentionnées, avec l'autorisation du juge des droits et libertés, conformément à l'article 152 du nouveau Code de procédure pénale[2628].

Soulignant l'importance de la protection des droits fondamentaux dans un procès pénal, en février 2016[2629], dans le cadre de la décision n° 51, la Cour constitutionnelle de Roumanie a procédé à une analyse du caractère constitutionnel des dispositions du paragraphe 1 de l'article 142[2630] du Code de procédure pénale. Analysant les conditions dans lesquelles les interceptions peuvent être effectuées, la Cour décide que les dispositions contestées – l'ambiguïté de l'expression « autres organes spécialisés de l'État » –[2631] sont inconstitutionnelles, violent le droit au respect de la vie privée garanti par l'article 28[2632] de la Constitution roumaine, et oblige le législateur à revoir et à améliorer la réglementation.[2633]

916. Utilisation des interceptions dans les procédures pénales. Une autre décision relative aux interceptions effectuées et à leur utilisation dans le cadre de procédures pénales est la décision no 55/2020[2634] de la Cour constitutionnelle de Roumanie (CCR), à l'exception de

---

[2625] T. Bene, *Lintecettazione di comunicazioni*, Cacucci Editore, Bari, 2018. https ://iris.unipa.it/retrieve/handle/10447/295510/583604/9788866117315%20Estratto%20%27Lintercettazione%20di%20comunicazioni%27%20-%20Maggio.pdf

[2626] *Loi no 135/2010 du 1er juillet 2010 portant sur le Code de procédure pénale* https ://anes.gov.ro/wp-content/uploads/2018/07/l-135-2010.pdf

[2627] *Loi n° 51/1991 sur la sécurité nationale de la Roumanie* https ://lege5.ro/Gratuit/gm4teobtg4/legea-nr-51-1991-privind-securitatea-nationala-a-romaniei?d=2024-09-29

[2628] *Art. 152 Le nouveau Code de procédure pénale* Obtention de données générées ou traitées par les fournisseurs de réseaux publics de communications électroniques méthodes spéciales de surveillance ou de recherche https ://legeaz.net/noul-cod-procedura-penala-ncpp/art-152

[2629] Décision *n° 51 du 16 février 2016* sur l'exception d'inconstitutionnalité des dispositions de l'article 142, paragraphe 1, du Code de procédure pénale https ://legislatie.just.ro/Public/DetaliiDocumentAfis/176576

[2630] *Code de Procédure Pénale du 1er juillet 2010 (loi no 135/2010), article 142* https ://legislatie.just.ro/Public/DetaliiDocumentAfis/269774

[2631] Conformément au paragraphe 1 de *l'article 142 du Code de procédure pénale*, les mandats de contrôle technique peuvent être ordonnés par : les procureurs, les organes d'enquête criminelle, les agents spécialisés de la police et „d'autres organes spécialisés de l'État"!

[2632] *Constitution de la Roumanie, Art. 28 – Le secret de la correspondance.* https ://www.constitutia.ro/art-28-secretul-corespondentei.htm

[2633] Décision *n° 64 du 2 octobre 2023* concernant la délivrance d'une décision préliminaire sur la mise en place des infrastructures nécessaires, conformément à l'article 142 du Code de procédure pénale, respectivement à la procédure prévue à l'article 148, paragraphe 3, du Code de procédure pénale de https ://legislatie.just.ro/Public/DetaliiDocumentAfis/276458

[2634] Décision *n° 55 du 4 février 2020* sur l'exception d'inconstitutionnalité des dispositions de l'article 139, paragraphe 3, la thèse finale du Code de procédure pénale et de l'article 11, paragraphe 1, lettre d), de la loi n° 51/1991 sur la sécurité nationale de la Roumanie https ://www.ccr.ro/wp-content/uploads/2020/06/Decizie_55_2020-1.pdf

l'inconstitutionnalité du paragraphe 3, dernière phrase, de l'article 139[2635] du Code de procédure pénale et de l'article 11, paragraphe 1, lettre d de la loi no 51/1991[2636]. Gardant le raisonnement juridique des arrêts précédents, le CCR décide que les interceptions sont une mesure intrusive[2637] dans la vie privée et doivent être effectuées dans des circonstances exceptionnelles, uniquement avec l'approbation d'un juge et en même temps il doit y avoir une possibilité légale de procéder à un contrôle *post*-approbation. Dans la même décision, il est indiqué que la méthode de formulation du paragraphe 3 de l'article 139, dernière phrase du Code de procédure pénale, n'est pas conforme[2638] aux " exigences de clarté " et de " prévisibilité ", raison pour laquelle il admet l'exception d'inconstitutionnalité. Dans la mesure où les services de renseignement pouvaient faire des enregistrements de quelque nature que ce soit, sans que la légalité de ce moyen de preuve soit contestée, la Cour a jugé que des actes d'intrusion dans la vie privée de personnes étaient commis. Dans le même contexte, la Cour note que l'utilisation dans une procédure pénale des résultats obtenus à la suite de « l'activité spécifique de collecte d'informations qui implique », y compris une ingérence dans la vie privée et « l'attribution de la qualité de la preuve » des dossiers ne confère pas de garanties suffisantes quant à la légalité et à la loyauté de l'administration de ces preuves.

Compte tenu des dispositions légales, l'article 138, paragraphe 1, lettre a, du Code de procédure pénale autorise apparemment l'interception de toutes les communications effectuées par tout moyen de communication, y compris WhatsApp, signal, applications de messagerie télégramme, etc. Cependant, comme ils utilisent un cryptage de bout en bout, les chevaux de Troie malveillants sont nécessaires pour intercepter ces appels, et l'installation d'un tel programme n'est pas autorisée.[2639] Par conséquent, en raison de ce vide législatif, les

---

[2635] « *Les enregistrements prévus au présent chapitre par les parties ou d'autres personnes constituent des moyens de preuve pour leurs propres conversations ou communications avec des tiers. Tout autre enregistrement peut constituer un moyen de preuve s'il n'est pas interdit par la loi*. »

[2636] « (1) *Les informations dans le domaine de la sécurité nationale peuvent être communiquées : […] d) aux organes de poursuite pénale, lorsque les informations se rapportent à la commission d'un délit.* »

[2637] Paragraphe 36 : « *La Cour a donc conclu que, dans le cas de mesures de surveillance technique, qui constituent une ingérence dans la vie privée des personnes soumises à ces mesures, il doit y avoir un examen postérieur à l'approbation et à l'exécution de la surveillance technique. Ainsi, la personne faisant l'objet des mesures de surveillance technique doit être en mesure d'exercer ce contrôle afin de vérifier le respect des conditions prévues par la loi pour la prise de la mesure, ainsi que les modalités d'exécution du mandat de contrôle technique, procédure régie par les dispositions de l'article 142-144 du Code de procédure pénale*. »

[2638] Paragraphe 55 : « *Ainsi, la Cour constate que la réglementation de la possibilité de conférer des éléments de preuve sur des documents résultant d'activités spécifiques à la collecte d'informations qui impliquent une restriction de l'exercice des droits de l'homme ou des libertés fondamentales ne s'accompagne pas d'un ensemble de règles qui permettraient de les contester dans des conditions légales efficacité. En réglementant simplement la possibilité de déposer de tels documents, sans créer le cadre approprié pour contester leur légalité, le législateur a légiféré sans se conformer aux exigences de clarté et de prévisibilité*. »

[2639] *Code de procédure pénale*, titre IV : preuves, moyens de preuve et procédure de présentation de la preuve, chapitre IV - méthodes spéciales de surveillance ou d'enquête, article 138 https ://legislatie.just.ro/Public/DetaliiDocumentAfis/269774

communications acheminées par l'intermédiaire d'applications de messagerie ne peuvent pas être interceptées à l'heure actuelle.

A. France : le refus de remettre la clé de décryptage est pénalement sanctionné

917. En France, face à une situation sécuritaire tendue, la Cour de cassation a statué en 2022, dans le cadre de[2640] l'arrêt n° 21-83146, que le refus de remettre aux enquêteurs la clé de décryptage nécessaire à l'enquête sur un délit est punissable par la loi pénale.[2641] La loi principale sur l'accès aux données cryptées reste la loi n°-731 du 3 juin 2016[2642], également appelée « Loi sur la lutte contre le terrorisme et le crime organisé ». Il donne aux autorités étatiques la possibilité de demander le décryptage des données aux opérateurs de services en cas d'enquête, le refus étant sévèrement sanctionné, y compris l'emprisonnement. Actuellement, en France, l'utilisation d'un logiciel de surveillance aux fins d'interception, d'enregistrement et d'accès à des données informatiques n'est légale en vertu de l'article 706-102-1 du Code de procédure pénale que dans des cas graves, tels que la lutte contre le terrorisme ou la criminalité organisée et uniquement sur mandat délivré par le juge.[2643]

918. Les autorités françaises ont intercepté les communications cryptées de plus de 6000 personnes. Le démantèlement du réseau crypté EncroChat[2644] en 2020, grâce à un effort conjoint d'Europol et d'Eurojust, a été un processus historique qui illustre la manière dont les autorités peuvent utiliser la technologie pour lutter contre la criminalité organisée. Il s'agissait d'un réseau informatique crypté utilisé par des criminels pour des activités illégales telles que le trafic de drogue, les tentatives de meurtre, les actes de torture[2645]. Les autorités françaises[2646] ont réussi à intercepter ces communications, bien que cryptées, à l'aide de chevaux de Troie

---

[2640] Ass. plén., *07-11-2022, n° 21-83,146,* Cassation https ://www.lexbase.fr/jurisprudence/89632935-ass-plen-07112022-n-2183146-cassation

[2641] P. Le Maigat, *Du bon usage de la cryptologie en droit pénal,* Actu-Juridique.fr, 2022. https ://www.actu-juridique.fr/droit-penal/du-bon-usage-de-la-cryptologie-en-droit-penal/

[2642] *Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale*, https ://www.legifrance.gouv.fr/jorf/id/JORFSCTA000032627246

[2643] *Code de procédure pénale* , Chapitre II : Procédure (articles 706-80 à 706-106), Section 6 : Des autres techniques spéciales d'enquête (articles706-95-11 à 706-102-5), paragraphe 4 : de la captation des données informatiques (articles 706-102-1 à 706-102-5)

[2644] Affaire *C-670/22* https ://eucrim.eu/documentation/ecj-eu-criminal-law-cases-overview/case-c-67022/

[2645] EncroChat est un exemple emblématique de réseau crypté utilisé à des fins criminelles. Il était principalement utilisé par des téléphones mobiles spécialement conçus pour garantir la confidentialité absolue des messages. En 2020, une opération conjointe des polices française et néerlandaise, coordonnée par Europol et Eurojust, a réussi à infiltrer le système EncroChat, ce qui a conduit à des milliers d'arrestations et à des saisies massives de drogues, d'armes et d'argent.

[2646] En France, l'opération a été baptisée "*Emma 95*", avec des ressources considérables et un réel succès. L'opération a été autorisée par le tribunal de Lille en vertu des articles 706-102-1 du Code de procédure pénale. https ://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organized-crime-groups-across-europe

malware, jusqu'à présent plus de 6000 personnes ont été arrêtées dans plusieurs pays, avec des peines de plus de 7000 ans de prison.[2647]

919. Controverses concernant la confidentialité de la coopération entre États. Actuellement, dans des pays comme la France, l'Allemagne ou le Royaume-Uni, ces arrestations sont contestées, les accusés invoquant des violations du droit à la vie privée ainsi que des règles de collaboration entre les états en matière de partage et de divulgation des preuves.[2648] La principale question qui s'est posée était, comment la France a-t-elle réussi à intercepter légalement une telle quantité de communications, de tous les utilisateurs d'EncroChat, y compris ceux qui n'avaient pas d'intention criminelle ![2649] L'affaire susmentionnée a été portée devant la Cour européenne des droits de l'homme (CEDH) et la Cour de justice de l'Union Européenne (CJUE). Dans le cas des demandes nos 44715/20 et 47930/21, la CEDH estime que l'utilisation des données obtenues à partir des communications d'EncroChat viole le droit à la vie privée, soulignant la nécessité d'assurer la protection des données personnelles conformément aux normes européennes.[2650] La CJUE examine la recevabilité des éléments de preuve obtenus par de telles interceptions dans les États membres de l'UE[2651],, l'avis du procureur général étant que, si la législation nationale de l'État dans lequel les éléments de preuve sont recueillis le permet, les autres États ne devraient pas réévaluer[2652] la légalité de la collecte des éléments de preuve.

a). Backdoors, une solution de décryptage controversée

920. Risques liés à la cybersécurité. Une autre solution pour intercepter les conversations cryptées est l'introduction de portes dérobées[2653]. Les experts avertissent que ces mécanismes pourraient affaiblir les systèmes de cryptage pour tous les utilisateurs, les exposant ainsi à des

---

[2647] *Le démantèlement des communications EncroChat criminelles cryptées entraîne plus de 6 500 arrestations et près de 900 millions d'euros saisis*, Europol, 2023. en https ://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized#:~:text=Dismantling%20encrypted%20criminal%20EncroChat%20communications,EUR%20900%20million%20seized%20%7C%20Europol

[2648] *Le chemin d'EncroChat vers les plus hautes juridictions européennes* European parliament, 2022. https ://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2022)739268

[2649] *Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée,* Bureau des affaires criminelles, 2020. https ://www.gendarmerie.interieur.gouv.fr/gendinfo/enquetes/2020/retour-sur-l-affaire-encrochat

[2650] Requêtes nos 44715/20 et 47930/21, *A.L. contre la France* et *E.J. contre la France*

[2651]L'affaire *C-670/22*, https ://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2024/05/c-670.22.pdf

[2652] *Opinion de l'avocat général ćapeta, rendue le 26 octobre 2023, affaire C670/22,* InfoCuria, 2023. -https ://curia.europa.eu/juris/document/document.jsf?text=&docid=279144&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=203503

[2653] *Topic: Backdoor*, Vectra. https ://www.vectra.ai/topics/backdoor

risques de cybersécurité[2654]. La mise en place de portes dérobées, qui permettraient aux autorités d'accéder aux communications cryptées, pourrait compromettre la sécurité globale des systèmes, les rendant vulnérables aux cyberattaques ou autres abus.[2655] La méthode est également critiquée par la CEDH, qui au début de 2024, dans l'affaire Podchasov contre Russie (présentée ci-dessus) confirme catégoriquement toute attaque contre le cryptage (y compris l'utilisation de « portes noires »), viole le droit à la vie privée de tous les utilisateurs, conformément à l'article 8 de la Convention européenne des droits de l'homme.[2656]

B. Allemagne, les conversations peuvent être décryptées en cas de délits très graves

921. Mesures de surveillance des citoyens. Une affaire fondamentale concernant l'équilibre entre la sécurité nationale et le droit à la vie privée est Klass et d'autres contre l'Allemagne[2657]. Les requérants font valoir que le droit allemand permet aux autorités d'intercepter des communications sans prévoir de garanties suffisantes contre les abus, ce qui constituerait une violation de leur droit au respect de la vie privée, à savoir l'article 8 de la CEDH.[2658] Le 6 septembre 1980, la CEDH a rendu un arrêt établissant que l'interception de communications n'est pas incompatible avec l'article 8 de la Convention européenne des droits de l'homme, mais a souligné que ces mesures doivent être justifiées dans le cadre de la protection de la sécurité nationale et de la lutte contre la criminalité.[2659]

Avec une histoire marquée par des régimes oppressifs[2660], l'Allemagne est extrêmement sensible à l'idée de surveiller les citoyens, confrontée au fil des ans à un véritable dilemme d'assurer la sécurité nationale tout en respectant le droit à la vie privée.[2661] Le Code de procédure pénale allemand réglemente actuellement l'utilisation de « *Bundestrojaner* » (un

---

[2654] B. Schneier, *Data and Goliath : The Hidden Battles to Collect Your Data and Control Your World,* W.W. Norton & Company, 2015.
[2655] A. Harold et al., *The Risks of Key Recovery, Key Escrow and Trusted Third-Party Encryption*, MIT Press, 1997 .
[2656] S.L. Perez, *The European Court of Human Rights Concludes Encryption Backdoor Mandates Violate the Right to Private Life of All Users Online,* center for democracy and technology, 2024. https ://cdt.org/insights/the-european-court-of-human-rights-concludes-encryption-backdoor-mandates-violate-the-right-to-private-life-of-all-users-online/
[2657] *Affaire Klass et autres c. Allemagne*, requête no. 5029/71. https ://hudoc.echr.coe.int/eng#{"itemid":["001-57510"]}
[2658] H. O'Boyle, C. Warbick , *Law of the European Convention on Human Rights*,Oxford University Press, 2023.
[2659] International court decisions, *Klass and ors v Federal Republic of Germany, Judgment, Merits, App no 5029/71 (A/28), (1979-80) 2 EHRR 214, IHRL 19 (ECHR 1978),* European Court of Human Rights [ECHR*],* Oxford reports and International Law, 1978. https://opil.ouplaw.com/display/10.1093/law:ihrl/19echr78.case.1/law-ihrl-19echr78
[2660] S. Roller, *The Stasi : The Most Terrifying Secret Police in History?,* Hystory Hit, 2021. https ://www.historyhit.com/the-stasi-the-most-terrifying-secret-police-in-history/
[2661] A. Adams, S. Hosell, K. Murata, Kiyoshi, *Following Snowden, German uncertainty about monitoring,* Journal of information, Communication and Ethics in Society, vol.15, 2017. p.232-246.

cheval de Troie malveillant) par les autorités allemandes pour prévenir les délits graves (article 100a). Des règlements spécifiques pour l'utilisation licite des chevaux de Troie sont ratifiés à l'article 100b.[2662] La légalisation des logiciels de chevaux de Troie en 2017, permettant aux autorités allemandes d'accéder aux communications cryptées à partir d'applications comme WhatsApp ou Telegram, a bien sûr fait l'objet de nombreuses critiques et controverses sur la vie privée et les violations de la vie privée.[2663] En 2008, la Cour constitutionnelle fédérale d'Allemagne a imposé des restrictions strictes à l'utilisation de ce cheval de Troie.[2664] Suite à la décision du Bundesverfassungsgericht, 1 BvR 370/07[2665] du 27 février 2008, l'utilisation du « *Bundestrojaner* » n'est admise qu'en cas d'infractions très graves, sur la base du principe de proportionnalité et l'approbation d'un juge est obligatoire.

Conclusions du chapitre 2

Ce chapitre examine le statut juridique du cryptage en tant qu'outil technique situé à la croisée de la protection de la vie privée et de la prévention des infractions graves. Il en ressort un cadre dans lequel les législations et les documents européens ne traitent pas le cryptage comme un phénomène marginal, mais l'intègrent expressément dans la politique de protection des communications électroniques. Les références au règlement ePrivacy, à la résolution du Conseil de l'Europe sur la « sécurité par cryptage et sécurité malgré le cryptage » et à l'inclusion du concept de cryptographie post-quantique dans le droit français confirment le choix de garantir la confidentialité des communications en tant qu'exigence juridique positive, et non seulement en tant que pratique technologique tolérée.

Dans le même temps, le chapitre souligne la tension structurelle entre le cryptage robuste et les intérêts légitimes de l'enquête pénale. L'analyse du conflit Apple-FBI, du blocage de Telegram en Russie, des procédures visant le fondateur de l'application et des préoccupations liées à l'utilisation du cryptage à des fins illicites montre que la protection de la vie privée ne peut être dissociée de la question de l'accès des autorités aux preuves. La référence à la jurisprudence de la CEDH, qui admet la possibilité d'obtenir des informations sans

[2662] *Code allemand de procédure pénale (Strafprozeßordnung–StPO*). https ://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

[2663] C.F. Azubuike, *Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks*, Nnamdi Azikiwe Journal of Political Science, vol.9., 2023. p.101-114.

[2664] B. Schafer, *The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems — a case report on BVerfG, NJW 2008, 822*. SCRIPT-ed, 2009. https ://www.academia.edu/84795991/_The_German_Constitutional_Court_on_the_Right_in_Confidentiality_and_Integrity_of_Information_Technology_Systems_a_case_report_on_BVerfG_NJW_2008_822

[2665] BVerfG, *Order of the First Senate of 27 February 2008-1 BvR 370/07, paras.1-333*, https ://www.bverfg.de/e/rs20080227_1bvr037007en.html

compromettre de manière généralisée le cryptage, soutient l'idée que les outils d'enquête doivent être calibrés de manière ponctuelle, sans annuler les garanties techniques destinées au grand public.

Les réglementations relatives à l'interception des communications via des applications telles que WhatsApp, Telegram ou Signal mettent en évidence la diversité des solutions nationales. Le droit français incrimine le refus de fournir la clé de décryptage, conférant ainsi au destinataire d'une telle obligation un rôle procédural actif. Le débat sur les *backdoors* révèle le risque que les solutions techniques généralisées d'accès compromettent la protection de tous les utilisateurs. Le modèle allemand, qui autorise le décryptage dans le cas de certaines infractions particulièrement graves, illustre une approche conditionnelle, limitée à un seuil élevé de gravité.

Le chapitre établit ainsi les lignes d'un équilibre juridique délicat : le cryptage est reconnu comme un outil légitime de protection de la vie privée dans l'environnement numérique mondialisé, et toute limitation acceptée au profit de l'enquête pénale doit rester strictement nécessaire, proportionnée, individualisée et éviter les solutions qui rendraient la confidentialité des communications systématiquement vulnérable.

Conclusions Titre 1

Le titre I résume une évolution claire : les algorithmes deviennent un élément déterminant dans la définition des risques et la configuration de nouvelles formes d'illicéité, et le droit pénal est appelé à répondre à ce nouveau défi. Il ne peut y répondre par des formules générales ou par des extensions vagues des incriminations existantes. Une réglementation est nécessaire pour identifier clairement le rôle des personnes impliquées dans la conception, la mise en œuvre et l'utilisation des systèmes algorithmiques, pour distinguer entre utilisation licite et utilisation détournée et pour garantir que la responsabilité reste, en dernier ressort, localisée auprès de sujets de droit déterminés. Toute tentative de transférer la responsabilité à une « entité technique autonome » risque de relativiser les principes de légalité et de culpabilité et d'affaiblir la fonction préventive de la norme.

Dans le même temps, la protection de la vie privée ne peut être sacrifiée en bloc sur l'autel de l'efficacité technologique ou de la facilitation des poursuites pénales. L'utilisation d'algorithmes à des fins de surveillance, d'analyse comportementale ou d'enquête doit être soumise à des conditions strictes de nécessité, de proportionnalité et de contrôle juridictionnel effectif, sans dérogations générales qui autoriseraient un accès illimité aux données,

l'identification systématique des utilisateurs ou la neutralisation du cryptage. La solution n'est pas de renoncer aux garanties, mais de les adapter aux nouvelles formes d'atteinte : définition précise des faits, des moyens, des espaces numériques protégés et des conditions dans lesquelles l'intervention pénale est justifiée.

Dans un ordre juridique modelé par des algorithmes, l'efficacité du droit pénal dépend de sa capacité à intégrer les nouveaux risques sans renoncer à ses exigences structurantes : prévisibilité, personnalisation de la responsabilité et protection effective de la vie privée en tant que droit fondamental, et non en tant que variable ajustable en fonction des performances technologiques.

TITRE II
INTRUSION DE L'ÉTAT DANS LA VIE PRIVÉE. SYNCHRONISATION DU DROIT PÉNAL AVEC L'ÉVOLUTION TECHNOLOGIQUE

922. La notion de vie privée par rapport à l'autorité publique. Dans l'article publié en 1941 sous le nom de « les origines de l'État total »[2666], le savant allemand Erich Kahler[2667] définit l'État total : « la caractéristique essentielle de l'état totalitaire est qu'il étend son contrôle sur toute la vie du citoyen et ne reconnaît aucune sphère de la vie privée comme étant exclue de la préoccupation de l'état ou au-delà de la préoccupation de l'état. » Dans cet article, Erich Kahler résume historiquement l'évolution de la notion de vie privée par rapport à l'autorité de l'État et à la nécessité de l'intrusion de l'État. De l'Antiquité au moyen âge, dans l'état théocratique[2668], le rôle des prêtres[2669] était de surveiller comment les individus respectaient les coutumes anciennes liées au culte des dieux. Cette forme primitive d'intrusion dans la vie privée n'a pas la connotation moderne que Samuel Warren a définie en 1890[2670].

Kahler soutient qu'à cette époque, « la vie individuelle n'avait pas encore évolué » et que les prêtres « manquaient des moyens de contrôle qu'un État moderne détient ». Même le pouvoir oppressif des gardes[2671] payés par les tyrans de la Grèce antique n'a pas directement influencé la vie privée[2672]. Le moyen âge a été caractérisé par la précarité du pouvoir étatique[2673] et la véhémence du défi sociétal[2674]. Dans ce contexte, l'État n'était pas en mesure de commettre des actes d'intrusion dans la vie privée des membres de la communauté. Les raisons initiales de

---

[2666] E. Kahler, "*The Origins of the Total State"*, The German Quarterly, vol.14, no.2, 1941. p.73-80

[2667] E. von Kahler (14 octobre 1885 – 28 juin 1970) est né à Prague dans une famille juive et est l'une des principales figures culturelles du milieu du XXe siècle, étant ami avec Albert Einstein, Thomas Mann et Hermann Broch. Il perd la citoyenneté allemande en 1933 à la suite de la montée du régime nazi et émigre aux États-Unis où il devient professeur à l'Université de Princeton. Il était l'un des partisans de la théorie de la création d'un gouvernement mondial et luttait contre la guerre et l'armement nucléaire. Le contexte dans lequel il a écrit l'article est sensible, il n'avait pas encore obtenu la citoyenneté américaine, et l'humanité était au milieu de la première Guerre mondiale.

[2668] M. Potz, "*Theocracies as Political Systems*", Political Science of Religion, 2019. https ://link.springer.com/chapter/10.1007/978-3-030-20169-2_4

[2669] R. M. Glassman, "*From the Theocratic State to the Kingly-Bureaucratic State*", Springer, 2017. p.367-386 https ://link.springer.com/chapter/10.1007/978-3-319-51695-0_41

[2670] S.D. Warren, L.D. Brandeis, *The Right to Privacy,* Harvard Law Review, vol.4, no.5, 1890. p.193-220.

[2671] G.L. Cawkwell, *Early Greek tyranny and the people*, The Classical Quarterly, vol.45(1), 1995. p.73-86. doi :10.1017/S0009838800041707

[2672] „*The secret police was a creation of the Greek tyrants, but its activity was confined within the limits of the actual safety of the regime*", p.73, E. Kahler, op. cit.

[2673] T. Bisson, *Cultures of Power : Lordship, status, and process in Twentieth-Century Europe*, Law and History Review, vol.16, 1995. p. 175

[2674] B. Aguilera-Barchet, *From Kings to Monarchs: The Resurgence of Public Power in Late Medieval Europe*, in *A History of Western Public Law*, Springer, 2015. p.177-210. https ://doi.org/10.1007/978-3-319-11803-1_8

l'exercice du contrôle de masse[2675] étaient directement liées aux luttes de pouvoir et aux conflits politiques entre dynasties. Lorsque l'armée féodale a été payée[2676] et que les dépenses des cours royales ont été exagérées, [2677]un système d'organisation mercantiliste de[2678] l'activité économique a été mis en place.

[2675] R. B. Weingast, „*Adam Smith's Industrial Organization of Religion : Explaining the Medieval Church's Monopoly and Its Breakdown in the Reformation",* Economic History eJournal, 2015. https ://doi.org/10.2139/ssrn.2675590

[2676] J. Burgers, M. Damen. „*Feudal Obligation or Paid Service? The Recruitment of Princely Armies in the Late Medieval Low Countries*", The English Historical Review, 2018. https ://academic.oup.com/ehr/article-abstract/133/563/777/5043263?redirectedFrom=fulltext&login=false

[2677] C. Ingrao, "*Jeroen Duindam. Vienna and Versailles : The Courts of Europe's Dynastic Rivals, 1550-1780*, Cambridge University Press, 2003. p.349, illus., tables. Austrian History Yearbook. https ://www.cambridge.org/core/journals/austrian-history-yearbook/article/abs/jeroen-duindam-vienna-and-versailles-the-courts-of-europes-dynastic-rivals-15501780-cambridge-cambridge-university-press-2003-pp-349-illus-tables/38AAF61C6AAA95AA53F6118812AC318C Dans cet article, il est indiqué que le maintien des cours royales de Versailles et de Vienne se classait au troisième rang des dépenses de l'État, d'abord de la guerre

[2678] R. Ekelund, R. Tollison, *Politicized Economies : Monarchy, Monopoly and Mercantilism*, Choice, 1997. https ://doi.org/10.5860/choice.35-1006.

Chapitre 1
INTRUSION GOUVERNEMENTALE: DU MANDAT DE PERQUISITION À L'INTERCEPTION DES CONVERSATIONS

Section 1. ORIGINE DE L'ÉTAT TOTAL, DE LA VISION THOMISTE À LA SURVEILLANCE GOUVERNEMENTALE

La pression de l'État pour couvrir les dépenses a conduit à la vente d'une charge publique privilégiée[2679] ou à la demande d'aide de financiers, également appelés « intermédiaires commerciaux extraordinaires », qui dévaluent souvent les biens publics au profit de la monarchie[2680]. D'autre part, l'Angleterre a choisi l'option de l'expansion coloniale[2681] afin d'augmenter ses ressources financières.

§1. LA NÉCESSITÉ D'INTRUSION: DE LA PHILOSOPHIE AU DROIT

923. Formes historiques de contrôle et de surveillance de la société. Dans ce contexte historique, Erich Kahler soutient que Frédéric-Guillaume Ier[2682] est le père de *l'état total* dans lequel il y avait une forme de contrôle et de surveillance de la société, ce qui est assez similaire à celui de l'époque moderne. L'armée est devenue le point central du pouvoir d'État en Prusse[2683] et le modèle de discipline, de rigueur, d'organisation et de contrôle est passé dans la société civile. Dans le but principal de consolider la monarchie, l'intrusion dans la vie privée de l'individu est devenue un acte de normalité : « des inspections inattendues et des espions ont

[2679] J. Rogister, *Venality : The Sale of Offices in Eighteent-Century France,* American Journal of Legal History, vol.42, issue3, 1998, p.295–296 – « dans l'ancien régime, la France, presque tous les postes de responsabilité publique devaient être liés ou hérités. Plutôt que de taxer directement leurs sujets les plus riches, les rois français préféraient leur vendre des fonctions publiques privilégiées, que d'autres paiements leur permettaient de vendre ou de léguer à volonté. Au XVIIIe siècle, il y avait 70,000 bureaux vénaux, rassemblant la magistrature de l'entité, la plupart de la profession juridique, des officiers de l'armée et un large éventail d'autres professions »

[2680] J. Felix, *Profit, embezzlement, restitution. The role of the traitants in the Nine Years' War and Chamillart's tax on financial benefits*, Revue Historique, 2015. p.831-874
https ://shs.cairn.info/revue-historique-2015-4-page-831?lang=fr&tab=texte-integral

[2681] F. West, "*The Colonial History of the Norman Conquest.*" History, vol.84, 1999. p.219-236

[2682] Friedrich Wilhelm Ier (1688-1740) était un membre de la dynastie Hohenzollern et est considéré par les historiens comme ayant modernisé l'État prussien. Les réformes militaires et économiques ont transformé la Prusse en une véritable puissance européenne, l'un des éléments clés étant la collecte des impôts auprès de la population. Dans le même temps, des soldats ont été recrutés dans toute l'Europe, l'une des conditions d'accès au service militaire étant de plus de 1.88.

[2683] C. Winkel, *The King and His Army: A New Perspective on the Military in 18th Century Brandenburg-Prussia*, International Journal of Military History and Historiography, 2019.

vérifié la fiabilité des fonctionnaires. Un fonctionnaire coupable de faux rapports, de retards ou de corruption a été publiquement frappé au visage et dispersé à vie[2684]. »

Fondamentalement, le moment où l'on peut parler d'intrusion de l'État dans la vie privée de l'individu, au sens moderne, juridique, c'est le XVIIIe siècle[2685]. La Révolution française (1789-1799) fut l'aboutissement de la redéfinition du concept et des règles de cette intrusion[2686]. Avant cette époque, pendant près de deux siècles (XVII-XVIII), la société tentait de séparer l'espoir public de la sphère privée. Je comprends que sans cette séparation juridique entre *le public* et *le privé*, il est inapproprié d'analyser une intrusion de l'État dans la vie privée.

924. La délimitation des notions de public et privé. La plupart des historiens de l'ancien régime[2687], qui cherchaient des explications supplémentaires pour certains phénomènes sociaux ou juridiques contemporains, ont émis des théories assez larges sur les notions de c *public* et *privé.*

Parmi les principaux théoriciens qui ont analysé ce sujet, on trouve les auteurs suivants : Jürgen Habermas[2688], Reinhart Koselleck[2689], Philippe Ariès et [2690]Roger Chartier[2691].

[2684] E. Kahler, op. cit., p.76

[2685] E. Longfellow, "*Public, Private, and the Household in Early Seventeenth-Century England",* Journal of British Studies, vol.45, 2006. p.313 - 334

[2686] G. S. Wood, „*The Great Demarcation Between Public and Private"*, Power and Liberty, 2021. pf.149 - 174 https://academic.oup.com/book/39956/chapter-abstract/340250039?redirectedFrom=fulltext&login=false

[2687] P.H.Wilson, *New Approaches under the Old Regime.* in: G. Mortimer(eds*), Early Modern Military History, 1450–1815*, Palgrave Macmillan, London, 2004. – « le terme « ancien régime » (ancien régime) a été inventé par les révolutionnaires français pour distinguer leur nouveau monde courageux des monarchies qu'ils espéraient détester. Grâce à la convention selon laquelle leur révolution a été un tournant majeur dans l'histoire du monde et la naissance de la « modernité », elle est restée une étiquette générale pour la période de 1648 à 1789' https ://link.springer.com/chapter/10.1057/9780230523982_9#citeas

[2688] Né en 1929 à Düsseldorf, il est considéré comme le plus important érudit allemand vivant, avec des théories développées dans le domaine de la philosophie sociale, de la politique ou du droit naturel ayant un fort impact sur la société. Habermas, professeur d'université exceptionnel, soutient que les lumières sont un « projet inachevé » et qu'il devrait être amélioré et adapté à la société d'aujourd'hui. Ainsi, elle est clairement délimitée par la pensée pessimiste, radicale et parfois exagérée de l'école de Francfort. Dans son ouvrage « la transformation structurelle de la sphère publique », Habermas montre que la sphère publique (Öffentlichkeit) a émergé après la Révolution française à la suite du développement du capitalisme.

[2689] Reinhart Koselleck (1923 – 2006), né en Allemagne, est considéré comme l'un des historiens les plus importants du XXe siècle au niveau international. Il a développé des recherches essentielles dans le domaine de l'histoire du droit, de l'anthropologie et de l'histoire sociale, étant l'un des fondateurs de l'histoire conceptuelle. Dans critique and Crisis (1959), Koselleck soutient que « l'État absolutiste a fait de la moralité une question de jugement strictement privé et individuel, interdisant à la conscience morale tout rôle dans la prise de décision politique ».

[2690] Philippe Ariès (1914 – 8 février 1984) est l'un des historiens français les plus importants de la période médiévale, travaillant avec Georges Duby pour écrire et coordonner un ouvrage complet, histoire de la vie privée, 5 volumes : I. de l'Empire romain à l'an mil ; I. de l'Europe féodale à la Renaissance ; III. de la Renaissance aux lumières ; IV. de la Révolution à la Grande guerre ; V. de la première Guerre mondiale à nos jours, Maison d'édition seuil, de 1985 à 1987. Il est considéré comme un pionnier dans le domaine de l'histoire des mentalités. Il a apporté une contribution significative à la définition et à l'argumentation de la distinction entre vie publique et vie privée, rendant une analyse diachronique nécessaire pour comprendre le contexte juridique de l'époque contemporaine.

[2691] Roger Chartier (né en 1945 à Lyon) est un historien influencé par les idées du mouvement culturel connu sous le nom d'École des Annales. Il est l'un des auteurs du volume III de l'histoire de la vie privée, coordonnée par Georges Duby et Philippe Ariès. Il est connu pour ses recherches sur les relations entre la société des XVIe-XVIIIe

Koselleck et Habermas partent de l'idée que *la sphère privée* n'aurait pas pu exister sans *la sphère publique*, les deux étant interdépendantes. Dans ses recherches, Koselleck propose que la théorie de *la sphère publique* soit perçue comme le résultat du conflit entre critique et absolutisme[2692], et de cette confrontation émerge la « société bourgeoise » et la Révolution française. L'absolutisme, basé sur la doctrine de *la raison d'Etat*, excluait la morale de la politique sans interférer dans la sphère privée de la conscience individuelle. Koselleck soutient également que « les mouvements internes du cœur étaient l'affaire de tous et ont donc été retirés de l'arène publique où des conflits pouvaient surgir ».[2693]

925. Changement des formes de socialisation. Philippe Ariès résume l'essor de l'État au cours du XVIIIe siècle individuel par rapport à trois facteurs essentiels : le développement de l'État, l'alphabétisation de la population et les nouvelles formes de religion[2694]. Selon les autres auteurs mentionnés ci-dessus, Ariès souligne que « toute l'histoire de la vie privée se réduit à un changement des formes de socialisation ». [2695]

La conclusion de la doctrine[2696] qui a analysé les théories des quatre auteurs qui ont essayé de comprendre la société actuelle par rapport à l'ancien régime et à la Révolution française est que la sphère publique et la sphère privée n'étaient pas en opposition réelle et les lieux de socialisation entre les individus étaient « le terrain sur lequel le privé et le public se rencontraient ». Aujourd'hui, les plateformes numériques sont le lieu principal des réseaux sociaux, le terrain de rencontre entre le public et le privé.

A. Théorie de Jürgen Habermas

926. L'œuvre de Habermas, publiée sous le titre "la transformation structurelle de la sphère publique"[2697], est considérée comme l'une des expositions les plus pertinentes de la pensée sociale du XXe siècle, et a été publiée pour la première fois en allemand en 1962[2698] sous

---

siècles en France et la littérature, la politique, l'économie et l'éducation. « Les origines culturelles de la Révolution française » (1991) est l'un des livres les plus célèbres de Chartier

[2692] R. Koselleck, *Critique and Crisis : Enlightenment and the Pathogenesis of Modern Society*, Cambridge Mass., 1988.

[2693] R. Koselleck, op. cit., p. 8

[2694] P. Ariès (coord), *Histoire de la vie privée - Tome 3, de la Renaissance aux Lumières*, Maison d'édition Seuil, 1986. pg 8,9,10

[2695] P. Ariès, op. cit., p. 9

[2696] D. Goodman, „*Public Sphere and Private Life: Toward a Synthesis of Current Historiographical Approaches to the Old Regime"*, History and Theory, vol.31, no.1, 1992. p.1-20

[2697] J. Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, Polity Press, 1989.

[2698] La version originale a été publiée sous le titre "*Strukturwandel der Öffentlichkeit. Untersuchungen zu einer Kategorie der bürgerlichen Gesellschaft "*

l'influence des idées kantiennes et marxistes[2699] qui en ont une impact remarquable[2700] dans la compréhension du développement de la sphère publique et de l'évolution ultérieure de la démocratie et des notions de séparation entre l'individu et l'état. Habermas estime que les salons français ou les cafés anglais représentaient les espaces sociaux qui ont contribué à la formation d'une sphère publique basée principalement sur l'expérience rationnelle[2701]. Lorsque ce forum de débat public rationnel[2702] dans les salons et les cafés a été transféré aux pages des journaux[2703], la version moderne de la notion d'opinion publique est apparue[2704]. Cela a permis à tous les citoyens de participer au processus de prise de décisions et, par conséquent, la démocratie est devenue fonctionnelle.

927. Interaction constante entre le public et le privé. Selon la théorie d'Habermas, la sphère publique et la sphère privée sont en interaction constante, les deux n'étant pas en opposition[2705]. Le débat et les décisions prises dans la sphère privée peuvent être directement influencés par ce qui est discuté dans la sphère publique et vice versa[2706]. Dans le même temps, le développement des systèmes économiques et politiques a facilité l'intrusion de plus en plus agressive de l'État dans la vie privée. Le sociologue allemand soutient également que « l'État et la sphère publique ne se chevauchent pas, comme on le comprendrait du langage habituel, au contraire, ils se font face en adversaires ».

Dans l'article encyclopédique « la sphère publique »[2707] publié en 1964, Habermas propose les explications suivantes : « par « la sphère publique », nous entendons d'abord un champ de notre vie sociale dans lequel peut se former quelque chose de proche de l'opinion publique. L'accès est garanti à tous les citoyens. Une partie de la sphère publique apparaît dans

---

[2699] *L. H. Elizalde et al., "The Structural Transformation of the Public Sphere*", Church, Communication and Culture, vol.8, 2023. p.325 - 329

[2700] M. Hofmann, *Influences théoriques et pratiques du bestseller académique mondial de Habermas : transformation structurelle de la sphère publique aux États-Unis*, Kybernetes, vol.50, 2020. p.955-968

[2701] P. Duelund, *Jürgen Habermas, The structural transformation of the public sphere: an inquiry into a category of bourgeois society*, International Journal of Cultural Policy, vol.16, 2010. p.26 - 28

[2702] M. Gardiner, *Wild Publics and Grotesque Symposiums: Habermas and Bakhtin on Dialogue, Everyday Life and the Public Sphere,* The Sociological Review, vol.52, 2004. p.28 - 48

[2703] « *Grâce à la diffusion de la presse et de la propagande, l'organisme public s'est étendu au-delà des limites de la bourgeoisie. L'organisme public a non seulement perdu son exclusivité sociale, mais aussi la cohérence créée par les institutions sociales bourgeoises et un niveau d'éducation relativement élevé. Les conflits, jusque-là confinés à la sphère privée, entrent désormais dans la sphère publique. Les besoins des groupes qui ne peuvent attendre satisfaction d'un marché autorégulateur tendent maintenant à réguler l'État. La sphère publique, qui doit maintenant servir de médiateur à ces exigences, devient un terrain de concurrence d'intérêts, de compétitions qui prennent la forme de conflits violents* », opinion exprimée par Habermas dans l'article la sphère publique (1964)

[2704] C. Calhoun. "*Habermas and the public sphere*." German Studies Review, vol.17, 1993. p.613

[2705] C. Calhoun, *Habermas and the Public Sphere*, The MIT Press, 1992. https ://calhoun.faculty.asu.edu/sites/default/files/publications/articles/habermas_and_the_public_sphere.pdf

[2706] *« Les lois qui sont manifestement tombées sous la « pression de la rue » peuvent difficilement être comprises comme provenant du consensus de particuliers engagés dans des discussions publiques* », Habermas, The Public Sphere

[2707] J. Habermas, et all., *The Public Sphere: An Encyclopedia Article (1964)*, Duke University Press, no.3, 1974. https://www.jstor.org/stable/487737

chaque conversation dans laquelle des individus privés se réunissent pour former un organisme public. » En 2023, 61 ans après la parution du livre « la transformation structurelle de la sphère publique », Habermas revient avec une continuation de son travail de 1962 sous le titre « une nouvelle transformation structurelle de la sphère publique et politique délibérative »[2708]. Aujourd'hui, les notions de *sphère publique*[2709] et *de sphère privée* sont analysées à travers l'émergence des réseaux sociaux et la chute des médias classiques : « un effet est l'auto-autonomisation des utilisateurs des médias ; l'autre est le prix que ces derniers paient pour être libérés de la tutelle des anciens médias tant qu'ils ne sont pas encore suffisamment efficaces dans leurs relations avec les médias. Tout comme l'impression a fait de chacun un lecteur potentiel, aujourd'hui, la numérisation transforme tout le monde en auteur potentiel. »

a). Les réseaux sociaux facilitent la surveillance gouvernementale

928. Les réseaux sociaux, facteur déterminant dans l'intrusion dans la vie privée. L'échec prophétique de Habermas à remplacer les produits et contenus journalistiques de qualité par un contenu qui ne vise qu'à maximiser les profits est reconnu dans le nouveau volume[2710]. Dans le même contexte, l'auteur allemand soutient également que les médias numériques, y compris les réseaux sociaux, doivent assumer des responsabilités supplémentaires par rapport au contenu affiché, même s'ils sont produits et édités par de simples internautes et non par des professionnels. Un autre danger noté par Habermas est que, par rapport à la nature algorithmique[2711] des médias numériques, non seulement les géants de l'informatique s'infiltrent dans la vie privée individuelle, mais créent également les conditions d'un contrôle facile par l'État. Fondamentalement, les réseaux sociaux sont considérés comme

[2708] Simon Susen, professeur de sociologie à l'Université de Londres, a publié Un article intitulé « Une nouvelle transformation structurelle de la sphère publique ? Avec, contre et au-delà d'Habermas » est analysée l'idée lancée par Habermas dans son dernier travail du point de vue de la transformation structurelle de la sphère publique. Le sociologue britannique évalue également les limites auxquelles Habermas est soumis, par rapport à une mauvaise analyse de l'évolution sociale au début du XXIe siècle. Dans la première partie, les arguments soutenant les idées de Habermas dans la transformation structurelle de la sphère publique sont évalués, et dans la seconde partie, les lacunes de l'argument sont mises en évidence.

[2709] C. Guy-Uriel, L. Fuentes-Rohwer, *Habermas, the Public Sphere and the Creation of a Racial Counterpublic*, Michigan Journal of Race & Law, no21, 2015. https ://repository.law.umich.edu/cgi/viewcontent.cgi?article=1048&context=mjrl

[2710] R. Foster, *Review: A New Structural Transformation of the Public Sphere and Deliberative Politics by Jürgen Habermas,* Oxford Political Review, 2024. https://oxfordpoliticalreview.com/2024/08/26/review-a-new-structural-transformation-of-the-public-sphere-and-deliberative-politics-by-jurgen-habermas//

[2711] S.N. Just, *The Digital Transformation of the Public Sphere." Controversial Encounters in the Age of Algorithms : How Digital Technologies are Stifling Public Debate and What to Do About It*, 1st ed., Bristol University Press, 2025, p. 41-66. https ://doi.org/10.2307/jj.12348220.7. Consulté le 16 novembre 2024.

un facteur déterminant dans l'intrusion dans la vie privée parce que le pouvoir étatique a un intérêt direct à influencer le comportement des individus et l'opinion des masses[2712].

Ce fait est également soutenu par le sociologue américain Gary T. Marx[2713], qui a constaté que la surveillance traditionnelle et ciblée s'est transformée en un modèle qui utilise des techniques avancées pour surveiller de grands groupes de personnes, y compris des « schémas de comportement »[2714]. La « nouvelle supervision » de Marx représente une rupture historique avec les régimes de surveillance précédents, en ce sens qu'elle est avant tout systémique et technologique, plutôt qu'occasionnelle et interpersonnelle[2715].

b). Autonomie individuelle

929. Attaque contre l'autonomie individuelle. Les utilisateurs des médias sociaux se transforment en consommateurs influencés par la délibération fondée sur les arguments justes des démocraties authentiques[2716]. Habermas identifie le danger engendré par le développement des réseaux sociaux en termes d'autonomie individuelle, et les effets négatifs de l'intrusion de l'État dans la vie privée peuvent être limités si une distinction claire entre *la sphère publique*[2717] et *la sphère privée* est maintenue.

La question de l'autonomie individuelle a attiré l'attention des critiques d'Habermas, y compris dans cette perspective d'intrusion extérieure dans la vie privée, mais les choses ne doivent pas être vues sur une note très pessimiste : « bien que la constitution de la sphère publique contemporaine soit marquée par des transformations structurelles majeures et, à plusieurs égards, sans précédent, leur importance ne doit pas être surestimée. Nous ne pouvons qu'espérer que ce qui détermine votre cours de l'histoire ne sera pas une logique systémique

[2712] J. Culp. *Democratic Citizenship Education in Digitized Societies: A Habermasian Approach,* Educational Theory, vol.73(2), 2023. p.178-203 https ://web-p-ebscohost-com.docelec.u-bordeaux.fr/ehost/pdfviewer/pdfviewer?vid=0&sid=1c838778-2946-4951-af90-5f7b75b51d77%40redis

[2713] Gary T. Marx, (né en 1938) professeur émérite au Massachusetts Institute of Technology (MIT), est l'un des principaux chercheurs dans le domaine de la surveillance gouvernementale. Dans ses études, il a créé une carte conceptuelle des façons de collecter et d'analyser les données privées dans le contexte du développement technologique.

[2714] G.T. Marx, *Windows into the soul: surveillance and society in an age of high technology*, The University of Chicago press, 2016.

[2715] J. Clapp, „*Windows into the Soul : surveillance and Society in an Age of High Technology, by Gary T. Marx*". Law & Literature, vol.30, 2018. p.479 – 481

[2716] M. Hofmann, „*Political Deliberation vs. Social Media Branding Crisis-Prone Capitalist Democracies",* Journal of Political Sociology, 2023. https ://journalofpoliticalsociology.org/article/view/17736

[2717] J. Habermas, *L'espace public*, Paris, Payot, 1978.

ancrée dans des technologies apparemment incontrôlables, mais la capacité critique des gens. »[2718]

B. De la philosophie thomiste à la surveillance des masses

930. La relation entre l'individu et l'État. Selon Thomas d'Aquin, l'État « est une communauté parfaite » et les lois, même si elles visent le « bien commun »[2719], sont souvent imparfaites. De l'avis thomiste, l'individu et la famille doivent être soumis à l'État, mais en même temps l'État ne doit pas trop impliquer les affaires internes de la famille, le père ayant la possibilité de faire ses propres lois et de les appliquer comme il le souhaite[2720]. Il existe de nombreuses théories selon lesquelles la domination de l'État sur l'individu est la plus utile et qu'elle fournit les garanties d'une plus grande protection pour[2721] l'ensemble de la société, et que l'oppression est le moyen le plus efficace de promouvoir le bien commun dans la sphère privée[2722]. Quelles que soient les théories adoptées et les avantages et les inconvénients, l'ingérence de l'État dans la vie privée est nécessaire lorsque le but poursuivi est le bien commun. Une synthèse de cette idée se trouve, entre autres à Montesquieu, « le droit n'est pas un obstacle à la liberté, au contraire, c'est celui qui forme la liberté »[2723] mais aussi dans les réalités sociojuridiques d'aujourd'hui. Il est compréhensible que l'ère de l'intrusion forcée de l'État dans la vie privée ait subi une transformation radicale depuis le 11.11.2001, immédiatement après les attentats terroristes aux États-Unis[2724]. Au nom du bien commun, notamment au nom de la prévention du terrorisme, les méthodes de surveillance ont été diversifiées et leur contrôle éthique a été amoindri[2725]. Dans ce contexte, la « communauté

[2718] S.A. Susen, *New Structural Transformation of the Public Sphere? With, against and beyond Habermas,* Soc 60, 2023. p.842–867 https ://link.springer.com/content/pdf/10.1007/s12115-023-00908-y

[2719] T. d'Aquin, *Somme de théologie (Summa theologiae)*, 1266-1273. le livre le plus lu après la Bible concernant les théories religieuses, expose une série de questions et d'objections concernant la loi (verset 90-108).

[2720] Question 90, objection 3 – « *Comme le souverain d'un État gouverne l'État, chaque père de famille gouverne sa maison. Mais le souverain d'un État peut faire des lois pour l'État. Par conséquent, chaque père de famille peut faire des lois pour sa maison.* »

[2721] A. Le Goff, « *Introduction au parcours par Philip Pettit* », Raisons politiques, n°43, 2011. p.151-176 : "*de la même manière que l'immunité n'est pas l'absence de maladie, mais la protection contre certaines agressions auxquelles le corps peut être soumis, la non-nomination n'est pas l'absence d'ingérence, mais la garantie de ne pas être soumis à une ingérence arbitraire*."

[2722] P. Pettit, *Républicanisme : Une théorie de la liberté et du gouvernement*, Gallimard, 2004. p.91

[2723] Montesquieu, *De l'esprit des lois,* Paris, 1748.

[2724] E. J. Knight, A. Gekker, « *Mapping Interfacial Regimes of Control: A Qualitative Analysis of America's Post-9/11 Security Technology Infrastructure. »,* Surveillance & Society, 2020.

[2725] D. Lyon. "*Surveillance after 11 September*", Sociological Research Online, vol.6, 2001. p.116-121. Introduction : « *Au contraire, l'État-nation s'appuie maintenant sur un ensemble accru de surveillance pour ses propres besoins. Deuxièmement, la dépendance à l'égard de méthodes de surveillance de haute technologie n'est*

parfaite » de D'Aquino est une communauté dans laquelle chaque individu est bien encadré par l'État, y compris dans sa propre famille, dans sa propre maison.

931. L'intimité à l'ère des appareils intelligents. Je comprends que l'intimité de sa propre maison est aujourd'hui menacée par des choses qui semblent avoir un usage différent : le fer à repasser peut enregistrer audio-vidéo une querelle conjugale tout en repassant un t-shirt, le réfrigérateur envoie des préférences culinaires à des serveurs tiers, la montre transmet la santé du propriétaire aux réseaux sociaux et la télévision prend des photos des adeptes d'une série hollywoodienne. La collecte de données privées par les géants de l'informatique et les gouvernements est devenue un acte de normalité, il n'est pas naturel de se produire autrement. À l'heure actuelle, la maison d'Aquino, où les lois de l'État sont secondaires, semble encore plus exposée au contrôle qu'un espace public. Sans être entièrement d'accord avec cette opinion, j'ai noté que certains auteurs[2726] soutiennent qu'en raison des appareils ménagers intelligents, les espaces publics offrent plus d'intimité que leur propre maison.

a). Premier jugement limitant l'intrusion de l'État, le procès de Semayne (1604)

932. Le contexte historique, philosophique et social décrit ci-dessus a conduit à une réaction du droit en termes de limitation de l'intrusion de l'État dans la vie privée. Nous pouvons identifier les premiers éléments concrets de cette réaction dans le droit anglais, la sécurité des citoyens étant mentionnée dans les anciennes lois saxonnes[2727]. La protection de la vie privée entre dans le contexte où le XVIe siècle apporte comme nouveauté une plus grande attention aux formes et procédures, y compris dans le domaine du droit pénal[2728]. Nous identifions également le premier processus dans lequel une délimitation est imposée entre ce que l'État est

pas dissuadée par des attaques de faible technologie ou la défaillance de systèmes de sécurité de haute technologie déjà en service. Bien que ces systèmes ne contribuent peut-être pas à réduire le terrorisme, ils sont susceptibles d'entraver les droits civils des citoyens, qui seront davantage profilés et contrôlés. Troisièmement, la lutte pour rendre les systèmes de surveillance de plus en plus responsables démocratiquement et soumis à un contrôle éthique est ralentie par les régimes de panique d'après le 11 septembre. »

[2726] S. Gandrén, N.B. Lundblad, *Smart Household Devices qnd the Negotiation of Public and Private Spaces*, Faculté de Droit, Université de Stockholm, Travail de recherche no. 94, TPRC49 : la 49e Conférence de recherche sur la communication, l'information et la politique Internet, 2021. – « *traditionnellement, la vie privée dans les sphères privées comme nos maisons a été tout sauf tenu pour acquis. Cependant, avec le nombre croissant d'appareils ménagers intelligents, cela change rapidement. Lorsque les pièces, les capteurs et les microphones deviennent des parties de plus en plus intimes de nos vies, collectant continuellement et discrètement des données sur nous, l'idée traditionnelle de ces environnements comme espaces privés est faussée par inadvertance. Les espaces publics traditionnels peuvent même, dans certains cas, accorder plus d'intimité que nos propres maisons* » disponible sur SSRN : https ://ssrn.com/abstract=3902051 ou http ://dx.doi. Org/10.2139/ssrn.3902051

[2727] O. Lisi, *The Beginnings of English Law,* Toronto : University of Toronto Press, 2002.

[2728] J. Hernandez Velez, *La procédure, matrice des libertés anciennes : aux origines du droit au procès (XVIe-XVIIIe siècles),* thèse ss à dir. du Pr Saint-Bonnet, Université Paris II Panthéon Assas, 2020.

autorisé à faire et ce qui est interdit. L'affaire Semayne[2729] présente la situation d'un citoyen anglais mécontent du fait que l'agent du roi a brisé les portes de sa maison pour entrer et faire exécuter une sentence sur le recouvrement de dettes.

Dans une décision rendue en 1604 par la Cour du banc du Roi[2730], il a été décidé que des restrictions claires devraient être imposées à l'entrée des agents du gouvernement dans les maisons privées. Le juge a déclaré qu'un fonctionnaire de l'État ne peut entrer dans un espace privé pour faire appliquer la loi sans avoir suivi une procédure de notification préalable pour la personne concernée. « La maison de chacun est pour lui comme un château et une forteresse[2731], ainsi que pour sa défense contre les blessures et la violence, et pour son repos », a déclaré le tribunal dans[2732] un communiqué. Si la porte de la maison est fermée, elle ne peut être cassée que si la raison concerne un cas de sécurité publique, par exemple, attraper un criminel[2733].

C. Méthodes de surveillance et d'intrusion

a). Origine juridique du mandat de perquisition

933. Souveraineté sur l'espace privé. Fondamentalement, cette affaire est la prémisse pour définir le mandat de perquisition domiciliaire, dans la forme réglementée aujourd'hui. [2734]En 1763, William Pitt écrivait au Parlement : « L'homme le plus pauvre peut, dans son chalet, défier toute la force de la couronne. Il peut être fragile, son toit tremble, le vent peut souffler à travers lui, la tempête peut entrer, la pluie peut entrer, mais le roi d'Angleterre ne peut pas entrer, toute sa force n'ose pas franchir le seuil de la maison en ruine. » [2735]

[2729] *Semayne's Case, (1604) Michaelmas Term, 2 James 1 in the court of King's Bench*, first published in the Reports, vol.5, p.91a.

[2730] La cour précise le droit anglais qui fonctionnait sous l'autorité du roi, établi à la fin du XIIe siècle. Jusqu'en 1421, il suit le roi dans ses voyages, ayant une compétence matérielle dans les affaires pénales et civiles

[2731] « *Et domus sua cuique est tutissimum refugium* » (la maison de chaque personne et son plus sûr refuge) est une expression commune qui remonte à cette période, à la suite du discours (1628) promu par Sir Edward Coke, avocat et homme politique

[2732] La Décision a été publiée par l'avocat Sir Edward Coke (1552-1634) dans Institutes of the Lawes of England en 1628

[2733] Les détails de l'affaire la décision de la cour dans le dossier Semayne sont disponibles sur le site Web du Massachusetts Institute of Technology : https ://groups.csail.mit.edu/mac/classes/6.805/admin/admin-fall-2005/weeks/semayne.html

[2734] William Pitt le Jeune (1759-1806) détient le record d'être le plus jeune premier ministre de l'histoire britannique, occupant ce poste à l'âge de 24 ans. Pendant son mandat, la Révolution française et les guerres de Napoléon ont eu lieu.

[2735] Cet extrait fait partie du discours de William Pitt à la Chambre des Communes en 1763, connu historiquement sous le nom de discours sur le projet de loi sur l'accise. Il est considéré comme un événement décisif dans l'histoire des droits civils, soulignant la nécessité de protéger l'espace privé contre l'intrusion de l'État. Ce discours a influencé le droit à l'inviolabilité du domicile par l'État et les institutions juridiques qui protègent la vie privée.

Dans le même temps, le dossier Semayne a influencé l'introduction du quatrième amendement dans la Constitution des États-Unis, qui interdit les perquisitions arbitraires et établit des règles claires pour la délivrance de mandats par un juge[2736]. Le contexte historique de l'établissement de cet amendement est généré par les réalités de l'expérience coloniale de l'Empire britannique, les maisons des conquis étant perquisitionnées sans préavis et les biens confisqués abusivement.[2737]

934. Apparition des mandats de perquisition. Dans l'affaire Riley v. California, 573 U.S. 373 (2014)[2738], un résumé intéressant est donné de l'apparence de l'institution juridique du mandat de perquisition : « Le quatrième amendement était la réponse de la génération fondatrice aux « mandats généraux » et aux « mandats d'assistance » condamnés de la période coloniale, qui permettaient aux officiers britanniques de perquisitionner leurs maisons sans être entravés par des preuves d'activité criminelle. » La question des mandats généraux de perquisition, qui n'avaient pas une validité exacte, a également été examinée dans deux autres affaires retentissantes qui ont influencé la rédaction de l'amendement IV de la Constitution américaine (1787) : le procès *Entick v. Carrington*[2739] et *Wilkes v. Wood*[2740]. Les deux affaires sont considérées comme des jalons particulièrement importants pour les[2741] précédents judiciaires anglais qui ont changé le cours de l'histoire juridique du monde. Dans l'affaire *Entick c. Carrington,* même si l'agent du gouvernement avait un mandat délivré en vertu de la légalité apparente, le tribunal a déterminé que la procédure de délivrance de ce mandat n'était pas

---

[2736] «*Le droit du peuple à la sécurité des personnes, de leur maison, de leurs documents et de leurs biens ne doit pas être violé par des perquisitions et des saisies non fondées, et tous les mandats ne doivent être délivrés que sur une base plausible, étayés par un serment ou une déclaration et précisant en détail le lieu de la perquisition, personnes et biens à placer en détention*.»

[2737]Le contexte historique de la rédaction du quatrième amendement peut être consulté à l'adresse suivante : *Amdt4.2 Historical Background on Fourth Amendment*, Constitution Annotated, https://constitution.congress.gov/browse/essay/amdt4-2/ALDE_00013706/

[2738] *Riley v. California, 573 U.S. 373,* U.S. Supreme Court, 2014. https ://supreme.justia.com/cases/federal/us/573/373/

[2739] C'est un procès qui a été jugé en 1765 à la suite d'une perquisition par l'agent royal Nathan Carrington le 11 novembre 1762 dans la maison de John Entick, un écrivain qui avait écrit des pamphlets jugés dénigrants par le monarque. Le mandat de perquisition a été délivré par Lord Halifax. À la suite des perquisitions, des dommages importants ont été causés et des documents ont été recueillis qui n'avaient rien à voir avec l'objet de l'enquête. John Entick a intenté une action en justice alléguant une intrusion abusive du gouvernement dans la propriété privée et une violation des droits civils liés à la vie privée. Le tribunal a confirmé l'action d'Entick et a jugé que le mandat n'avait pas de base légale, n'était pas étayé par des preuves, et que l'intrusion de l'État dans « *la propriété privée sans base légale est illégale* ». En même temps, « *le droit à la propriété est sacré et inaliénable* ».

[2740] *Wilkes v. Wood* a été jugé en 1763 et raconte une histoire un peu similaire à celle de John Entick. John Wilkes était un homme politique et journaliste qui a publié du matériel satirique dans le numéro 45 de la Bretagne du Nord. L'article présentait en termes très négatifs l'activité du roi George III et des membres du gouvernement. Le 26 avril 1763, George Montagu-Dunk, comte d'Halifax, émet un mandat qui a pour objet : « *la saisie et la détention des auteurs, imprimeurs et éditeurs d'une œuvre séditieuse et perfide, intitulée The North Briton Number XLV* ». L'accusation criminelle était celle d'« *incitation à l'outrage à la Couronne ou à la rébellion par des mots ou des images publiés* ». Par la suite, le tribunal a établi que le pouvoir discrétionnaire de délivrer et d'exécuter le mandat était illégal. En même temps, c'est à ce moment que l'institution de l'immunité parlementaire a fonctionné pour la première fois.

[2741] C. Burset, T.T. Arvind*, A New Report of Entick v. Carrington (1765),* 110 Ky. L.J., 265*, 2022.*

suffisamment rigoureuse, qu'il est illégal de confisquer tous les documents de la personne concernée sans qu'il soit clairement établi ce qui a été recherché et ce qui a été confisqué. Le caractère général du mandat et le comportement abusif de ceux qui l'ont exécuté ont été sanctionnés. Le résultat de la victoire d'Entick en 1765 se trouve dans de récents arrêts de la Cour suprême américaine, qui pointent vers cette époque de l'histoire du droit : « la bataille de la liberté individuelle et de la vie privée a finalement été gagnée ».[2742]

John Wilkes[2743], journaliste incisif, fondateur du journal North Briton[2744] et député, s'est plaint d'un mandat de perquisition abusif visant son domicile et son bureau. Le tribunal a jugé qu'il n'y avait pas d'éléments essentiels à ce mandat : les noms des personnes concernées, les lieux, les documents demandés et les motifs de leur délivrance.

Ces trois cas sont en réalité un guide pour la rédaction du quatrième amendement par les fondateurs de la Constitution[2745].

b). Première réglementation du mandat de perquisition en France (1808)

935. En droit européen, le mandat de perquisition résidentielle a été institué pour la première fois dans la législation générée par la Révolution française. Ainsi, les prémisses se trouvent à l'article 7[2746] de la Déclaration des droits de l'homme et du citoyen de 1789 et dans le Code d'instruction criminelle de 1808, il est démontré que la perquisition du domicile peut être effectuée par le procureur impérial en cas de délit flagrant (art. 32[2747]) ou bien la perquisition est suivie par le juge d'instruction lui-même dans le cas d'infractions déjà consommées (obtenu 87[2748]). Dans le premier cas, celui de l'infraction flagrante, le procureur est tenu de demander

---

[2742] *Stanford v. Texas*, 379 US 476, 483 (1965).
[2743] D.G. Thomas, „*Wilkes, John (1725-1797), homme politique"*, Oxford Dictionary of National Biography, 2004.
[2744] Le premier numéro du journal, daté du 5 juin 1765, contenait la déclaration suivante : « *La liberté de la presse est le droit de naissance d'un Britannique et est considérée à juste titre comme le bastion le plus ferme des libertés de ce pays* ».
[2745] G. Stone, W.P. Marshall, *The Framers Constitution*, Democracy, 2011. https ://democracyjournal.org/magazine/21/the-framers-constitution/
[2746] « *Nul homme ne peut être accusé, arrêté ni détenu que dans les cas déterminés par la loi, et selon les formes qu'elle a prescrites. Ceux qui sollicitent, expédient, exécutent ou font exécuter des ordres arbitraires, doivent être punis ; mais tout citoyen appelé ou saisi en vertu de la loi doit obéir à l'instant : il se rend coupable par la résistance*».
[2747] « *Dans tous les cas de flagrant délit, lorsque le fait sera de nature à entraîner une peine afflictive ou infamante, le procureur impérial se transportera sur le lieu sans aucun retard, pour y dresser les procès-verbaux nécessaires à l'effet de constater le corps du délit, son état, l'état des lieux, et pour recevoir les déclarations des personnes qui auraient été présentes, ou qui auraient des renseignements à donner. Le procureur impérial demande avis de son transport au juge d'instruction, sans être toutefois tenu de l'attendre, pour procéder, ainsi qu'il est dit au présent chapitre* ».
[2748] « *Le juge d'instruction se transportera, s'il en est requis, et pourra même se transporter d'office dans le domicile du prévenu, pour y faire la perquisition des papiers, effets, et généralement de tous les objets qui seront jugés utiles à la manifestation de la vérité* ».

l'avis du juge d'instruction, sans être obligé d'attendre la réponse. Dans ce dernier cas, le juge n'était pas seulement l'émetteur du mandat de perquisition, mais il supervisait directement l'action elle-même. Si les documents ou objets à rechercher relèvent de la compétence territoriale d'un autre juge d'instruction, l'autorisation de ce dernier sera demandée[2749]. Dans la pratique, l'accent est mis de plus en plus sur la manière dont le droit pénal est appliqué, grâce à des procédures aussi claires et rigoureuses que possible. Par la suite, l'article 59 du Code de procédure pénale, entré en vigueur le 8 avril 1958, introduit encore plus de mesures concernant l'inviolabilité des logements privés, notamment la mise en place d'un programme interdisant les perquisitions de nuit[2750].

c). Mandat de perquisition en droit roumain

936. Évolution de la protection de l'espace privé. L'histoire du droit pénal roumain est étroitement liée à ce qui s'est passé sur la scène politique internationale, mais aussi à la séparation territoriale existant jusqu'à l'Union de 1918. Ainsi, les premières intentions faibles d'établir une réglementation légale se trouvent dans *Pravilniceasca Condică*[2751], adoptée en 1780, qui représente un ensemble de lois civiles et pénales, rassemblées dans un recueil. Concrètement, dans une tentative de protéger la propriété privée, mais aussi pour obtenir un recouvrement efficace des dettes dues à l'État, aucune confiscation ou vente de « choses immobiles » ne[2752] pouvait être faite sans un ordre écrit (« commandement ») émis par le dirigeant. Bien que le Code d'instruction criminelle de Napoléon soit déjà paru, la législation Caragea[2753], le prochain recueil de textes juridiques de Valachie (1818), ne reprend pas

[2749] Article 90 : *« Si les papiers ou les effets, dont il y aura lieu de faire la perquisition, sont hors de l'arrondissement du juge d'instruction, il requerra le juge d'instruction du lieu où l'on peut les trouver, de procéder aux opérations prescrites par les articles précédents* ».

[2750] « *Sauf réclamations faites de l'intérieur de la maison ou exceptions prévues par la loi, les perquisitions et les visites domiciliaires ne peuvent être commencées avant 6 heures et après 21 heures* ».

[2751] Il s'agit d'un document législatif rédigé en 1775 sous l'influence des lumières et souverain Alexandru Vodă Ipsilanti, mais qui est entré en vigueur en 1780 en Valachie. C'était la première tentative importante du droit roumain d'appliquer les principes modernes sur l'organisation de la justice. Aussi connu comme le Petit ordre juridique, ce recueil de lois civiles et pénales a été écrit en roumain et en grec, étant claire l'influence du règne phanariot de cette période. Il a été appliqué jusqu'en 1818, étant abrogé par le Code de Caragea.

[2752] C'est une expression tirée de la *Pravilniceasca Condică*. Le discours est archaïque du point de vue de l'utilisation de la langue roumaine, mais aussi très primitif en termes d'inégalités entre les droits civils des différentes catégories sociales ou ethniques. Par exemple, les membres de l'ethnie rom ont été considérés comme des choses qui ont une valeur d'inventaire, qui sont transmises avec le titre d'héritage, à la page 190 de la forme originale de la collection, nous les trouvons même avec le nom de "*catégories fiscales de Tsiganes*". Toutefois, la discussion sur la vie privée des Roms pourrait présenter un réel intérêt, étant donné que ce petit ordre juridique laisse suffisamment de place à la réglementation juridique à leur égard. Le document peut être consulté en format numérique, numérisé à ce lien : https ://biblioteca-digitala.ro/?volum=8892-pravilniceasca-condica—1957.

[2753] Il est considéré comme le premier code des lois de Valachie, adopté sous le règne Phanariot dirigé par Ioan Gheorghe Caragea (1812 - 1818). L'objectif est de moderniser le droit roumain et d'éliminer les effets négatifs du

l'institution juridique du mandat de perquisition, et ne donne pas beaucoup d'importance à l'inviolabilité de la propriété privée. L'objectif principal était de promouvoir des politiques budgétaires excessives et, à cette fin, la violation de la propriété privée et les saisies injustifiées semblaient être un acte de normalité. Même les règlements organiques de la Valachie et de la Moldavie (1831, 1832)[2754] n'ont pas résolu le problème de la protection claire de l'espace privé contre l'intrusion abusive de l'État. Bien qu'il ait été fait référence à la défense du droit à la propriété[2755], les termes étaient généraux et abstraits, sans procédures concrètes pour établir la protection.

Au lieu de cela, l'expression dans le Code d'instruction criminelle de Napoléon se retrouve sous une forme similaire dans le Code de procédure pénale[2756](1864), qui est entré en vigueur sous le règne d'Alexandru Ioan Cuza. Dans la pratique, l'entrée dans la propriété privée d'une personne soupçonnée („ président ") d'avoir commis une infraction est effectuée avec l'autorisation du juge d'instruction. Ce dernier est tenu d'assister directement à la perquisition : " Le juge instructeur SC transportera, s'il en fait la demande, et pourra se transporter d'office, au domicile du président du tribunal, pour faire les inquisitions des chartes, des œuvres et en général de tous les objets qui se jugeront utiles pour la découverte du certificat " (article 84).

Comme dans le Code français de 1808, s'il y a des choses qui relèvent de la compétence territoriale d'un autre comté, le premier juge perd sa compétence territoriale et la perquisition doit être effectuée avec l'autorisation du juge d'instruction de cette juridiction territoriale. En même temps, le juge d'instruction[2757], figure centrale de la phase d'enquête criminelle, veille au respect de la légalité de la collecte des éléments de preuve soulevés lors de la perquisition domiciliaire.

---

droit coutumier non écrit. Cet ensemble de textes juridiques comprenait à la fois des textes pénaux et civils, mais aussi certains aspects procéduraux.

[2754] Le Règlement Organique est entré en vigueur en Valachie et Moldavie en 1831 et 1832, sous la tutelle de l'autorité de l'Empire Russe, étant considéré comme le premier règlement similaire à une Constitution. Il est considéré comme un facteur de modernisation des deux territoires, étant le premier document juridique établissant un gouvernement commun.

[2755] Art. 209 : « *De cette façon, la vie, l'honneur et la propriété de tous les princes sont des dispositifs sous l'exemption et l'éclipsement des lois terrestres fondées sur son intérieurement administré, qui serviront pour toujours la base immuable et immuable de toute justice publique privée*. » Pour plus de détails : https ://bibl-dlr.solirom.ro/baza-extra/Regulamentele-organice-ale-valahiei-si-moldovei-1831-1832%20%28ed.%201944%29.pdf

[2756] Le 2 décembre 1864, le Code de procédure pénale roumain est entré en vigueur, un document juridique qui a servi de base à la consolidation de l'état de droit en Roumanie. Le code a été rédigé sur le modèle français, mais a également eu quelques influences autrichiennes ou prussiennes. Certains articles ont été entièrement copiés du droit français, et les institutions juridiques sont similaires. Ce Code de procédure pénale était en vigueur jusqu'en 1936.

[2757] Le Juge d'Instruction est une institution juridique spécifique au droit de procédure pénale français, qui a été exclue de la réglementation roumaine en vigueur. Le Code de 1864 dispose que le juge d'instruction était subordonné au Procureur général du Bureau du Procureur de la Cour d'Appel : « *les juges d'instruction seront soumis au contrôle du Procureur général de la cour d'appel, dans la mesure où ils touchent à leurs fonctions par la police judiciaire* » (art. 59).

S'il s'agit d'un délit flagrant, le procureur peut intervenir rapidement, mais il doit alors envoyer au juge d'instruction tous les documents qui concernent l'action pénale pour la vérification de la légalité (art. 57[2758]).

Le Code stipule également que toute perquisition au domicile ou dans d'autres locaux privés où la vérité pourrait être trouvée est effectuée en présence de la personne concernée (art. 38) et un dossier est conclu dans lequel le dossier est enregistré de ce qui a été trouvé, soulevé, et scellé (obtenu 36).

937. Des garanties toujours plus fermes. Dans le Code de procédure pénale promulgué en 1936, l'intention du législateur de protéger l'individu contre l'intrusion de l'État est beaucoup plus claire, elle offre des garanties plus fortes contre l'ingérence abusive. Par exemple, l'article 249 montre qu'aucune perquisition domiciliaire (sauf pour des actes criminels flagrants) ne peut être effectuée contre la volonté du locataire de 20,00 à 6,00. La nuit, cependant, toute perquisition peut être effectuée dans les locaux qui ont une destination publique, même s'ils sont fermés au moment de la perquisition[2759].

Une autre nouveauté destinée à protéger la vie privée est qu'il existe des règles assez claires en matière de fouille corporelle : elle ne peut être effectuée « qu'à l'occasion de l'arrestation ou de la détention de l'accusé » et les femmes ne peuvent être fouillées que par une autre femme[2760].

938. Situation actuelle. Actuellement, le Code de procédure pénale adopté en 2010 et entré en vigueur le 1er février 2014 prévoit quatre types de fouilles : domicile, corps, ordinateur et véhicule. Pour que les choses soient aussi claires que possible, l'article 156, paragraphe 2, dispose que : « la perquisition doit être effectuée dans le respect de la dignité, sans constituer une ingérence disproportionnée dans la vie privée ». Pour procéder à une perquisition à domicile (art. 157) et à une perquisition informatique (art. 168), le consentement du juge des droits et libertés est obligatoire. En revanche, la fouille corporelle (article 165) peut être effectuée par « des organes judiciaires ou toute autorité chargée d'assurer l'ordre public et la

---

[2758] « *Lorsque le délit flagrant sera établi et que le procureur enverra les documents au juge instructeur, il devra juger la procédure sans délai. Il peut refaire tous les actes, ou ceux des actes qui ne semblent pas complets ou réguliers.* »

[2759] Art. 247 du Code de procédure pénale (1936) « *Hormis le délit ou le délit flagrant, aucune enquête ne peut être menée de 20 heures jusqu'à 6 heures, à l'intérieur d'une maison, contre la volonté de celui qui l'habite, sauf par le juge d'instruction en personne.* »
La perquisition commencée pendant le jour peut continuer pendant la nuit.
Les perquisitions nocturnes peuvent être effectuées dans les hôtels, auberges, pubs et généralement, des locaux ouverts au public, même dans les heures où ils sont fermés. »

[2760] Art. 208 : « *L'officier de police judiciaire peut effectuer des perquisitions corporelles à l'occasion de l'arrestation ou de l'arrestation de la personne. La précision corporelle d'une femme ne peut être faite que par une femme. On dresse un procès-verbal tant pour la perquisition corporelle que pour celle domiciliaire*. »

sécurité » sans autorisation préalable du juge. Dans des conditions similaires, une fouille de véhicule est effectuée (article 167).

d). Manque de synchronisation entre le droit et la technologie ?

939. Vu les préoccupations[2761] concernant l'incapacité du droit à faire face aux nouveaux défis posés par l'évolution technologique actuelle, en ce qui concerne directement l'intelligence artificielle, nous nous attendions à ce que les mesures de surveillance de l'état sur les personnes impliquées dans la commission d'actes criminels soient réglementées en pleine simultanéité avec cette évolution. On peut facilement voir un manque de synchronisation entre le moment où la technologie apporte des nouvelles à la société et le moment où la loi réglemente ou utilise ces nouveautés. Par exemple, bien que le système mondial de positionnement (SPG) ait été inventé en 1909, la Roumanie a adopté après 112 la loi n° 146 du 17 mai 2021 sur le contrôle électronique dans les procédures pénales judiciaires et exécutoires. C'est une loi qui utilise le GPS pour localiser les condamnés ou ceux qui font l'objet de poursuites judiciaires et qui doivent être surveillés par bracelet électronique. Il est facile de comprendre qu'un exemple encore meilleur peut être relié à l'invention du téléphone. Après qu'Alexander Graham Bell ait breveté le premier dispositif capable d'émettre et de recevoir des mots en 1876, les avocats ont mis cent ans de plus pour « breveter » un « dispositif juridique » génériquement appelé le mandat d'interception téléphonique. Les exemples présentés peuvent présenter quelques lacunes étant donné qu'aujourd'hui, la technologie et le droit sont dans un galant concours pour s'adapter aux nouveaux besoins sociaux, la dynamique de l'évolution étant tout à fait différente.

§2. INTERCEPTION DES COMMUNICATIONS TÉLÉPHONIQUES, DANS LE CONTEXTE EUROPÉEN

940. Comme on peut le voir dans la présentation précédente, c'est la jurisprudence qui a sous-tendu la construction de l'institution juridique de la perquisition, depuis le procès Semayne (1604) contre le Royaume-Uni et jusqu'à aujourd'hui, des règles de plus en plus claires ont été élaborées pour limiter l'intrusion de l'État dans la vie privée. La jurisprudence semble

[2761] S. Chauhan, A. Keprate, « *Standards, Ethics, Legal Implications & Challenges of Artificial Intelligence* », IEEE International Conference on Industrial Engineering and Engineering Management, Kuala Lumpur, Malaysia, 2022, p. 1048-1052.

également avoir conduit à l'établissement de règles juridiques claires concernant l'interception de conversations par communication à distance.

A. Conditions d'émission du mandat d'interception

a). Malone versus Royaume-Uni (1984).

941. L'arrêt Malone c. Royaume-Uni[2762] de 1984 de la CEDH est le jalon entre le moment où les gouvernements interceptent les appels téléphoniques à volonté, dans un manque total de transparence, et le moment où la nécessité d'une réglementation juridique est devenue impérative. Bref, l'histoire de James Malone, vendeur d'antiquités en Grande-Bretagne, a radicalement changé la façon dont l'État s'est introduit dans la vie privée en interceptant les appels téléphoniques. En mars 1977, Malone a été accusé de commerce illégal de certaines marchandises dans le magasin d'antiquités, qui ont été volées. La principale preuve des illégalités qui auraient été commises par l'antiquaire anglais est les discussions interceptées au cours de conversations téléphoniques. Le mandat d'interception a été donné par le Secrétaire d'État du ministère de l'Intérieur et appliqué par la poste, à la demande de la police. Cette procédure n'avait pas de base juridique concrète mais seulement une interprétation exagérée de l'article 80[2763] de la loi de 1969 sur les postes, la lettre indique que « l'obligation de transmettre des informations à la police peut être imposée au bureau de poste », mais que cette « obligation » ne s'accompagne pas d'une vérification des conditions dans lesquelles un mandat d'interception a été délivré[2764]. En ce qui concerne le fait que les employés de la poste ont pu intercepter des conversations téléphoniques pour leur défense devant la Cour, le Royaume-Uni a affirmé que : En cas d'interception ou de divulgation de matériel intercepté par un employé du bureau de poste « contrairement à ses devoirs » ou « abusivement » et sans mandat du Secrétaire d'État, une infraction aux lois Telegraph Acts 1863 et 1868 et à la loi Post Office (protection) Act 1884 aurait été commise (En ce qui concerne les interceptions téléphoniques)

[2762] *Malone c. Royaume-Uni, no 8691/79*, CEDH, 1984.
[2763] « *Une obligation de faire ce qui est nécessaire pour informer les personnes désignées exerçant des fonctions sous l'autorité de la Couronne des questions et des choses transmises ou transmises par l'intermédiaire des services postaux ou de télécommunications fournis par la Poste peut être imposée à la Poste aux mêmes fins et de la même manière qu'au moment de l'adoption de cette loi, Le Directeur général de la Poste peut être tenu de prendre les mesures nécessaires pour informer ces personnes des questions et choses transmises ou transmises par l'intermédiaire des services qu'il fournit*. »
[2764] Paragraphe 71 de la décision Malone vs. Royaume-Uni

et conformément à la loi de 1953 sur les postes (en ce qui concerne les interceptions postales) ». [2765]

L'arrêt de la Cour portait sur deux aspects essentiels dont elle était saisie par la requérante : « D'une part, si la législation prévoyait qu'une communication transitant par les services postaux ne pouvait être interceptée, à des fins policières, que sur la base d'un mandat valide délivré par le secrétaire d'État et, d'autre part, dans quelle mesure les conditions dans lesquelles un mandat peut être délivré et exécuté sont elles-mêmes limitées par la loi. " [2766]Le gouvernement s'est défendu en invoquant les documents suivants qui vérifient la pratique de l'interception des appels téléphoniques en interne et qui sont « conformes à la loi » .

b). Le rapport Birkett de 1957[2767]

942. Est un rapport présenté au Parlement par Harold Wilson, qui décrit la réglementation juridique de l'interception des communications. Ce rapport a été préparé parce que l'on soupçonnait que les téléphones des députés de la Chambre des communes étaient écoutés. 50 il a été invoqué que l'interception de conversations téléphoniques est légale depuis l'invention du téléphone car auparavant, il était réglementé la situation des interceptions de lettres, cette réglementation a été étendue aux télégrammes et implicitement aux conversations téléphoniques[2768]. Les recommandations du rapport indiquaient, entre autres, que « les mandats ne devraient plus être valables jusqu'à leur annulation, leur validité devrait être pour une période déterminée qui apparaît publiquement » ; « il serait contraire à l'intérêt public que le secrétaire d'État fournisse des chiffres sur l'ampleur de l'interception dans les communications » ; "Le Parlement doit examiner s'il y a lieu d'adopter une loi pour réglementer l'infraction d'interception non autorisée d'une ligne téléphonique" ; chaque mandat doit contenir les données d'identification de la personne concernée, tous les détails inscrits sur le mandat[2769].

[2765] Paragraphe 57 de la décision Malone vs. Royaume-Uni
[2766] Paragraphe 70 de la décision *Malone vs. Royaume-Uni*
[2767] *Report of the Committee of Privy Councillors appointed to inquire into the interception of communications, (Birkett),* London, 1957. Le rapport complet peut être consulté à l'adresse suivante : https://www.fipr.org/rip/Birkett.htm
[2768] Paragraphe 51 du rapport Birkett : „ *nous pensons donc que l'état de droit pourrait être correctement exprimé de cette manière.*
(a) le pouvoir d'intercepter des lettres a été exercé des plus vieux temps et a été reconnu dans des lois successives du Parlement.
(b) ce pouvoir s'étend aux télégrammes.
(c) il est difficile de s'opposer à l'idée que si la loi autorise l'interception de communications sous forme de lettres et de télégrammes, elle est suffisamment large pour couvrir les communications téléphoniques. "
[2769] Paragraphe 56 du rapport Birkett : « *Le mandat du Secrétaire d'État détermine le nom et l'adresse ou le numéro de téléphone des personnes dont les communications doivent être interceptées. Parfois, un seul mandat a été émis dans le passé pour couvrir plusieurs noms. Nous pensons que cette pratique n'est pas souhaitable. À notre avis,*

Dans le même temps, même si le rapport commence par reconnaître « l'origine obscure du pouvoir du gouvernement d'intercepter les communications » et présente des arguments montrant que la situation est sous le contrôle effectif de l'État, il n'est pas nécessaire de la considérer comme une affaire pénale. Il est admis que le manque de clarté de la réglementation juridique aurait pour effet de « répulsion du public contre l'interception téléphonique pourrait affaiblir le soutien populaire et l'approbation des méthodes utilisées par la police » (par. 175). Si l'argument selon lequel l'interception de conversations téléphoniques relève du même régime juridique que l'interception de lettres n'est pas retenue, le rapport Birkett envoie également un message connotatif, ce qui signifie que le Parlement peut avoir l'obligation de légiférer[2770]. D'après les données officielles contenues dans ce rapport, le nombre de mandats d'interception émis par le ministère de l'Intérieur était relativement faible par rapport à ce qui se passait réellement : en 1937, la première année des statistiques présentées, 17 mandats ont été émis, 20 mandats ont été émis en 1939, 180 mandats ont été émis en 1941, et les statistiques de 1956 n'indiquaient que 159 interceptions autorisées. En fait, les chiffres indiquaient que ce n'était pas un problème d'État aussi important.

943. Le deuxième document public présenté à la Cour par le gouvernement est intitulé « **Interception du Livre blanc** » et représente une mise à jour des données du rapport Birkett. En avril 1980, ce document a été présenté au Parlement par le ministre de l'Intérieur et est également connu du public sous le nom de *Livre blanc*. Dans le débat parlementaire qui a eu lieu sur ce rapport du Ministre de l'intérieur, L'accent a été mis sur la nécessité de réformer le système juridique afin que des garanties concrètes soient fournies « afin que les citoyens de ce pays bénéficient pleinement de leur droit à la vie privée et à l'individualité de leur vie domestique, dans la mesure où ils peuvent être garantis, d'une manière qui tienne compte de nos intérêts dans la lutte contre la criminalité et les activités terroristes. » [2771]Dans ces interpellations parlementaires, les interlocuteurs n'ont pas suggéré que « l'utilisation des interceptions téléphoniques, de l'ouverture du courrier ou des méthodes de surveillance électronique devrait être arrêtée », mais ont signé un fait inquiétant : « le problème est que

chaque mandat devrait préciser à l'avenir le nom et l'adresse ou le numéro de téléphone de la personne visée par le mandat. »

[2770] Paragraphe 52 du rapport Birkett : « *Si, toutefois, on considérait que le pouvoir d'intercepter des messages téléphoniques était laissé dans un état incertain, ce qui n'est pas souhaitable, il appartiendrait au Parlement d'examiner les mesures à prendre pour éliminer toute incertitude, si cette pratique devait se poursuivre. En ce qui concerne les lettres et les télégrammes, les dispositions de la Loi Postale de 1953 semblent avoir fonctionné dans la pratique sans aucune difficulté. Si cela est jugé nécessaire, une modification appropriée de cet article de la Loi de 1953 éliminerait tout doute si les communications téléphoniques sont dans la même situation que les lettres et les télégrammes*. »

[2771] Voici une citation de l'interpellation de Lord Hooson au Parlement. L'interpellation complète peut être consultée ici : *Interception of Communications*, HL Deb., vol.409, 1980. https ://api.parliament.uk/historic-hansard/lords/1980/may/21/interception-of-communications

l'utilisation illimitée et surtout irresponsable de ces méthodes met en danger des personnes innocentes – le danger de violer leur vie privée, leur vie familiale et leurs communications intimes, qui sont ensuite stockées par l'état. » [2772]Le *Livre blanc* (1980) a mis en évidence des problèmes qui ressemblaient beaucoup à ceux du rapport Birkett, ajouté de nouveaux défis à la technologie et au nombre croissant de propriétaires de téléphones, et soulevé des préoccupations quant à l'intrusion arbitraire de l'État dans la vie privée. Ce fut l'une des étapes les plus importantes de l'évolution de la réglementation juridique que nous connaissons aujourd'hui, dans le domaine de l'interception des conversations téléphoniques. Ce document ne proposait donc pas la mise en place d'une législation concrète pour l'émission de mandats d'interception, il proposait la nomination d'une personne indépendante, de premier rang dans l'ordre juridique, pour vérifier si ce type d'intrusion de l'État dans la vie privée se fait dans de bonnes conditions ou au contraire.

944. Le troisième document est un **rapport de Lord Diplock**, la personne qui avait été proposée pour surveiller l'activité d'interception par le biais du Livre blanc. L'analyse de Diplock a été mise à la disposition du parlement en mars 1981 et n'a soulevé aucune question juridique ou éthique sur les interceptions, et il s'est dit « satisfait de ce qu'il a trouvé ». Le rapport indique également que : « les mandats n'ont été demandés que dans les cas appropriés et n'ont pas été prolongés plus longtemps que nécessaire pour atteindre leur objectif légitime ». La vérification a également permis de constater que les mandats avaient été délivrés dans des conditions de « sincérité » maximale des informations consignées dans les procédures de délivrance. Il est compréhensible qu'en réalité, le rapport de Lord Diplock dissimulait une situation difficile à croire même pour les années 1980 : l'exécution du mandat a été effectuée par un employé de la poste et non par les services d'enquête criminelle ; Si l'employé de la poste intercepte illégalement une personne sans mandat, une ordonnance pourrait être demandée par le tribunal pour empêcher une telle conduite à l'avenir ; les procédures de délivrance des mandats d'interception n'étaient pas transparentes ; le pouvoir discrétionnaire du secrétaire d'état qui délivre le mandat était absolu ; les interceptions ont été effectuées « conformément à la loi », mais il n'y avait pas de législation réglementant cette activité ; il n'y avait pas de procédure indépendante pour contester les mandats délivrés.

945. La position stricte de la CEDH. La Cour a répondu aux questions susmentionnées en admettant le recours introduit par l'antiquaire dont les conversations avaient été interceptées

[2772] Lord Hooson souligne en outre que : « *Le problème est de trouver le juste équilibre : permettre à la police de mener des enquêtes sérieuses sans ingérence mineure, mais dans le respect des droits des personnes innocentes potentielles. Comment atteindre cet équilibre ? Je suggère que la police soit autorisée à utiliser ces appareils, mais les cas dans lesquels ils peuvent être utilisés sont limités aux cas vraiment graves, avec un système de garanties pour prévenir les abus dans la mesure du possible*. »

pendant des années, considérant que le Royaume-Uni devait adopter une législation conforme à l'article 8 de la Convention[2773] : « en conclusion, en ce qui concerne l'interception des communications, l'ingérence dans le droit du requérant au respect de sa vie privée et de sa correspondance, prévu à l'article 8, n'était pas « conforme à la loi »[2774].

c). Loi sur l'interception des communications de 1985

946. Vision moderne. Dans tout ce contexte décrit ci-dessus, à la suite de la décision rendue dans l'affaire Malone, le « brevetage » du mandat d'écoute électronique pour le droit anglais a été réalisé par la rédaction et l'entrée en vigueur le 10 avril 1986 de la *loi sur l'interférence des communications de 1985*[2775]. Avec cette loi, le Parlement britannique a cherché à exprimer un point de vue relativement moderne sur la manière de limiter l'intrusion de l'État dans la vie privée. Parmi les aspects essentiels de la loi, le mandat devait être délivré par le Secrétaire d'État lorsque cela était nécessaire pour protéger la sécurité nationale, prévenir ou découvrir des infractions graves ou protéger les intérêts économiques du Royaume-Uni.

947. Critiques. Bien que l'esprit de la loi soit régi par les idéaux les plus justes, tels que la prévention des abus et la réglementation d'une pratique visant à un contrôle gouvernemental absolu, le document est remis en question par[2776] l'environnement juridique et politique. La principale critique était qu'elle donnait trop de pouvoirs au Secrétaire d'État et qu'il n'existait aucun contrôle judiciaire sur la délivrance des mandats d'interception, l'article 2[2777] de cette loi élargissant le champ de l'interception par rapport aux pratiques antérieures.

[2773] Paragraphe 86 : « *En Angleterre et au pays de Galles, bien que la police ne soit pas habilitée, en l'absence d'une ordonnance de présentation, à exiger la production de dossiers de contrôle, il existe une pratique selon laquelle la poste, à certaines occasions, créer et fournir de tels dossiers à la demande de la police si les renseignements sont essentiels aux enquêtes policières liées à des délits graves et ne peuvent être obtenus d'autres sources. Le requérant peut donc prétendre, conformément à l'article 25 (article 25) de la Convention, qu'il est « victime » d'une violation de l'article 8 (article 8) du fait de l'existence même de cette pratique, indépendamment de toute mesure coercitive concrète prise à son encontre. Cette conclusion reste valable malgré la clarification fournie par le Gouvernement selon laquelle la police n'a pas fait surveiller le téléphone*. »

[2774] Paragraphe 80

[2775] Il est considéré comme le précurseur du droit moderne sur la réglementation juridique du processus d'autorisation et de supervision des appels téléphoniques au Royaume-Uni. Le document complet peut être consulté à l'adresse suivante : *Interception of Communications Act, 1985.* https ://www.legislation.gov.uk/ukpga/1985/56/contents

[2776] J. Hörnle, et al., "*How to control interception – does the UK strike the right balance?",* Comput. Law Secur. Rev., vol.26, 2010. p.649-654

[2777] Art. 2 paragraphe (1) de Interception of Communications Act du 1985 : « *Sous réserve des dispositions du présent article et de l'article 3 ci-après, le Secrétaire d'État peut délivrer un mandat enjoignant à la personne à laquelle il s'adresse d'intercepter, lors de la transmission par la poste ou par un système public de télécommunications, les communications visées dans le mandat ; le mandat peut également exiger que la personne à qui il est adressé divulgue le matériel intercepté à certaines personnes et de la manière décrite dans le mandat*.»

Les garanties procédurales prévues par cette loi n'étaient pas suffisantes pour protéger pleinement la vie privée contre les intrusions arbitraires de l'État, d'autant plus que tous les employés de la poste exécutaient les mandats d'interception sans qu'ils soient autorisés en aucune façon par un juge. Certains avocats britanniques[2778] soutiennent que la décision dans l'affaire Malone s'est avérée être juste un prétexte pour promouvoir une législation qui élargissait la capacité de l'État à superviser les conversations privées[2779].

Dans le même contexte, Adam Tomkins souligne que l'impact de la décision de la CEDH sur le droit national a été mitigé, même si le droit lui-même est devenu plus clair, le suivi du statut étant plus intrusif[2780].

B. Allemagne – première réglementation juridique explicite sur l'interception

948. En même temps que ces tensions sociales et juridiques ont été signalées en France et au Royaume-Uni, la législation fédérale et les pratiques en matière d'interceptions n'ont pas échappé à la critique. La principale différence est que l'Allemagne semble avoir une longueur d'avance sur les autres états en ce qui concerne la réglementation du mandat d'écoute électronique. En 1968, la loi sur le G10 a été adoptée[2781], la première loi à prévoir une réglementation légale explicite pour l'interception des appels téléphoniques.

Comme dans le cas d'autres pays, jusqu'en 1968, les interceptions étaient effectuées sur la base d'interprétations subjectives de règles juridiques générales, qui n'avaient pas le pouvoir de protéger adéquatement la vie privée. Le sujet est devenu un sujet d'intérêt réel dans le contexte des menaces extérieures croissantes qui pèsent sur l'Allemagne fédérale après la guerre froide[2782]. Ainsi, les motifs de délivrance d'un mandat d'interception étaient similaires à ceux

---

[2778] Adam Tomkins, professeur de droit public à la Faculté de Droit de l'Université de Glasgow

[2779] A. Tomkins, *Intercepted Evidence : maintenant vous m'entendez, maintenant vous ne m'entendez pas*, The Modern Law Review, No.57 , 1994. p.941-954 « *Ainsi, dans l'affaire Malone, la Cour a confirmé ce qui s'est avéré être un silence malheureux quant à la question de savoir si l'interception du téléphone de Malone était nécessaire à des fins licites. Ce silence a incité le gouvernement à étendre le pouvoir de l'État d'intercepter des communications en vertu de l'article 2(2) de la Loi de 1985*. »

[2780] A. Tomkins, op. cit.: « *Bien que la loi soit devenue plus claire à la suite de la décision de la Cour européenne dans l'affaire Malone, le silence de la Cour sur la question plus large a fourni à l'État une occasion en or d'étendre ses propres pouvoirs et, dans le même temps, exclure un contrôle parlementaire ou judiciaire effectif dans ce domaine. »*

[2781] La loi tire son nom de *l'article 10 de la Constitution allemande*, qui protège le droit à la vie privée par l'inviolabilité de la correspondance et des télécommunications. La gamme complète de la loi peut être trouvée ici : https ://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl168s0949.pdf%27%5D__1732914691279

[2782] La guerre diplomatique a commencé le 12 mars 1947 avec le tracé de la ligne de démarcation entre l'Europe occidentale et orientale (chute du Rideau de Fer) et s'est terminée avec la dissolution de l'Union Soviétique le 26 décembre 1991. L'Allemagne fédérale faisait partie du bloc occidental dirigé par les États-Unis, et la sécurité nationale au moment de l'adoption de la loi du G10 était en danger réel car cette ligne de démarcation avait déjà coupé le pays de moitié.

que l'on trouve 17 ans plus tard en droit britannique et 23 ans plus tard en droit français : il y a des menaces à la sécurité de l'état, l'ordre démocratique doit être défendu et les délits graves doivent être évités ou découverts[2783].

a). La loi G10 (1968) permettait une surveillance totale de la population

949. Garanties insuffisantes. La loi a fait l'objet d'un examen attentif par les juges de la CEDH dans l'affaire *Klass et autres c. Allemagne (1978)*[2784], lorsqu'il a été constaté qu'il n'offrait pas de garanties suffisantes quant à la possibilité pour les personnes visées par un mandat d'interception d'être informées de la surveillance, de la cessation des effets du mandat et de la possibilité de contester les mesures ordonnées. En pratique, les demandeurs ne pouvaient prouver qu'ils étaient des victimes directes de la surveillance de l'État, mais la Cour a jugé que cela n'avait pas d'importance puisqu'ils étaient déjà des victimes potentielles d'une surveillance que le gouvernement peut exercer secrètement sur tous les citoyens[2785], Puisque la loi du G10 permettait une telle supervision totale.

950. Impossibilité de contester le mandat de perquisition. La Cour a déclaré que l'article 8 de la Convention n'avait pas été violé, étant donné que les requérants ne pouvaient prouver qu'ils avaient été interceptés illégalement, mais qu'ils en étaient victimes[2786] du fait que la législation ne leur donnait pas la possibilité de contester le mandat d'interception.

Dans le même contexte, la Cour considère également que : « lorsqu'un État établit une surveillance secrète dont l'existence reste inconnue des personnes surveillées et qui ne peut

---

[2783] Il n'y a pas de définition claire de la criminalité grave ni de liste des infractions pour lesquelles un mandat d'interception peut être délivré, en fonction d'un seuil minimum de peine

[2784] *Klass and others v. Germany, no. 5029/71*, CEDH 1978. https ://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57510%22]}

[2785] Le paragraphe 37 est éclairant pour souligner que la législation interne autorisant la surveillance des appels téléphoniques de tout citoyen doit être modifiée : « *en ce qui concerne les faits de l'espèce, la Cour note que la législation contestée établit un système de surveillance en vertu duquel toute personne en République fédérale d'Allemagne peut potentiellement utiliser les informations prévues dans cet article. Veiller à ce que la correspondance, le courrier et les télécommunications soient surveillés à leur insu, à moins qu'il n'y ait eu indiscrétion ou notification ultérieure, conformément aux circonstances énoncées dans l'arrêt de la Cour constitutionnelle fédérale (voir par. 11 ci-dessus). À cet égard, la législation litigieuse affecte directement tous les utilisateurs ou utilisateurs potentiels des services postaux et de télécommunications en République fédérale d'Allemagne. En outre, comme les délégations l'ont souligné à juste titre, cette menace de surveillance peut en soi être considérée comme une restriction de la libre communication par les services postaux et de télécommunications, constituant ainsi pour tous les utilisateurs ou utilisateurs potentiels une ingérence directe dans le droit garanti par l'article 8 (article 8). Lors de l'audience, le représentant du Gouvernement a informé la Cour qu'à aucun moment les mesures de surveillance prévues par le G10 n'avaient été ordonnées ou appliquées à l'égard des requérants (voir par. 13 ci-dessus). La Cour prend note de la déclaration du représentant. Toutefois, à la lumière de ses conclusions sur l'effet de la législation attaquée, la Cour ne considère pas que cette clarification rétrospective influence l'appréciation du statut de « victimes » des requérantes*. »

[2786] Paragraphe 38 : « *Compte tenu des circonstances particulières de l'espèce, la Cour conclut que chacun des requérants a le droit de « prétendre être victime d'une violation » de la Convention, même s'il ne peut prétendre avoir fait l'objet d'une mesure de surveillance concrète* ».

donc être contestée, l'article 8 pourrait, dans une large mesure, être réduit à une simple formalité. Dans une telle situation, il est possible qu'une personne soit traitée d'une manière contraire à l'article 8 ou même privée du droit que lui confère cet article, sans en avoir connaissance et donc sans pouvoir obtenir non plus un recours au niveau national, Ni devant les institutions de la Convention " (par. 36).

En revanche, dans le cadre de la procédure devant la Cour, les représentants du Gouvernement[2787] ont fait valoir que la personne surveillée disposait d'autres voies de recours contre les mesures ordonnées : Contester la légalité de l'application des dispositions de la loi G10, intenter une action devant le tribunal civil si la personne estime avoir subi un préjudice ou intenter une action en justice pour la destruction des preuves obtenues. Enfin, si ces instruments n'atteignent pas leur objectif, l'intéressé peut saisir la Cour constitutionnelle fédérale pour examen de la violation de la Constitution.

b). L'interception des appels à distance doit être nécessaire

951. Interception des conversations – atteinte à la vie privée. Le raisonnement de la Cour dans cette affaire a eu un impact très fort tant en Allemagne fédérale, qui a dû renforcer ses mécanismes de surveillance et de contrôle indépendants de la surveillance, que dans le reste des pays européens, dont la France. Cependant, la loi du G10, toujours en vigueur aujourd'hui sous la règle de plusieurs modifications et reconfigurations, a été vérifiée au fil du temps par la CEDH[2788], réitérant à cette occasion que l'interception de conversations est une ingérence dans la vie privée et doit être nécessaire[2789] et proportionnée.

En l'an 2021, cette loi a subi des changements[2790] qui ont donné lieu à des controverses qui ont eu un fort écho juridique et social[2791] – les pouvoirs de surveillance de la police fédérale et des services de renseignement ont été augmentés et l'utilisation de « programmes d'espionnage » pouvant être insérés dans les téléphones a été approuvée Les utilisateurs pour décrypter et intercepter les conversations tenues sur des applications qui garantissent le cryptage, telles que WhatsApp ou Telegram[2792].

[2787] De plus amples explications figurent au point 24 de la décision de la Cour

[2788] Affaire *Weber et Saravia c. Allemagne,* 2006 – https ://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-76586%22]}

[2789] J. Gerards, *How to Improve the Necessity Test of the European Court of Human Rights*. International Journal of Constitutional Law, no 11, 2013.p.466-490

[2790] https ://www.buzer.de/gesetz/4705/index.htm

[2791] D. Fischer, *Germany's New Surveillance Laws Raise Privacy Concerns,* Human Rights Watch, 2021. https://www.hrw.org/news/2021/06/24/germanys-new-surveillance-laws-raise-privacy-concerns

[2792] Vous trouverez plus de détails à ce sujet dans la section sur les effets juridiques de la cryptographie

c). Surveillance technique des étrangers versus surveillance des propres citoyens

952. Protection différente selon la nationalité et la citoyenneté. Alors que la situation concernant la protection des citoyens d'un État semble assez claire, la législation de l'Allemagne, de la France, du Royaume-Uni et surtout des États-Unis a accordé un régime spécial à la surveillance des conversations étrangères. Fondamentalement, il y a deux poids, deux mesures d'appréciation de l'intrusion dans la vie privée entre citoyens et étrangers, dans ce dernier cas les limites sont beaucoup plus larges[2793].

Le problème a été signalé pour la première fois par Edward Snowden, un ancien employé de la National Security Agency des États-Unis, qui a présenté en 2013 des preuves montrant l'utilisation de programmes de surveillance mondiale par les services de renseignement. L'histoire de Snowden était déjà bien connue, non seulement très médiatisée, mais aussi l'objet d'un film qui choque l'opinion publique à travers les données fournies[2794].

En vertu de la loi BDN[2795] de 2016, l'Allemagne réglemente la surveillance de masse des étrangers, des journalistes, des agences de presse ou d'autres personnes se trouvant à l'étranger. En réponse à la question rhétorique posée par les avocats – « qui mérite la protection de la vie privée »[2796] – en vertu de la loi BDN, l'Allemagne a montré que la protection diffère selon la nationalité et la citoyenneté.

d). Iniquités liées à l'intrusion de l'État dans la vie privée

953. Violation du droit à l'égalité. En 2020, la Cour constitutionnelle est intervenue par une décision historique[2797] et a sanctionné les dérapages évidents constatés dans le contenu de la

[2793] M. Rojszczak, « *Extraterritoriale Bulk Surveillance after the German BND Act Judgment*. », European Constitutional Law Review, vol.17, no.1, 2021. p.53-77

[2794] Snowden est un thriller biographique de 2016 dirigé par Oliver Stone et détaille la motivation de l'employé de la NSA à introduire le monde à la pratique des services d'information de surveillance de la population de masse. Au moment de la sortie du film, Edward Snowden était déjà en fuite, étant accusé par les États-Unis d'avoir violé la Loi sur l'espionnage de 1917 et volé des documents gouvernementaux

[2795] *La loi du 23 décembre 2016 sur le contrôle des télécommunications étrangères par le Service fédéral de renseignement (Bundesnachrichtendienst*), qui régit notamment l'activité de surveillance exercée par le Service allemand de renseignement étranger, a été publiée après que la France eut adopté une législation similaire un an plus tôt.

[2796] M. Milanovic, „*Human Rights Treats and Foreign surveillance : Privacy in the Digital Age*", Harvard International Law Journal, vol.56, 2015 p.81-146. La version complète du document peut être trouvée ici : https ://www.ilsa.org/Jessup/Jessup16/Batch%202/MilanovicPrivacy.pdf

[2797] La décision peut être consultée ici : https ://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html

loi. L'affaire a été portée devant la Cour constitutionnelle à la suite d'une plainte de deux personnes, à laquelle environ 6000 autres personnes, en particulier des journalistes étrangers[2798], se sont jointes, les principales plaintes concernant la violation du droit à l'autodétermination en matière d'information et du droit à la confidentialité des télécommunications.

Il est également allégué que la loi viole la « garantie générale du droit à l'égalité » dans le contexte où les citoyens de l'Union Européenne ne bénéficient pas d'une protection similaire à celle des citoyens à l'intérieur des frontières allemandes, ce qui est contesté par les avocats depuis l'adoption de la loi[2799]. La question de ces inégalités concernant l'intrusion de l'État dans la vie privée des citoyens par rapport aux étrangers était déjà abordée dans l'environnement juridique[2800].

954. Critique de la Cour constitutionnelle à l'égard de la loi BND. Les principales conclusions de la Cour sont les suivantes :

- La loi BND violait les droits fondamentaux des personnes en dehors des frontières du pays, permettant une surveillance massive des télécommunications sans[2801] autre justification
- Le droit à la vie privée a été appliqué discrètement aux personnes à l'étranger[2802], ce qui est contraire à la Constitution et aux conventions internationales auxquelles l'Allemagne est partie. Il ressort de l'analyse de la décision que la différence de protection juridique offerte aux

[2798] *Criticism of the BND Act*, RSF. https ://www.reporter-ohne-grenzen.de/en/topics/internet-freedom/criticism-of-the-bnd-act

[2799] C. Schaller, „*Strategic surveillance and external Basic Rights protection : German Intelligence Law After Snowden*", German Law Journal, vol.19, 2018. p.941-80. L'article complet peut être trouvé ici : https ://www.cambridge.org/core/services/aop-cambridge-core/content/view/494F82EE78DCF2709B07A2B57D95454C/S2071832200022926a.pdf/strategic-surveillance-and-extraterritorial-basic-rights-protection-german-intelligence-law-after-snowden.pdf

[2800] L. Asaf, « *We Only Spy on Foreigners » : The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance,* 18 Chicago Journal of International Law, 2018. p.502. L'article complet peut être trouvé ici : https ://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1730&context=cjil

[2801] Paragraphe 134 : « *Le défaut de préciser spécifiquement les droits fondamentaux affectés ne peut être justifié par le fait que les dispositions contestées consacrent en premier lieu une pratique administrative ancienne. En particulier, on ne peut soutenir que l'obligation de préciser expressément les droits fondamentaux concernés ne s'applique pas lorsque la loi prévoit des restrictions aux droits fondamentaux qui existent déjà dans la législation précédente ou n'introduit que des modifications mineures à ces droits. Une pratique administrative dénuée de fondement juridique ne constitue ni une loi applicable ni une restriction valable des droits fondamentaux. En outre, une simple pratique administrative ne peut servir d'avertissement équivalent à celui prévu par une loi qui respecte l'obligation de préciser les droits fondamentaux affectés. C'est d'autant plus vrai pour une pratique secrète d'un service de renseignement*. »

[2802] Paragraphe 96 : « *Ce lien entre les droits fondamentaux et les garanties des droits de l'homme est incompatible avec l'idée que l'applicabilité des droits fondamentaux en vertu de la Loi Fondamentale s'arrête aux frontières nationales, cela exempterait les autorités allemandes de l'obligation de respecter les droits fondamentaux et les droits de l'homme lorsqu'elles agissent à l'étranger à l'égard de citoyens étrangers. Une telle idée irait à l'encontre de l'objectif de la Loi Fondamentale qui est de garantir à chaque personne des droits inaliénables en vertu des conventions internationales et au-delà des frontières nationales – y compris la protection contre la surveillance*. »

étrangers ne peut toutefois pas être la même que celle offerte aux nationaux à l'intérieur des frontières[2803]

- Il n'y a pas de contrôle indépendant de l'activité menée en vertu de la loi BND, bien que cela soit aussi nécessaire que possible. Il est proposé d'embaucher du personnel spécialisé, pas seulement des superviseurs honoraires qui ont une autre profession[2804]
- Il n'y a pas de restriction claire à l'interception des communications internationales, les journalistes faisant partie des catégories de personnes les plus exposées sous surveillance
- Il y a eu un échange abusif et incontrôlé de données recueillies au cours de la surveillance entre différents états[2805]. Ainsi, les données collectées par les services de sécurité allemands, principalement celles qui visent à protéger la vie privée, pourraient atteindre un autre État, contournant certaines restrictions législatives[2806]. Cette pratique a été signalée pour la première fois par Snowden en 2013 concernant les activités de la NSA.
- Il n'y avait pas de procédure claire pour supprimer les données privées qui avaient été recueillies involontairement ou les données qui n'avaient fait l'objet d'aucune analyse au moment où de grands volumes de données ont été interceptés. En appliquant le principe de proportionnalité[2807], la Cour constitutionnelle a déclaré l'inconstitutionnalité de la loi également

---

[2803] Rojszczak, Marcin, *Extraterritorial bulk surveillance after the German BND Act judgment*, European Constitutional Law Review, vol. 17, n° 1, 2021. p. 64

[2804] Paragraphe 287 : « *Dans l'ensemble, il convient de veiller à ce que la surveillance soit exercée de manière compétente et professionnelle par la nomination, en général, de personnes au sein de l'organe de surveillance dont elle est l'activité principale ; la surveillance exercée principalement à titre honorifique n'est pas suffisante. La composition des organes de surveillance doit également être équilibrée. Tant structurellement qu'en ce qui concerne le personnel, une distance suffisante par rapport au Service Fédéral de Renseignement doit être garantie pour assurer l'indépendance nécessaire à ces organes de contrôle*. »

[2805] Paragraphe 211 : « *Les données à caractère personnel issues de la surveillance stratégique ne peuvent être partagées avec d'autres organismes que s'il existe une base juridique claire et suffisamment spécifique, qui subordonne ce partage à la protection d'intérêts juridiques et à certains seuils reflétant la gravité de l'ingérence résultant de la surveillance stratégique. Le partage de données à caractère personnel provenant de la surveillance stratégique n'est autorisé qu'aux fins de la protection d'intérêts juridiques d'une importance particulière et nécessite, comme seuil, l'existence d'indices de danger identifiable (konkretisierte Gefahrenlage) ou de motifs suffisamment spécifiques de suspicion de comportement criminel (hinreichend konkretisierter Tatverdacht). Cela ne s'applique pas aux rapports soumis au Gouvernement Fédéral, dans la mesure où ils visent uniquement à fournir des informations politiques et à préparer des décisions gouvernementales. »*

[2806] Paragraphe 236 : « *Toutefois, le partage de données personnelles avec d'autres états n'est autorisé que si la gestion des données partagées dans ces états ne porte pas atteinte à la protection des données personnelles garantie par les droits de l'homme. Cela ne signifie pas que l'ordre juridique de l'autre État doit garantir des mesures de protection institutionnelles et procédurales équivalentes à celles de l'Allemagne ; en particulier, il n'est pas nécessaire de reproduire les mesures formelles et institutionnelles prévues par la loi allemande sur la protection des données. Il est toutefois nécessaire de garantir un niveau substantiellement adéquat de protection des données dans sa gestion dans l'État destinataire. À cet égard, il convient notamment de se demander si les limites résultant de la limitation de la finalité, des exigences de suppression et des exigences fondamentales en matière de surveillance et de sécurité des données – toutes communiquées lors du partage des données – sont respectées, du moins en général, dans l'utilisation des données. Pour déterminer si ces conditions sont remplies, il faut se fonder sur le droit interne de l'État d'accueil, ainsi que sur ses obligations internationales et leur mise en œuvre dans la pratique quotidienne*. »

[2807]Paragraphe 208 : « *Le principe de proportionnalité impose également des obligations d'effacement en ce qui concerne les mesures de surveillance. Le but de ces obligations est de s'assurer que l'utilisation des données personnelles reste limitée aux finalités justifiant leur traitement et que les données ne puissent plus être utilisées une fois ces finalités atteintes.* »

sur cette question, en ce qui concerne l'absence de réglementation de la suppression des données et en particulier le moment où cela devrait être fait, le stockage illimité n'étant pas autorisé[2808]. Avant la décision de la Cour, les organisations internationales avaient soulevé un fait inquiétant : « la technologie d'interception de masse supprime toute considération de proportionnalité, permettant une surveillance non discriminatoire. Il permet à l'État de copier et de surveiller chaque acte de communication dans un pays ou une région, sans obtenir d'autorisation pour chaque cas individuel d'interception.[2809]

- L'application du principe de proportionnalité, antérieure à l'arrêt de la Cour, a

également été précisée par la Cour que lorsque l'analyse des données est effectuée manuellement « la loi doit veiller à ce que la vérification complémentaire cesse dès qu'il apparaît que la surveillance atteint le cœur de la vie privée ». Il est interdit d'avoir un double contrôle des mêmes données qui touchent les zones les plus sensibles de la vie privée.

La Cour déclare qu'« il doit être absolument interdit que le noyau de la vie privée devienne la cible d'enquêtes étatiques ou que des informations relatives à ce noyau soient utilisées de quelque manière que ce soit ou servent de base à d'autres enquêtes » et que la protection offerte « ne se limite pas aux situations qui le sont je ne regarde que des questions très personnelles. » Ce « noyau », « essence » de la vie privée, doit être « protégé à la fois au stade de la collecte des données et au stade de l'analyse »[2810]. Afin de ne pas mettre en danger les enquêtes pénales fondées sur ces données obtenues à partir de la surveillance des conversations à distance, la Cour constitutionnelle complétera le raisonnement exposé ci-dessus par ce qui suit : « cependant, les communications dans lesquelles des actes criminels sont discutés et planifiés ne font pas partie de l'essence de la vie privée, même lorsqu'elles concernent aussi des questions extrêmement personnelles. »

[2808] Paragraphe 209 : « *Les mesures de surveillance, telles que celles qui sont en cause en l'espèce, qui interceptent de grands volumes de données, dont une partie seulement peut être consultée pour analyse, doivent faire l'objet de dispositions claires en matière de suppression. Ces dispositions doivent garantir que les données interceptées involontairement, mais pour lesquelles l'examen du contenu est interdit en vertu du droit constitutionnel, sont immédiatement séparées des autres données et supprimées définitivement sans laisser de traces. Dans la mesure où l'analyse des données s'effectue en plusieurs étapes, où le volume de données est progressivement réduit, des dispositions spécifiques sont nécessaires pour assurer une analyse rapide des données et pour garantir qu'à chaque étape, les données identifiées pour la suppression sont immédiatement supprimées. Dans la mesure où les informations sont classées comme pertinentes et doivent être conservées pendant une période plus longue en vue d'utilisations ultérieures, il convient d'adopter des dispositions appropriées. Le législateur doit créer l'obligation de contrôler le stockage des données à des intervalles suffisamment courts pour s'assurer que les données ne sont pas conservées sans justification.* »

[2809] *Rapport du Rapporteur Spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, Frank la Rue, Organisation des Nations Unies, A/HRC/23/40. La version complète peut être lue ici : https ://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

[2810] Paragraphe 205 de la *décision de la Cour Constitutionnelle*

e). Les services secrets sont tenus de respecter le droit à la vie privée au-delà des frontières

955. La Cour constitutionnelle impose une modification de la législation. Cette décision a confirmé les pratiques de surveillance mondiale des utilisateurs de technologies, qu'il s'agisse de conversations téléphoniques, d'utilisation des réseaux sociaux ou simplement de trafic de données à partir de n'importe quel système informatique. En déclarant ces pratiques inconstitutionnelles, la Cour a imposé la modification de la loi avant la fin de 2021.

Dans la pratique, les services de renseignement ont été tenus de respecter le droit à la vie privée garanti par la Constitution et au-delà des frontières de l'État allemand. Les associations non gouvernementales spécialisées dans la défense des droits fondamentaux considèrent cette décision comme la fin de la surveillance de masse[2811]. Dans le même temps, la décision a été accueillie avec beaucoup d'enthousiasme par les organisations de journalistes[2812], l'opinion publique[2813] et les avocats[2814].

956. Prévention des atteintes transnationales à la vie privée. Cette décision est la pierre angulaire d'une approche juridique dans laquelle il est proposé que les services de sécurité respectent le droit à la vie privée au-delà des frontières étatiques. Toutefois, la question de l'extraterritorialité de la défense des droits fondamentaux, y compris de la vie privée, a connu une dynamique qui n'était même pas prévue par la CEDH lorsqu'elle a rendu sa décision dans l'affaire Bankovic c. Belgique (1999)[2815], il a déclaré que « les violations des droits de l'homme

---

[2811] Liberties.eu, *The End of Mass Surveillance: German Constitutional Court Strengthens Basic Rights Abroad,* Society for Civil Rights, 2020. https ://www.liberties.eu/en/stories/bnd-ruling-mass-surveillance-declared-unconstitutional/18635

[2812] Reporter ohne Grenzen, *Worldwide mass surveillance by Germany's intelligence service declared unconstitutional in landmark ruling on press freedom in the digital age*, déclaration de presse, 2020. https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/Dokumente/200519_Press_statement_BND_ruling_EN-final.pdf

[2813] "*Hallo BND, das Grundgesetz Gilt auch für euch* !" c'est le titre d'un article paru dans la presse nationale allemande. L'introduction de l'article est : « *Überwachung ist gefährlich und braucht klare Grenzen, immer und überall » (« la surveillance est dangereuse et nécessite des limites claires, toujours et partout* »). https ://www.zeit.de/politik/deutschland/2020-05/bundesverfassungsgericht-urteil-bnd-auslandsueberwachung-grundrechte

[2814] K. Kappler, « *Conséquences de la décision de la Cour constitutionnelle allemande sur le Service allemand de renseignement étranger : l'importance des droits de l'homme dans la coopération des services de renseignement »*, German Law Journal, vol.23, 2022. p.173–185. « *Il est déjà remarquable de voir avec quelle intensité la Cour constitutionnelle fédérale intègre le droit international, en tenant compte de la situation juridique dans la Convention Européenne des Droits de l'Homme (CEDH). Cela pourrait entraîner un réexamen au-delà du cas individuel : en raison des multiples interrelations entre le droit international et national et la coopération internationale, la Loi Fondamentale doit être interprétée et appliquée conformément au droit international* » (p.174).

[2815] HUDOC, European Court of Human Rights, „*Decision Bankovic and Others v. Belgium & 16 other Contracting States. Press Release*", 2001, numéro de référence: 003-470135-471261. https ://hudoc.echr.coe.int/eng-press?i=003-470135-471261

de nature extraterritoriale seront rares et ne perturberont pas l'application traditionnelle de la loi ».

À la suite de la décision du 19 mai 2020, la littérature juridique a constaté que la transnationalité ne s'applique plus uniquement au commerce, tel qu'il était traditionnellement perçu, mais également à la protection des droits fondamentaux[2816].

C. Partenariats d'échange de données entre la France, l'Allemagne, les États-Unis et le Royaume-Uni

Quant à la question du partage de données qui concerne la vie privée des individus, elle est plus ancienne dans des pays comme l'Allemagne ou la France. En particulier, après l'entrée en vigueur de la loi du G10 en 1968, l'Allemagne, la France, le Royaume-Uni et les États-Unis ont signé des accords sur l'échange de données obtenues par la surveillance des citoyens par les services de renseignement.

En 2012, le professeur Josef Foschepoth[2817] a souligné le problème de la coopération trop peu transparente et potentiellement abusive. L'information de Foschepoth a été confirmée peu après les révélations de Snowden et l'impact sur la société a été très fort, car des inquiétudes étaient déjà soulevées dans l'espace public au sujet de[2818] la surveillance de masse des citoyens européens par les États-Unis. Le 6 août 2013, l'accord administratif entre la France et l'Allemagne a été annulé en 1968[2819], après la clôture de l'accord avec les États-Unis et le Royaume-Uni[2820], au motif que ces documents violaient le droit à la vie privée des citoyens

---

[2816] D. Palombo, « *Droit Extraterritorial, Universel ou Transnational des droits de l'homme* ? » Israel Law Review vol.56, no.1, 2023. p.92–119. « *L'universalité a toujours fait partie intégrante de la rhétorique des droits de l'homme, mais les tribunaux internationaux sur le terrain ont largement ignoré ou minimisé sa pertinence. La « transnationalité » est une dimension qui appartient traditionnellement au commerce, mais qui est également adoptée dans les différends stratégiques relatifs aux droits de l'homme. Au lieu de se concentrer sur l'extraterritorialité et ses nombreuses exceptions, les tribunaux internationaux des droits de l'homme et les chercheurs devraient se tourner vers un horizon plus large de langues et de concepts pour mettre en œuvre le droit des droits de l'homme dans un monde globalisé*. » (p.118)

[2817] Josef Foschepoth (né en 1947), professeur à l'Université de Fribourg, historien spécialisé dans la recherche sur la surveillance en Allemagne après la guerre, a publié des documents attestant que les accords de 1968 étaient toujours en vigueur et que les états signataires se fournissaient mutuellement les données privées recueillies.

[2818] Sous le titre « *Annulation des concessions de surveillance* », publié le 08.02.2013, des journalistes allemands ont montré qu'il existe de sérieuses preuves d'une activité de surveillance de la population par le Royaume-Uni et les États-Unis à travers un logiciel tel que XKeyscore, un outil de collecte massive de données https ://www.dw.com/en/germany-cancels-cold-war-era-surveillance-pact-in-wake-of-spying-revelations/a-16994741

[2819] Auswärtiges Amt, « *Déclaration du ministère des Affaires étrangères sur la résiliation de l'accord avec la France* », newsroom, 2013. https ://www.auswaertiges-amt.de/de/newsroom/130806-g10-frankreich/257000

[2820] « *L'annulation des accords administratifs, pour laquelle nous avons insisté ces dernières semaines, est une conséquence nécessaire et juste des récents débats sur la protection de la vie privée* », a déclaré le Ministère des Affaires Étrangères dans un communiqué.

allemands. Outre le partage des données, l'accord a permis à la France d'utiliser l'infrastructure de communication allemande pour les activités de surveillance.

a). Obama : « Vous ne pouvez pas avoir 100 % de sécurité et 100 % de respect de la vie privée en même temps »

957. Réactions fermes de la part de l'Allemagne. La scène politique et sociale en Europe a été très chaude à propos de ces accords, ce qui a provoqué une réaction ferme de l'ancienne présidente Angela Merkel, accusée même de complicité dans l'utilisation de programmes d'espionnage de masse : « L'Allemagne n'est pas un État supervisé »[2821].

Avant cette déclaration, le journal allemand Spiegel[2822] a publié une série de preuves que la NSA[2823] surveillait dans le cadre du programme connu appelé PRISM[2824]plus d'un demi-milliard d'appels téléphoniques, de courriels, de SMS, de conversations privées d'utilisateurs en Allemagne.

958. Collecte massive de données dans le cas de l'Allemagne. Les données ont montré qu'en quelques jours, des données sur plus de 20 millions d'appels téléphoniques et plus de 10 millions de connexions internet ont été collectées par des citoyens allemands. Les statistiques ont montré que pendant les vacances d'hiver, la quantité de données augmentait, avec des jours avec plus de 60 millions de connexions téléphoniques supervisées. Une surveillance similaire a été constatée dans des pays comme la Chine, l'Arabie saoudite et l'Iraq.

En revanche, les publications allemandes ont exprimé leur surprise qu'en France, la quantité de données collectées soit beaucoup plus faible[2825].

[2821] The Daily Star, *"Merkel says 'Germany not a surveillance state'"*, AFP, 2013. https://www.thedailystar.net/news/merkel-says-germany-not-a-surveillance-state?

[2822]Spiegel Online, *„NSA überwacht 500 Millionen Verbindungen in Deutschland"*, 2013. https ://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwacht-500-millionen-verbindungen-in-deutschland-a-908517.html

[2823] The Editors of Encyclopaedia Britannica, *National Security Agency (NSA) – History, Role, & Surveillance Programs*, Encyclopaedia Britannica. https ://www.britannica.com/topic/National-Security-Agency#ref1201263

[2824] PRISM est le nom de code donné par la National Security Agency des États-Unis à un programme qui collecte plus de 90% des données Internet stockées par des géants de l'informatique comme Google ou Apple. Certains termes de recherche de données clés peuvent être analysés, y compris des informations qui sont normalement cryptées mais qui ont « *traversé la colonne vertébrale d'Internet* ». Le programme a été lancé en 2007 sous l'administration George Bush, avec la collecte massive de données étant le principal objectif du programme. Il s'agit de surveiller le trafic Internet et les communications téléphoniques des citoyens américains et du reste du monde.

[2825] « *Ainsi, la NSA est plus active en Allemagne que dans tout autre pays de l'Union Européenne. En comparaison, pour la France, les Américains ont enregistré, en moyenne, plus de deux millions de données de connexion par jour* », le journal Spiegel, 2018.

Au moment de la publication de ces statistiques, au milieu des tensions sur la surveillance de masse des citoyens européens et au-delà[2826], appliquant un raisonnement similaire à la réponse stalinienne bien connue : « vous ne pouvez pas faire une omelette à moins de casser quelques œufs », a déclaré le président américain Barack Obama : « vous ne pouvez pas avoir 100 % de sécurité et en même temps 100 % de confidentialité et aucun inconvénient. » [2827] Pendant ce temps, le président américain est également venu en Allemagne pour soulager la tension politique.

D. Surveillance de type Big Brother : ciblée et massive. Le point de vue de la CEDH

La surveillance ciblée s'est développée autour de la procédure pénale et de la sécurité nationale, en tant qu'instrument ponctuel axé sur des personnes déterminées, à l'égard desquelles il existe des indices ou des soupçons concrets, dans le but de recueillir des preuves et de documenter des faits déjà soupçonnés. Elle s'inscrit, du moins en théorie, dans un cadre exceptionnel, individualisé et contrôlable juridiquement[2828]. La surveillance de masse apparaît lorsque les infrastructures numériques (réseaux mondiaux, câbles à fibre optique, communications électroniques) permettent la capture et l'analyse simultanées des flux de données de populations entières, dans une logique de prévention des risques diffus (terrorisme, criminalité organisée, cybermenaces), sans lien nécessaire avec une suspicion individuelle préalable[2829]. La tension centrale devient ainsi le passage de l'« exception » de la surveillance ponctuelle à la « normalisation » de mécanismes structurels de surveillance généralisée. Cette situation est sévèrement sanctionnée par les opinions doctrinales : « par l'effet d'un troublant parallélisme, elle provoque des atteintes au droit de l'homme et particulièrement au droit au respect de la vie privée, du domicile et de la correspondance d'une telle ampleur qu'elle est presque aussi redoutable que les périls qu'elle prétend endiguer »[2830].

[2826] Z. Kleinman, *"What does Prism tell us about privacy protection?"*, BBC News, 2013. https://www.bbc.com/news/technology-22839609

[2827] J. Mayer, *"NSA surveillance program includes collection of e-mail and phone data of millions of Americans"*, The New York Times, 2013.

[2828] L. Laref, M. Laref (dir.), *Surveillance*, Paris, Dalloz, coll. "Themes & commentaires – Actes", 1re éd., 28 nov. 2024, p.341: « Pour simplifier, on dira qu'elle vise une ou plusieurs personnes précises à qui l'on a déjà quelques reproches à adresser ou sur qui l'on a déjà quelques soupçons à nourrir. Elle tend à accumuler des preuves contre elles pour pouvoir les confondre et les sanctionner pénalement, disciplinairement ou civilement. Il est à parier que tout ce qui pouvait en être dit a été développé au cours de la séance intitulée surveiller et prouver. »

[2829] *Op. cit*., p.342: « la surveillance de masse est exercée dans le plus grand secret sur des milliers et des milliers de personnes anonymes sur lesquelles ne pèse encore aucun soupçon précis et qui ne sont pas encore prises dans les mailles d'une procédure pénale. »

[2830] *Op. cit*. p.342.

a. La surveillance ciblée dans la vision de la CEDH

La jurisprudence de la CEDH en matière de surveillance secrète ciblée définit progressivement un noyau dur de protection de la vie privée face aux nouvelles technologies, sans pour autant valider la surveillance de masse. Dans l'affaire Vetter c. France[2831], l'installation de micros dans un appartement montre que toute ingérence cachée dans l'espace privé nécessite une base juridique claire et des garanties contre l'arbitraire. Dans l'affaire Uzun c. Allemagne[2832], la Cour admet la surveillance par GPS dans le cadre d'une enquête grave, mais la qualifie d'ingérence au sens de l'article 8, légitime uniquement sous réserve de restrictions strictes et d'un contrôle judiciaire. L'affaire Roman Zakharov c. Russie[2833] marque un saut qualitatif : les systèmes structurels d'interception des communications mobiles sont sanctionnés pour absence de garanties effectives, même en l'absence d'une victime identifiée. Dans l'affaire Peck c. Royaume-Uni[2834], la divulgation d'images de vidéosurveillance d'un geste suicidaire montre que même dans l'espace public, il peut exister des situations « profondément privées ». Ensemble, ces arrêts définissent le paradigme de la surveillance secrète ciblée : admissible, mais soumise à des exigences matérielles et procédurales rigoureuses afin d'empêcher qu'elle ne se transforme en un mécanisme diffus, quasi généralisé, d'érosion de la vie privée.

b. La surveillance de masse selon la CEDH. Big Brother Watch

L'évolution de la jurisprudence de la CEDH en matière de surveillance de masse montre le passage d'une attitude principalement critique et défensive à une reconnaissance de son admissibilité, à condition de respecter un ensemble strict de garanties procédurales et institutionnelles. Dans l'affaire Liberty c. Royaume-Uni (2008), la Cour sanctionne l'interception en bloc des communications externes sur la base d'un cadre vague, affirmant que l'existence même d'un tel régime porte atteinte à l'article 8. Les arrêts de la Grande Chambre Big Brother Watch c. Royaume-Uni et Centrum för Rättvisa c. Suède (2021) marquent un tournant : la Cour admet que l'interception en masse n'est pas, en soi, interdite, mais impose un ensemble de garanties « end-to-end » (base juridique détaillée, contrôle indépendant, limitation de l'accès, destruction et contrôle a posteriori), constatant des violations lorsque ces mécanismes restent insuffisants.

[2831] CEDH, 31 mai 2005, *Vetter c. France*, req. n° 59842/00, HUDOC, en ligne : ttps://hudoc.echr.coe.int/eng?i=001-97986

[2832] CEDH, 2 sept. 2010, *Uzun c. Allemagne*, req. n° 35623/05, HUDOC, en ligne : https://hudoc.echr.coe.int/eng?i=001-100293

[2833] CEDH (Gde Ch.), 4 déc. 2015, *Roman Zakharov c. Russie*, req. n° 47143/06, HUDOC, en ligne : https://hudoc.echr.coe.int/eng?i=001-159324

[2834] CEDH, 28 janv. 2003, *Peck c. Royaume-Uni*, req. n° 44647/98, HUDOC, en ligne : https://hudoc.echr.coe.int/eng?i=001-60898

Big Brother Watch marque, de manière emblématique, le passage du paradigme de la surveillance secrète classique à l'acceptation juridique de la surveillance de masse assistée par des algorithmes, à condition que des filtres et des garanties procédurales soient mis en place, acceptant ainsi l'entrée officielle dans l'imaginaire orwellien[2835]. Cette décision devient une référence indispensable dans l'analyse du rapport entre la sécurité nationale, la surveillance et le profilage de masse, la protection des données et de la vie privée, ainsi que le rôle du droit pénal dans un écosystème dominé par les infrastructures techniques et les services de renseignement. Elle souligne le fait que, même au niveau de la CEDH, l'option n'est pas l'interdiction radicale de la surveillance de masse, mais le raffinement et la sophistication des mécanismes de contrôle, ce qui alimente la question essentielle : le droit pénal et le droit procédural pénal peuvent-ils encore fonctionner comme des garanties effectives de la vie privée ou risquent-ils d'être réduits à de simples instruments de légitimation juridique de mécanismes techniques déjà consacrés ?

En 2013, Edward Snowden, spécialiste en sécurité informatique, est devenu célèbre après avoir divulgué à la presse des informations classifiées sur les programmes de surveillance de masse et de partage d'informations entre les États-Unis et le Royaume-Uni[2836]. Face au sentiment de surveillance de masse créé par ces révélations, la CEDH répond, du point de vue de la jurisprudence et des observations doctrinales, par un arrêt de plus de 200 pages[2837] dans l'affaire Big Brother Watch et autres c. Royaume-Uni, du 25 mai 2021[2838]. La Grande Chambre de la Cour européenne des droits de l'homme a constaté que le régime britannique d'interception, institué par le « Regulation of Investigatory Powers Act 2000 »,[2839] violait l'article 8 de la CEDH (droit à la vie privée) et l'article 10 de la CEDH (liberté d'expression), en raison de l'absence de garanties adéquates contre les abus. En outre, la CEDH a estimé que le régime d'accès aux données des fournisseurs de services de communication ne respectait pas les exigences de la Convention, car il n'était pas limité aux infractions graves et n'était pas

[2835] L. Laref, M. Laref (dir.), *Surveillance, op. cit.* p.342 : « il est permis de distinguer entre la surveillance exercée par Big Brother sur tout un chacun qui n'a pas l'impression d'être dans une cage et qui ne sait jamais quand, ni comment, ni pourquoi, ni par qui il peut être surveillé et la surveillance exercée par le forain de la joyeuse famille qui pourrait être tout aussi bien un maton ou un patron, sur quelqu'un qui se sait ou devrait se savoir dans une cage et qui se sait ou devrait se savoir surveillé. »

[2836] N. Younger, *The case of Edward Snowden*, NWC, 2020.

[2837] *Quand le législateur devient Big Brother, la CEDH veille-t-elle au grain ?,* AJ Pénal, 2018, p.529. Obs. sous CEDH, 13 septembre 2018, Big Brother Watch et autres c. Royaume-Uni (req. n° 24960/15, 58170/13 et 62322/14).

[2838] Case of Big Brother Watch and others v. The United Kingdom, (applications nº 58170/13, 62322/14 and 24960/15).

[2839] Regulation of Investigatory Powers Act 2000 (UK), *at* https://www.legislation.gov.uk/ukpga/2000/23/contents.

soumis à un contrôle indépendant. Initialement, l'affaire a été jugée en 2018 et la CEDH a décidé que le régime britannique violait les articles 8 et 10 de la Convention[2840].

D'autre part, l'échange d'informations avec des services étrangers (par exemple, la NSA) respecte les normes établies par la CEDH, grâce à l'existence de garanties suffisantes en matière d'examen et de stockage des données[2841].

Une marge de manœuvre décisionnelle élargie accordée aux États membres

La Cour a toutefois reconnu que l'interception de masse n'était pas, en soi, incompatible avec la Convention, les pays membres bénéficiant d'une marge de manœuvre considérable dans le choix des moyens à mettre en œuvre pour assurer la protection de leur sécurité nationale[2842]. Pour que des motifs de sécurité nationale puissent être invoqués, la Cour souligne le respect de « six exigences minimales » :

- Définition claire des infractions
- Définition des catégories de personnes pouvant être visées
- Limitation de la durée de l'interception
- Procédures claires concernant l'examen, l'utilisation et le stockage des données collectées
- Règles strictes concernant la communication et la transmission des données à des tiers
- Conditions strictes concernant la suppression ou la destruction des données[2843]

La Cour « reconnaît donc que l'interception de masse revêt une importance vitale pour les États contractants dans la détection des menaces pesant sur leur sécurité nationale »[2844].

Circonstances relatives à l'échange et à la transmission de telles informations

La Cour admet la possibilité d'échanger des informations entre États, mais précise que cet échange doit se limiter aux données collectées et conservées conformément à la Convention et être soumis à des garanties strictes : clarté du cadre juridique interne, vérification de

---

[2840] *Ibidem* : paragraphes 524-25.

[2841] Voorhoof D., *European Court of Human Rights (Grand Chamber) : Big Brother Watch and Others v. the United Kingdom, IRIS 2021-7 :1/20*, Observatoire européen de l'audiovisuel / merlin.obs.coe.int, 2021.

[2842] *European Court of Human Rights*, Big Brother Watch and Others v. the United Kingdom, Applications nº 58170/13, 62322/14 et 24960/15, *Surveillance Oversight Database*, data.guardint.org, consulté le 6 novembre 2025, paragraphe 308.

[2843] *Ibidem*, paragraphe 335. Ces règles sont également connues sous le nom de « règles Weber », d'après l'arrêt Weber et Saravia c. Allemagne (n° 54934/00, du 29 juin 2006), une autre décision essentielle de la CEDH concernant l'interception des communications à des fins de protection de la sécurité nationale. Bien que la CEDH ait validé l'interception stratégique pratiquée par l'Allemagne, elle a établi pour la première fois un ensemble de règles, c'est-à-dire des normes de base, qui sont devenues le fondement de toutes les décisions ultérieures concernant la surveillance de masse.

[2844] Case of *Big Brother Watch and others v. The United Kingdom*, (applications nº 58170/13, 62322/14 and 24960/15), paragraphe 424. Ceci a été reconnu par la Commission de Venise (European Commission for Democracy through Law). Report on the Democratic Oversight of Signals Intelligence Agencies (étude n° 719/2013), adopté lors de la 102e session plénière, Venise, 20-21 mars 2015, document CDL-AD(2015)011.

l'existence de mesures de protection adéquates dans l'État destinataire et mise en place d'un contrôle indépendant des transferts d'informations[2845]. En d'autres termes, ce n'est pas la transmission en soi qui est incriminée, mais la manière dont elle a été effectuée, qui devrait faire l'objet d'un contrôle indépendant. La protection des sources journalistiques est essentielle et tout accès des services de renseignement à des données confidentielles issues de l'activité de la presse doit être strictement contrôlé et autorisé par une autorité indépendante. En l'absence de ces garanties, dans l'affaire Big Brother Watch, une violation de l'article 10 par le Royaume-Uni a été constatée[2846]. Ainsi, certaines voix s'élèvent pour affirmer que les normes actuelles en matière d'interception ne sont pas suffisamment rigoureuses, ce qui peut réduire l'efficacité de la protection du droit à la vie privée[2847]. On parle même d'une tendance inquiétante à la normalisation de la surveillance de masse, malgré les constatations de violation dans certains cas[2848].

L'affaire Big Brother Watch et autres c. Royaume-Uni constitue la première décision de la Cour européenne des droits de l'homme relative aux programmes de surveillance de masse, établissant ainsi un précédent juridique pour les futures évaluations des systèmes d'interception[2849]. Cette décision est importante, mais insuffisante, car la norme procédurale imposée est considérée comme relativement souple[2850], n'obligeant pas l'État à démontrer de manière très stricte la nécessité de la surveillance de masse. Bien que la Cour impose des garanties procédurales, elle est critiquée pour le fait que l'accent reste mis sur les procédures et non sur l'efficacité réelle ou sur l'exigence d'une nécessité ex ante strictement vérifiée. Ainsi, le risque d'une « banalisation » de la surveillance de masse persiste[2851]. Dans cette affaire, la CEDH est critiquée, y compris par ses propres juges, pour ne pas avoir suffisamment renforcé

[2845] Case of *Big Brother Watch and others v. The United Kingdom*, (applications nº 58170/13, 62322/14 and 24960/15)., paragraphe 362.
[2846] CEDH, gr. ch., 25 mai 2021, *Big Brother Watch et autres c/ Royaume-Uni*, note : « La CEDH admet le principe de la surveillance électronique de masse », in *AJDA*, 2021, p.1060.
[2847] Turanjanin, V., *When does bulk interception of communications violate the right to privacy? The limits of the state's power and the European Court of Human Rights Approach*., Int. Cybersecur. Law Rev. 4, 2023, 115–136.2023. https://doi.org/10.1365/s43439-022-00074-7
[2848] Zalnieriūtė M., *A Dangerous Convergence : The Inevitability of Mass Surveillance in European Jurisprudence*, EJIL: Talk!, 2021.
[2849] Zalnieriute M., *Big Brother Watch and Others v. the United Kingdom*, American Journal of International Law, vol. 116(3), 2022.
[2850] Dubuisson, F., « La Cour européenne des droits de l'homme face à la surveillance de masse (obs. sous Cour eur. dr. h., Gde Ch., arrêt Big Brother Watch et autres c. Royaume-Uni, 25 mai 2021) », in *Revue trimestrielle des droits de l'Homme*, 129(1), 2022, p.123-141. https://doi.org/10.3917/rtdh.129.0123.
[2851] Parsa, S., Volcansek E., « L'impact de la protection des données sur la surveillance de masse : examen de l'arrêt Big Brother Watch et autres c. Royaume-Uni de la Cour européenne des droits de l'homme », in *DPO news*, 16(1), 2022, p.8-13. https://doi.org/10.3917/dpo.016.0008.

la protection de la vie privée, ce qui se traduit par une difficulté à trouver un équilibre stable entre la sécurité nationale et les droits fondamentaux à l'ère numérique[2852].

Quoi qu'il en soit, avant la publication de cette décision, le Royaume-Uni a adopté la nouvelle loi Investigatory Powers Act 2016 (IPA 2016), qui est entrée en vigueur en grande partie à partir de 2018, destinée à remplacer l'ancien régime basé sur la Regulation of Investigatory Powers Act 2000 (RIPA)[2853].

Dans ce contexte tumultueux, les idées exprimées par le sociologue bordelais Jacques Ellul[2854] semblent plus que jamais d'actualité : le droit ne parvient pas toujours à instaurer l'ordre qu'il est censé réaliser.

[2852] Marguénaud J.-P., « La protection de la vie privée contre l'interception en masse des communications transfrontières », in *Revue trimestrielle de droit civil* (RTD civ.), 2021, n° 04, p.843.
[2853] Voorhoof D., European Court of Human Rights : Big Brother Watch and Others v. the United Kingdom, *IRIS 2018-10 :1/1*, Observatoire européen de l'audiovisuel / merlin.obs.coe.int, 2018.
[2854] J. Ellul, *Le fondement théologique du droit*, Dalloz, coll. « Le fondement théologique du droit », n° 1, juill. 2008 p.81-82 : « Il est difficile d'imaginer le droit sans penser en même temps à l'ordre sous quelque vocable qu'on l'invoque: ordre public, sécurité, police. Nous avons tous plus ou moins la certitude que droit et ordre sont deux choses liées, et ceci est partiellement exact. Et c'est pourquoi l'ordre ne peut pas être en lui-même une valeur, pas davantage que le droit ne justifie l'ordre, car précisément le droit est toujours un instrument d'arrêt ; nous considérons l'ordre comme statique et nous ne saurions cependant dire, sans une mauvaise conscience, que cet ordre est la vérité. Comme le disait Mounier, ce n'est pas de l'ordre, c'est le désordre établi. »

Section 2. **LA SURVEILLANCE TECHNIQUE : MÉCANISMES GOUVERNEMENTAUX DE LUTTE CONTRE LA CRIMINALITÉ (FRANCE/ROUMANIE)**

§1. LA SURVEILLANCE TECHNIQUE EN DROIT FRANÇAIS

A. Passivité difficile à comprendre en France : aucune réglementation avant 1991

959. Réglementation des conversations téléphoniques. En France aussi, les choses ne sont pas faciles en matière de télésurveillance. La première réponse ferme à la réglementation légale des conversations téléphoniques se trouve relativement récemment dans la loi n° 646 de juillet 1991.

Auparavant, la France n'avait pas de législation réglementant cette forme d'intrusion dans la vie privée. Comme je l'ai indiqué plus haut, le Code de procédure pénale contenait des dispositions protégeant le domicile contre un mandat de perquisition abusif ou une confiscation injustifiée, et au niveau international, les controverses à ce sujet étaient aussi présentes que possible.

960. La passivité de la France. J'ai présenté la situation de la Grande-Bretagne et de l'Allemagne précisément afin de mettre en évidence le contexte dans lequel la France est restée dans une passivité difficile à comprendre jusqu'en 1991. Il y a eu une tentative de réglementation en 1982, lorsqu'un rapport a été préparé par les membres d'une Commission dirigée par le Président de la Cour de cassation, mais il n'a pas été concrétisé. Par la suite, Entre 1989 et 1991, la Commission pour la justice pénale et les droits de l'homme a rédigé un rapport qui discutait de la préparation des affaires pénales et à cette occasion, il a été signalé une fois de plus l'absence du texte de loi sur lequel se fonde l'activité de supervision technique des conversations téléphoniques[2855].

961. Nécessité d'éclaircissements dans le cas des écoutes téléphoniques. La CEDH a exprimé sa position sur la nécessité d'une réglementation claire et prévisible des interceptions,

[2855] « *De même, les interceptions caractéristiques peuvent procéder la police, même sur ordre des autorités judiciaires, constituant une violation du droit au respect de la vie privée qui ne trouve pas de fondement dans un texte spécifique* » pris de la page 34 du Rapport. *Le rapport préparé par la Commission de Justice Pénale et des Droits de l'Homme*, crée par le Ministre de la Justice par arrêté du 19 octobre 1988 et dirigée par le Professeur Mireille Delmas-Marty, contient une radiographie détaillée du droit pénal français de l'époque. La version complète de ce rapport peut être consultée à l'adresse suivante : https ://mafr.fr/IMG/pdf/rapport_delmsas_marty.pdf

dans l'affaire Kruslin c. France[2856] et dans l'affaire Huving c. France[2857] (les deux arrêts du 24 avril 1990). En grande partie, les questions soulevées étaient les mêmes que celles soulevées dans l'affaire Malone c. Royaume-Uni : la législation ne définit pas les catégories de personnes dont les conversations peuvent être interceptées, il n'y a aucun moyen de supprimer des documents en cas de règlement, il n'y a aucune procédure pour certifier l'intégrité des documents, le contenu du mandat d'interception, la nature des infractions pour lesquelles un mandat d'interception peut être émis ou sa durée ne sont pas réglementés.

a). Pratique judiciaire, principale source de droit

962. Jusqu'à l'introduction de la loi, la pratique judiciaire de cette période, qui semblait être la véritable source du droit, montrait ce qui suit : la durée du mandat d'interception doit être limitée dans le temps - « ne pas durer plus longtemps que nécessaire » ou « ne pas dépasser le temps nécessaire pour manifester la vérité »[2858]- la durée maximale autorisée était de 11 mois ; il s'agissait de contribuer à la preuve d'un délit qui affecte gravement l'ordre public ; les personnes surveillées ne doivent pas nécessairement être uniquement celles contre lesquelles il existe des soupçons de culpabilité, y compris les témoins dans une affaire qui pourraient être passifs ; les médias sur lesquels se trouvent les dossiers doivent être scellés, tenus à la disposition des autorités, et les interceptions transcrites peuvent être discutées en contradiction.

B. Interceptions judiciaires

963. La loi et la doctrine françaises ont identifié deux types d'écoute électronique des communications à distance : judiciaire et administratif. Les interceptions judiciaires sont celles prévues par le Code de procédure pénale et sont placées sous le contrôle du juge d'instruction[2859]

[2856] European Court of Human Rights, *Case of Kruslin v. France*, no. 11801/85, 1990. https ://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57626%22]}
[2857] European Court of Human Rights, *Case of Huvig c. France*, n° 11105/84, 1990. https ://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-55545%22]}
[2858] Cass. crim., 26 mars 1991 : Dr. pén. 1991, comm. 333, 4e arrêt.
[2859] Art. 100 Code de procédure pénale : « *En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à trois ans d'emprisonnement, le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques. Ces opérations sont effectuées sous son authorité et son contrôle* »

et les interceptions administratives sont ordonnées et surveillées par le Gouvernement, avec l'autorisation du premier Ministre[2860].

964. Différence législative entre les interceptions judiciaires et administratives. Sans prétendre à une réglementation pleinement adaptée à la réalité sociale de 1991, la loi 646 sur le secret de la correspondance transmise par les communications électroniques a résolu le problème de la différenciation des interceptions judiciaires et administratives et a passé le test des recours qui ont été formés au fil du temps à la CEDH. Il a également étendu la puissance d'un mandat à tout type de conversation à distance, pas seulement les conversations téléphoniques[2861].

Le principe général établi avait pour point de départ le contenu de l'article 8 de la Convention, le secret des conversations électroniques étant garanti par la loi, et sa violation pouvant être commise par les autorités judiciaires « dans les cas strictement nécessaires d'intérêt public, prévus par la loi et dans les limites qu'elle établit »[2862].

965. Les écoutes téléphoniques – dernier moyen de prouver les infractions. Après l'entrée en vigueur de la loi, le Code de procédure pénale a été modifié, le siège des nouvelles institutions judiciaires étant trouvé aux articles 100 à 100-7. Dans le même temps, l'autorisation du mandat doit être faite par un juge auquel toutes les données de l'enquête pénale sont mises à la disposition jusqu'alors, l'ingérence dans la vie privée étant autorisée à titre exceptionnel, pour la lutte contre la criminalité.

Dans leurs commentaires sur la loi, les avocats français[2863] ont déclaré que l'interception de conversations devrait être le dernier moyen de prouver une infraction pénale contre laquelle les autorités judiciaires doivent faire appel, parce qu'il ne s'agit pas en grande partie du délit en question et qu'il s'agit d'une forme d'intrusion dégradante et injuste dans la vie privée de l'individu.

966. Interception des conversations des avocats ou des parlementaires. Par la suite, la loi a subi des changements qui ont limité l'intrusion des interceptions dans les conversations des

[2860] Service-Public.fr, *Écoutes téléphoniques*, 2023. https ://www.service-public.fr/particuliers/vosdroits/F2515
[2861] Pradel, J. « *Un exemple de restauration de la légalité criminelle »,* Dalloz, 1992. p.49
[2862] Art. 1 paragraphe 2 de la *Loi 646/1991*
[2863] P. Chambon, « *Analyse et commentaire de la loi du 10 juillet 1991* », ALD. 1991. p.173

avocats[2864] (1993), dans les conversations des parlementaires [2865](1995) ou dans les conversations des magistrats[2866] (2004).

a). Affaire ordonnant l'interception, mais sans que des poursuites pénales soient engagées

967. Parmi les modifications pertinentes apportées au cadre juridique, je voudrais souligner[2867] que la modification de l'article 80-4 du Code de procédure pénale (2002) a étendu le champ d'application des interceptions judiciaires en cas de mort suspecte d'une personne ou en cas de disparition d'un mineur ou d'une personne aliénée, même si les poursuites pénales pour un délit spécifique n'ont pas été engagées. Cela est contraire à l'article 100 du Code de procédure pénale. La loi no 204/2004 a également apporté des modifications, en ce sens qu'il est permis d'intercepter la correspondance à l'occasion d'un délit flagrant ou d'une enquête préliminaire, bien que les dispositions de l'article 100 prévoient la possibilité d'intercepter la correspondance uniquement après le début des poursuites pénales (art. 706 à 95). Par la même loi, il est introduit dans le Code art. 74-2, qui permet le recours à des interceptions pour retrouver une personne pour laquelle un mandat d'arrêt a été délivré ou condamnée par une décision définitive.

b). Utilisation de IMSI catcher – les données du téléphone sont accessibles à distance

968. Les modifications apportées au Code de procédure pénale en 2016[2868] ont donné une importance accrue à l'utilisation de moyens techniques modernes par les autorités judiciaires, afin de prévenir et de combattre les activités spécifiques à la criminalité organisée. Ainsi, le nouveau cadre législatif « permet l'accès à la correspondance électronique stockée sans avoir

[2864]Par *la loi du 1013/24 août 1993*, le Code de procédure pénale a été réformé et l'article 100-7 a été modifié en ce sens qu'il était interdit d'intercepter le téléphone ou de perquisitionner sans en informer le doyen du barreau : « *Aucune interception ne peut avoir lieu sur une ligne dépendant du cabinet d'un avocat ou de son domicile sans que le bâtonnier en soit informé par le juge d'instruction. Les formalités prévues par le présent article sont prescrites à peine de nullité* ».

[2865] *Loi n° 95-125 du 8 février 1995 relative à l'organisation des juridictions et à la procédure civile, pénale et administrative.*

[2866] *Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité*.

[2867] Amendement déposé par la *loi n° 2002-1138 du 9 septembre 2002 d'orientation et de programmation pour la justice.*

[2868] *Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et visant l'efficacité et les garanties de la procédure pénale*.

recours au préalable à l'interception ou à la perquisition judiciaire »[2869]. Cela a permis l'utilisation d'un dispositif informatique[2870] appelé IMSI-Catcher[2871], qui a la capacité d'intercepter la correspondance ou de visualiser les données qui sont déjà stockées sur un courrier ou des applications de messagerie. Parce qu'il s'agit d'une mesure extrêmement radicale et intrusive, l'autorisation d'interception peut être délivrée pour une durée de 48 heures et ne peut être prolongée qu'une seule fois. Ces mesures de surveillance sont « subordonnées aux besoins de l'enquête ou de la formation et doivent être autorisées par des ordonnances motivées émises par le juge des libertés (pour l'instruction) ou le juge d'instruction (pour la procédure judiciaire) »[2872].

c). Les agents pénitentiaires pouvaient effectuer une surveillance technique

969. Actualités pour prévenir la criminalité organisée. La modification du Code de procédure pénale de 2016 en a apporté un nouveau, accordant aux agents pénitentiaires le droit de procéder à une surveillance technique similaire à celle décrite ci-dessus, y compris l'utilisation du dispositif IMS-Catcher pour collecter le trafic Internet, l'identification de l'opérateur mobile, interception de conversations téléphoniques en prison ou accès à distance aux appareils utilisés par les personnes incarcérées[2873].

L'objectif est de lutter contre le phénomène de la radicalisation dans les prisons et de prévenir la criminalité organisée. L'article 721-1[2874] du Code de procédure pénale a été modifié

[2869] F. Chopin, «*Cybercriminalité — Responsabilité pénale des fournisseurs de contenu*», Répertoire de droit pénal et de procédure pénale, Dalloz, 2020 (actualisation mars 2024).

[2870] Art. 106-95-1 Code de procédure pénale : « *Si les nécessités de l'enquête relative à un crime ou à l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 l'exigent, le juge des libertés et de la détention peut, à la requête du procureur de la République, autoriser par ordonnance motivée l'accès, à distance et à l'insu de la personne visée, aux correspondances stockées par la voie des communications électroniques accessibles au moyen d'un identifiant informatique. Les données auxquelles il a été permis d'accéder peuvent être saisies et enregistrées ou copiées sur tout support* ».

[2871] Ce dispositif a parmi ses fonctionnalités la possibilité de révéler l'identité de l'abonné d'un opérateur mobile s'il se trouve à une courte distance du téléphone de la personne concernée ou s'il peut intercepter le trafic de données mobiles comme s'il agissait comme un clone du téléphone ou de tout autre système ordinateur. L'IMSI-Catcher peut également trouver le code IMEI (identité internationale des équipements mobiles) d'un appareil à proximité.

[2872] F. Chopin, op. cit.

[2873] P. Beauvais, D. Chilstein, E. Dreyer (dir.), *Le droit pénal de l'avenir*, Paris, Dalloz, 2024. p.211: « *Dans sa version en vigueur en 2016, l'article 727-1 du Code de procédure pénale autorisait les agents pénitentiaires à accomplir, afin de prévenir les évasions et d'assurer la sécurité et l'ordre dans les prisons ou dans les établissements médicaux destinés aux personnes incarcérées, une série de mesures de surveillance analogues à celles de la sécurité intérieure*».

[2874] « *Conformément aux dispositions de l'article L. 223-2 du code pénitentiaire, le procureur de la République est immédiatement avisé de la découverte, au sein d'un établissement pénitentiaire ou d'un établissement de santé destiné à recevoir des personnes détenues, de tout équipement terminal, système informatique ou support de données informatiques dont la détention est illicite.*

le 30 mars 2022 en ce sens que tous les pouvoirs qui permettaient aux agents pénitentiaires d'exercer un contrôle technique dans des conditions similaires à celles des organes judiciaires ont été supprimés[2875].

d). Principes régissant les interceptions judiciaires

La procédure est écrite et définitive. Conformément à l'article 100 du Code de procédure pénale, la procédure d'obtention d'un mandat d'interception de correspondance transportée par voie électronique, en matière pénale et pénitentiaire, est éminemment écrite et ne peut faire l'objet d'aucun recours. Étant donné que la procédure est secrète, le procureur serait le seul à avoir un motif hypothétique de contestation, mais ce fait n'est pas prévu par la loi.

970. Nature du délit. Le mandat peut être intercepté si la peine encourue pour l'acte faisant l'objet de poursuites pénales est de trois ans ou plus. La version originale de l'article 100 prévoyait que la peine devait être de deux ans ou plus. En ce qui concerne cette base juridique, aucune autre précision n'est apportée quant à la nature de l'infraction, la gravité étant évaluée en fonction du montant de la peine.

Dans les conditions prévues par les dispositions du même article, le procureur de la République peut autoriser l'administration pénitentiaire à conserver ces matériels », contenu modifié par l'Ordonnance du 30 mars 2022, en vigueur au moment de la rédaction du présent document.

[2875] Voici quelques exemples tirés du contenu de l'article 727-1 de la version en vigueur avant l'amendement : «*Sous le contrôle du procureur de la République territorialement compétent et aux fins de prévenir les évasions et d'assurer la sécurité et le bon ordre des établissements pénitentiaires ou des établissements de santé destinés à recevoir des personnes détenues, les agents individuellement désignés et habilités appartenant à l'administration pénitentiaire peuvent être autorisés à* :

1° «*Recueillir auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne détenue, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications»*;

2° «*Recueillir directement, au moyen d'un appareil ou d'un dispositif technique mentionné au 1° de l'article 226-3 du code pénal, les données techniques de connexion permettant l'identification d'un équipement terminal utilisé en détention ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés»;*

3° «Intercepter, enregistrer, transcrire ou interrompre des correspondances de personnes détenues émises par la voie des communications électroniques, à l'exception de celles avec leur avocat à raison de l'exercice de sa fonction»;

5° «Accéder à distance et à l'insu de la personne détenue visée aux correspondances stockées, émises par la voie des communications électroniques, accessibles au moyen d'un identifiant informatique, les enregistrer, les conserver et les transmettre».

Exceptionnellement, le juge peut autoriser l'interception de communications si la victime d'une infraction pénale le demande, la condition essentielle étant que la peine prévue pour l'infraction recherchée soit l'emprisonnement. Un seuil minimal de peine n'est plus imposé lorsque la victime demande l'interception de ses communications[2876].

La disposition générale de l'article 100 est complétée par l'incidence des articles 706-73 et 706-95-1, qui concernent la criminalité organisée, le trafic de stupéfiants, la contrefaçon de monnaie, l'entrée et le séjour irréguliers d'un étranger en France, le proxénétisme, la tromperie grave, les crimes commis par l'usage d'armes, etc.

971. La procédure n'est pas rendue publique. L'analyse du dossier, des éléments de preuve sur lesquels se fonde la demande de délivrance du mandat, se fait dans le cadre d'une procédure totalement non publique. Compte tenu de la nature spécifique de la demande, si l'intéressé connaissait la décision du juge, l'exécution d'un tel mandat serait totalement dénuée de sens. La pratique française a montré que les interceptions peuvent être autorisées non seulement contre le suspect, mais aussi intercepter des personnes qui ne sont pas encore identifiées[2877].

e). Durée du mandat et motivation des décisions

972. Durée du mandat La durée du mandat d'interception ne dépasse pas quatre mois. Il peut être prorogé dans des conditions similaires à celles qui sous-tendent l'arrangement, mais sans que la durée totale ne dépasse un an. Si les infractions concernées sont celles visées à l'article 706-73 (spécifique à la criminalité organisée), la durée totale peut atteindre deux ans[2878].

973. Motivation des décisions. Tant les raisons de la prise de la mesure d'interception que sa prorogation imposent au juge d'instruction l'obligation de motiver les faits et les éléments juridiques présentés par l'accusation. La littérature juridique précise que : « pour satisfaire à ces

---

[2876] Art. 100, paragraphe 3 : «*En cas de délit puni d'une peine d'emprisonnement commis par la voie des communications électroniques sur la ligne de la victime, l'interception peut également être autorisée, selon les mêmes modalités, si elle intervient sur cette ligne à la demande de la victime*».

[2877] C. Guéry, *«Instruction préparatoire — Saisie du juge d'instruction*», Répertoire de droit pénal et de procédure pénale, Dalloz, 2018. (actualisation octobre 2024): «*L'écoute peut être effectuée à l'insu des personnes intéressées, qui ne sont pas seulement celles sur qui pèsent des indices de culpabilité : il ne peut être reproché au juge de n'avoir pas spécifié les numéros de ligne dès lors que l'information ouverte contre X ne le permettait pas et alors que seuls les bars susceptibles de recevoir des paris clandestins ont été surveillés (Crim. 9 déc. 1991, no 90-84,994, Bull. crim. no 465 ; D. 1992. IR 7) ».*

[2878] Art. 100-2 Code de procédure pénale : « *Cette décision est prise pour une durée maximale de quatre mois. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée, sans que la durée totale de l'intervention puisse excéder un an ou, s'il s'agit d'une infraction prévue aux articles 706-73 et 706-73-1, deux ans* ».

exigences, le juge d'instruction doit, par un raisonnement concret en rapport avec les circonstances de l'affaire, préciser l'objet de la mesure. Cette motivation peut être complétée par l'inclusion dans l'autorisation d'une ou plusieurs parties spécifiques du régime. » [2879]

La pratique judiciaire récente a également été assez catégorique en ce qui concerne les situations de sanction où les motifs de la décision délivrant le mandat d'interception font défaut, montrant que « le juge d'instruction doit préciser, par un raisonnement concret sur les circonstances de l'affaire, l'objet de la mesure » et, dans le même temps, « l'absence d'une telle motivation, qui interdit tout contrôle effectif et effectif de la mesure, porte nécessairement atteinte aux intérêts de la personne concernée »[2880]

C. Interceptions administratives

a). Première attestation légale : le 28 mars 1968

974. L'origine juridique de ce type d'écoute électronique des conversations par communication à distance découle d'une décision du premier ministre français du 28 mars 1960, qui a créé le groupement interministériel de Contrôle (GIC)[2881]. Premièrement, il[2882] s'agissait d'une décision classifiée, qui visait également à renforcer le pouvoir du premier ministre sur les services de renseignement. Pour surveiller l'activité d'interception, des mécanismes de contrôle ont été créés qui fonctionnent encore aujourd'hui, à savoir : (1) centralisation des interceptions administratives – le lien direct entre les services de renseignement et les opérateurs de communication est interdit, et le nombre de demandes et la quantité de données obtenues ont été centralisés en un seul endroit ; (2) traçabilité de la mise en œuvre des interceptions – le parcours d'une demande d'interception peut être tracé à partir du moment de son initiation (qui l'a proposée, qui l'a autorisée, qui l'a mise en exécution) jusqu'à l'obtention du résultat.

[2879] F. Chopin, «*Cybercriminalité — Responsabilité pénale des fournisseurs de contenu*», Répertoire de droit pénal et de procédure pénale, Dalloz, 2020 (actualisation 2024).

[2880] Cour de cassation, Chambre pénale, *11 juin 2024 – N° 23-85.632*. La décision du tribunal peut être consultée en entier ici : https ://www-lexis360intelligence-fr.docelec.u-bordeaux.fr/document/JP_KODCASS-0519211_0KRH?doc_type=jurisprudence_courcassation&source_nav=EN_KEJC-172406_0KSJ&source=renvoi#mark_20

[2881] De plus amples informations sur cette Commission, qui fonctionne encore aujourd'hui selon une formule modifiée, peuvent être trouvées ici : https ://cf2r.org/travailler-dans-le-renseignement/au-service-de-letat/services-du-premier-ministre/groupement-interministeriel-de-controle/

[2882] En 1992, il a été déclassifié.

b). Les interceptions traditionnelles ne remplissent plus leur objectif

975. La loi n° 646/1991 sur le secret de la correspondance transmise par voie électronique a conduit à la création de la Commission nationale de contrôle des interceptions de sécurité (CNCIS)[2883], organisme indépendant chargé de surveiller l'activité d'interception. Cet organisme a fonctionné jusqu'en 2015, date à laquelle le législateur français a dû adapter sa législation aux nouvelles réalités numériques, avec pour résultat la promulgation de la loi du 24 juillet 2015 sur l'information[2884].

Dans la pratique, le nouveau cadre législatif met à jour les interceptions administratives face aux défis actuels qui n'existaient pas en 1991 : Le contexte est complètement numérisé, les interceptions traditionnelles n'ont pas rempli leur but, une surveillance stratégique impliquant une collecte massive de données a déjà été effectuée par les États-Unis, l'accès aux données doit être réalisé beaucoup plus rapidement, la criminalité a changé ses caractéristiques, etc.

La réglementation préexistante était complètement dépassée et une approche moderne était nécessaire pour « sécuriser juridiquement l'action des services impliqués, qui jusqu'alors avaient été maintenus sous une forme clandestine », a déclaré le communiqué, incompatible avec l'état de droit et les besoins de protection que leurs agents et fonctionnaires étaient en droit d'attendre de la loi. »[2885]

976. **Nouvelles autorités administratives**. Le CNCIS a été remplacé par un nouvel organe, la Commission nationale de contrôle du renseignement technique (CNCTR), qui a renforcé les pouvoirs en termes de contrôle de l'interception des activités de communication menées par les services de renseignement. Ce comité approuve toutes les demandes d'utilisation de la technologie de l'information par les services spécialisés.

c). Données statistiques sur les interceptions administratives en 2023

Afin d'élaborer ce document, nous avons demandé des données statistiques officielles à la CNCTR et nous avons pu constater que ces dernières années, les chiffres de surveillance effectués par les services de renseignement sont sur une tendance à la hausse.

[2883] *Écoutes téléphoniques P Bouchet,* Institut Paul Bouchet, 1995.

[2884] *Loi n° 2015-912 du 24 juillet 2015 relative au renseignement*. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899

[2885] Commission nationale de contrôle des techniques de renseignement (CNCTR), « *Bref historique* ». https://www.cnctr.fr/en/bref-historique.

977. Le nombre de demandes d'interception en hausse. Selon le rapport d'activité pour 2023, le nombre de demandes de techniques d'information utilisées était de 94 902, soit une augmentation de 6 % par rapport à 2022 et de 29 % par rapport à 2019.

La réglementation de ces techniques d'information se trouve dans le Code de sécurité intérieure (CSI)[2886] et celles-ci peuvent être : l'accès aux métadonnées, la capture d'images et de sons, l'entrée dans des espaces privés pour installer ou entretenir des équipements de surveillance, Capture de données informatiques en cassant les mots de passe ou en capturant en temps réel à partir de l'écran de l'utilisateur, en utilisant IMSI-Catcher pour identifier et localiser les téléphones mobiles, interception de communications en temps réel ou hors ligne.

978. Avec le titre par exemple, nous présentons les chiffres suivants sur l'utilisation concrète des techniques d'information : différents temps d'accès aux données de connexion - 33 657 requêtes (c'est l'identification du numéro d'abonnement téléphonique et du titulaire) ; accès aux factures détaillées des abonnés - 21 430 requêtes ; Accès en temps réel aux données de connexion[2887] - 763 requêtes ; géolocalisation en temps réel[2888] : 10,982 requêtes, soit une hausse de 44 % par rapport à 2019 ; interceptions de sécurité par GIC[2889] - 13 021 requêtes ; utilisation du *récepteur IMSI* pour la collecte de données privées : 607 demandes ; entrée dans des lieux privés pour l'installation ou l'entretien de matériel de surveillance : 4053 demandes.

979. Plus de 20.000 personnes suivies en 2023. En ce qui concerne le nombre de personnes surveillées, la CNCTR affirme dans le rapport[2890] qu'il est de 24 209. Sur ce nombre, 6 962 ont fait l'objet d'une surveillance pour la prévention du terrorisme (en baisse de 10 % par rapport à 2019), 7 058 pour la prévention de la criminalité organisée et 2 551 personnes ont fait l'objet

---

[2886] *Code de la sécurité intérieure.* https ://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000025504917/

[2887] Ce type d'accès en temps réel est basé sur choisi L851-2 du Code de la Sécurité intérieure : « *Sous réserve des conditions prévues au titre II, chapitre I, du présent code et exclusivement pour les besoins de la prévention du terrorisme, la collecte en temps réel peut être autorisée sur les réseaux d'opérateurs et de personnes visés à l'article L. 851-1, les informations ou documents visés à l'article L. 851-1, relatifs à une personne préalablement identifiée comme susceptible d'être liée à une menace, ainsi que les adresses complètes des ressources internet utilisées par cette personne. Lorsqu'il existe des raisons sérieuses de croire qu'une ou plusieurs personnes de l'entourage de la personne concernée par l'autorisation pourraient fournir des informations utiles aux fins de l'autorisation, cette autorisation peut également être accordée individuellement à chacune de ces personnes* ».

[2888] Art. L851-4 : « *Sous réserve des conditions prévues au titre II, chapitre I, du présent code, les données techniques relatives à la localisation des équipements terminaux utilisés, visées à l'article L. 851-1, peuvent être collectées à la demande du réseau et transmises en temps réel par les opérateurs à un service du Premier Ministre* ».

[2889] Le groupement interministériel de Contrôle est un organe placé sous la direction du Premier Ministre et assure une supervision indépendante des demandes de techniques d'information demandées par les Ministres de l'intérieur, de la Défense, des Finances et de la Justice. Il traite également de la centralisation des données collectées par les services de renseignement, en s'appuyant sur des spécialistes informatiques hautement qualifiés qui « *conçoivent, développent, mettent en œuvre et gèrent des systèmes d'information sécurisés utilisant les dernières technologies de traitement des données numériques et d'intelligence artificielle*». https ://www.sgdsn.gouv.fr/notre-organization/composantes/groupement-interministeriel-de-controle

[2890] CNCTR, *8e Rapport d'activité*, 2023. https ://cms.cnctr.fr/uploads/CNCTR_Rapport_2023_VERSION_NUMERIQUE_b1cd8eda21.pdf

d'une surveillance au[2891] titre des dispositions de l'article 811-3, point 5 (« attaques contre la forme républicaine des institutions »), "violences collectives susceptibles de porter gravement atteinte à l'ordre public" ou d'empêcher le rétablissement de groupes dissouts de milices militaires ou civiles). Pour le reste des personnes surveillées, des données sur les motifs de cette action sont fournies.

d). CNCTR : les conversations des personnes sont collectées sans autorisation préalable

980. Irrégularités signalées par la CNCTR. Dans le même rapport, la Commission montre également qu'il existe des zones grises (p. 90 du rapport) de l'intrusion des services secrets dans la vie privée des individus, et que celles-ci devraient être couvertes par une meilleure législation, y compris adaptée aux nouveaux défis posés par le développement numérique. Le rapport conclut que les services de renseignement « ont fait des efforts considérables pour assurer le respect de la loi dans l'utilisation de ces techniques. Toutefois, ces efforts n'ont pas permis de prévenir toutes les irrégularités, dont certaines sont récurrentes. Les irrégularités les plus sensibles sont celles liées aux méthodes d'application des techniques, par exemple, le non-respect du champ d'application, la collecte de conversations de personnes dont la supervision n'a pas été autorisée. »

Au lieu de cela, la CNCTR affirme avoir été en mesure de mettre en œuvre un algorithme capable de prouver les menaces terroristes[2892] et, d'ici 2027, elle rendra opérationnel un dispositif capable de contrôler de grands flux de données.

[2891] Art. 811-3 du Code de sécurité intérieure :
« *Pour l'exercice exclusif de leurs missions respectives, les services de renseignement spécialisés peuvent utiliser les techniques visées au titre V du présent code pour la collecte d'informations relatives à la défense et à la promotion des intérêts fondamentaux de la Nation, comme suit :*

1. *Indépendance nationale, intégrité territoriale et défense nationale ;*
2. *Les intérêts majeurs de la politique étrangère, le respect des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;*
3. *Les principaux intérêts économiques, industriels et scientifiques de la France ;*
4. *Prévention du terrorisme ;*
5. *Prévention :*
   a) attaques contre la forme républicaine des institutions ;
   b) les actions visant à maintenir ou à reconstituer des groupes dissous conformément à l'article L. 212-1 ;
   c) les violences collectives susceptibles de porter gravement atteinte à la paix publique ;
6. *Prévention de la criminalité organisée et de la criminalité ;*
7. *Prévention de la prolifération des armes de destruction massive ».*

[2892] « *En 2023, une nouvelle autorisation a été accordée pour mettre en œuvre un algorithme conçu pour détecter les connexions susceptibles de révéler une menace terroriste. Ainsi, le nombre total d'algorithmes autorisés a atteint cinq depuis l'introduction de cette technique pour les services de renseignement en 2015. Cette augmentation de la surveillance a été réalisée dans le respect de la loi : le nombre d'avis défavorables émis par la Commission pour des demandes de surveillance a diminué de 20 % (775 avis défavorables contre 974 en 2022) pour l'ensemble des techniques combinées, par rapport à 2022*».

§2. LA SURVEILLANCE TECHNIQUE EN DROIT ROUMAIN. UNE MENACE POUR LA VIE PRIVÉE ?

981. Adaptation. Au cours des quatre dernières décennies, l'accélération technologique — depuis les débuts de la téléphonie mobile et les premiers réseaux Internet (années 1980-1990) jusqu'aux plateformes de réseaux sociaux et aux applications basées sur l'intelligence artificielle — a remodelé la structure et le mode opératoire de la criminalité. En conséquence, le droit pénal matériel a intégré de nouvelles infractions intrinsèquement liées à l'environnement numérique, et le droit pénal procédural a été recalibré pour permettre la découverte et l'administration des preuves dans ce type d'affaires. C'est précisément dans ce contexte que certaines procédures spéciales[2893] innovantes ont été créées, parmi lesquelles la surveillance technique, une procédure qui empiète fortement sur la vie privée. Cette mesure est soumise au principe de nécessité, de subsidiarité et de proportionnalité, ainsi qu'à un contrôle judiciaire effectif.

A. Méthodes spéciales de surveillance

982. Définition. En ce qui concerne les mesures de surveillance technique, nous précisons que le fondement juridique est constitué par les articles 138 à 145[1] du Code de procédure pénale. L'article 138, paragraphe 1, énumère de manière restrictive les méthodes spéciales de

[2893] En anticipant légèrement le sujet, nous précisons que l'actuel Code de procédure pénale a repris de l'ancien Code de procédure pénale (publié initialement au Journal officiel n° 145-146 du 12 novembre 1968 et republié au Journal officiel n° 78 du 30 avril 1997) certaines procédures probatoires, telles que l'interception des communications, le recours à des enquêteurs sous couverture, la localisation ou la surveillance par des moyens techniques, etc. D'autre part, d'autres méthodes spéciales nouvelles, reprises de lois spéciales, ont été introduites. Par exemple, l'accès à un système informatique a été repris de l'article 27 de la loi n° 78/2000 relative à la prévention, la détection et la répression des actes de corruption, ainsi que d'autres lois : l'article 23 de la loi n° 143/2000 relative à la prévention et à la lutte contre le trafic et la consommation illicite de stupéfiants, l'article 23 de la loi n° 678/2001 relative à la prévention et à la lutte contre la traite des êtres humains, l'article 15 de la loi n° 39/2003 relative à la prévention et à la lutte contre la criminalité organisée, etc. De même, l'accès aux systèmes de communication/télécommunication a également été repris à partir des mêmes lois : article 27 de la loi n° 78/2000, article 23 de la loi n° 143/2000, article 23 de la loi n° 678/2001, article 15 de la loi n° 39/2003. On retrouve la même situation dans le cas du recours à des enquêteurs sous couverture, à des collaborateurs, à des livraisons surveillées et à l'obtention de données relatives aux transactions financières d'une personne, prévues dans diverses lois, telles que celles mentionnées ci-dessus : loi n° 78/2000, loi n° 143/2000, loi n° 39/2003, etc.

surveillance, respectivement d'enquête[2894], qui ne sont pas exemptes de controverses[2895]. Parmi celles-ci, celles prévues aux points a) à d) sont pertinentes, car il s'agit concrètement de mesures de surveillance technique, comme il ressort expressément des dispositions du paragraphe 13 de l'article 138 du CPP. Ainsi, par « surveillance technique », nous entendons l'utilisation d'une ou plusieurs des méthodes spéciales de surveillance/enquête suivantes : a) l'interception des communications ou de tout type de communication à distance ; b) l'accès à un système informatique ; c) la surveillance vidéo, audio ou par photographie ; d) la localisation ou la poursuite par des moyens techniques.

983. Conditions. Comme nous le verrons ci-après, les mesures de surveillance technique portent atteinte aux droits et libertés fondamentaux, en particulier au droit à la vie privée[2896] de la personne et, pour cette raison, leur adoption est, en principe, réservée au juge des droits et des libertés, conformément à l'article 139, paragraphe (1) du CPP. En outre, compte tenu de la restriction grave du droit à la vie privée, la loi impose également le respect cumulatif de plusieurs conditions, régies par l'article 139, paragraphes (1) et (2), à savoir :

[2894] Ainsi, nous soulignons la nécessité d'établir une distinction entre les méthodes de surveillance et celles d'enquête. Comme l'indique la doctrine (A. Crișu, *Drept procesual penal. Partea generală*, 6e éd., Ed. Hamangiu, Bucarest, 2022, p. 389 ; A. Boroi, G. Negruț, *Drept procesual penal*, 3e éd., Ed. Hamangiu, Bucarest, 2022, p. 257-258), la différence évidente entre les deux catégories de mesures – de surveillance et d'enquête – réside dans le moment où elles sont mises en œuvre. Ainsi, les méthodes de surveillance sont mises en œuvre en temps réel, c'est-à-dire pendant la période où se déroulent les activités faisant l'objet de la procédure. En revanche, les méthodes d'enquête sont mises en œuvre après le déroulement des activités.

[2895] Ainsi, la doctrine n'est pas parvenue à un consensus quant à la classification des méthodes en méthodes de surveillance et méthodes d'enquête. Ainsi, un auteur (A. Crișu, *op. cit.*, p. 389) considère que les procédures prévues à l'article 138, paragraphe (1), points a) à e) du CPP sont des méthodes de surveillance, tandis que les autres - points f) à j) - sont des méthodes spéciales d'enquête. En revanche, d'autres auteurs (A. Boroi, G. Negruț, *op. cit.*, p. 257 ; G.G. Teodoru, I.-P. Chiș, *Tratat de Drept procesual penal*, 4e éd., Ed. Hamangiu, Bucarest, 2020, p. 446 ; M. Udroiu, *Procedură penală. Partea generală*, 4e éd., Ed. C.H. Beck, Bucarest, 2017, p. 414), dont nous partageons l'avis, considèrent que les points a) à d) régissent des méthodes spéciales de surveillance, tandis que les autres points, y compris le point e), concernent les méthodes d'enquête.

[2896] Comme le souligne un auteur (A. Crișu, *op. cit.*, p. 387-388), la réglementation de ces méthodes qui permettent l'utilisation de techniques qui, par leur nature, portent atteinte à la vie privée et, implicitement, la violent, nécessite certaines garanties afin d'assurer une protection adéquate de ce droit. À cet égard, on invoque l'article 8, paragraphe (1), de la Convention européenne des droits de l'homme : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ». Toutefois, il est souligné que, dans certaines situations, l'ingérence de l'État et des autorités dans la vie privée d'une personne peut parfois être nécessaire dans une société démocratique (par exemple, pour défendre la sécurité nationale, l'ordre public etc.), ce qui justifie l'existence de telles méthodes. Ainsi, le paragraphe (2) de l'article 8 de la CEDH est mis en discussion : « *L'ingérence d'une autorité publique dans l'exercice de ce droit (n.n. concernant le droit au respect de la vie privée et familiale) n'est admissible que dans la mesure où cette ingérence est prévue par la loi et constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui* ». Dans ce contexte, l'auteur cité indique que, dès lors que « *l'ingérence dans leur exercice est autorisée, les droits prévus à l'article 8 de la Convention font partie de la catégorie des droits conditionnels, et pour que l'ingérence soit conforme aux dispositions de celle-ci, elle doit remplir les conditions suivantes : être prévue par la loi, poursuivre un but légitime, apparaître comme nécessaire dans une société démocratique et être proportionnée au but poursuivi* ».

- l'existence d'un soupçon raisonnable[2897] quant à la préparation ou à la commission d'une infraction prévue à l'article 139, paragraphe (2) du CPP[2898] ;

- la proportionnalité de la mesure de surveillance technique par rapport à la restriction des droits et libertés fondamentaux, compte tenu de plusieurs circonstances (les particularités de l'affaire, l'importance des informations ou des preuves qui seraient obtenues par la surveillance technique ou, éventuellement, la gravité de l'infraction)[2899] ;

- l'impossibilité d'obtenir les preuves par tout autre moyen ou, même si les preuves pourraient être obtenues par d'autres moyens, les preuves seraient obtenues avec des difficultés particulières et importantes qui porteraient préjudice à l'enquête (en d'autres termes, elles porteraient atteinte au bon déroulement de la procédure pénale) ou il existe un danger pour la sécurité des personnes ou des biens de valeur[2900] ;

- la mise en place d'une surveillance technique pour la commission de certaines infractions, notamment celles contre la sécurité nationale, le trafic de drogue, le terrorisme, le viol, le chantage etc. ou pour toute autre infraction dont la peine prévue par la loi est de 5 ans d'emprisonnement ou plus.

984. Proportionnalité. Par conséquent, la surveillance technique doit respecter le principe de proportionnalité, en mettant en balance la vie privée de la personne et la nécessité des mesures de surveillance technique pour le bon déroulement de la procédure pénale, de manière à ne pas porter atteinte au droit à la vie privée pour des questions mineures. Dans ce contexte, la proportionnalité impose le choix d'une méthode de surveillance appropriée et la prise en compte de plusieurs éléments expressément prévus par la loi : les particularités de l'affaire[2901], l'importance des informations ou des preuves à obtenir[2902] et la gravité de l'infraction[2903]. Nous précisons que, lorsque nous faisons référence à la gravité de l'infraction dans le contexte de la

---

[2897] T.V. Gheorghe, *Aflarea adevărului, principiu fundamental al procesului penal*, Ed. Hamangiu, Bucarest, 2021, p. 266.
[2898] B. Micu, R. Slăvoiu, A. Zarafiu, *Procedură penală*, 2e éd., Ed. Hamangiu, Bucarest 2024, p. 211.
[2899] *Idem*, p. 223-224.
[2900] C.S. Paraschiv, *Drept Procesual Penal. Curs pentru Master*, Éditions Hamangiu, Bucarest, 2024, p.81.
[2901] Par « particularités de l'affaire », nous faisons référence à la manière concrète dont l'acte a été commis ou est sur le point d'être commis. Par exemple, de ce point de vue, la proportionnalité de la surveillance technique serait respectée si, par exemple, l'acte pour lequel la poursuite pénale a été engagée est un délit informatique ou commis dans l'environnement numérique.
[2902] Lorsque nous faisons référence à l'importance des informations ou des preuves à obtenir, nous parlons essentiellement d'une anticipation de l'utilité, de la pertinence et de la force probante de la preuve que l'on cherche à obtenir en recourant à la procédure spéciale.
[2903] Comme l'indique la doctrine (B. Micu, R. Slavoiu, A. Zarafiu, *Procedură penală*, 2e éd., Ed. Hamangiu, Bucarest 2024, p. 224), il ne faut pas confondre la gravité de l'infraction et sa nature. « La loi considère la gravité de l'infraction comme une condition d'appréciation de la proportionnalité de la procédure probatoire, tandis que la condition relative à la présence de l'infraction parmi celles expressément énumérées à l'article 139, paragraphe (2) du Code de procédure pénale est une condition d'admissibilité ». Ainsi, il apparaît qu'il est possible que l'infraction faisant l'objet de poursuites pénales fasse partie de celles pour lesquelles la surveillance technique est autorisée, sans que celle-ci soit d'une gravité telle qu'elle nécessite une telle mesure.

proportionnalité, nous nous référons à son degré de dangerosité sociale concrète, et non abstraite, exprimé dans les limites des peines prévues par la loi.

985. Subsidiarité. Outre son caractère proportionné, la surveillance technique doit également être subsidiaire[2904] par rapport aux autres moyens de preuve pouvant être utilisés dans l'affaire, de sorte que les méthodes de surveillance technique s'utilisent comme *ultima ratio*, c'est-à-dire uniquement lorsque : 1. les preuves ne peuvent être obtenues d'une autre manière ou leur obtention présenterait des difficultés particulières qui compromettraient l'enquête ; 2. il existe un danger pour la sécurité des personnes ou des biens de valeur. En d'autres termes, la subsidiarité implique que les méthodes de surveillance technique soient utilisées lorsqu'elles sont les seules raisonnablement aptes à permettre l'obtention de preuves, mais aussi lorsque, même si elles ne sont pas les seules, l'utilisation d'autres moyens de preuve moins intrusifs dans la vie privée entraînerait des dangers pour la sécurité des personnes ou des biens de valeur[2905].

a). Mandats de surveillance obtenus avant le changement de cadre juridique

986. Controverses. Une question controversée dans la littérature juridique concerne l'hypothèse dans laquelle, après avoir autorisé la surveillance technique, l'autorité chargée des poursuites pénales procède à un changement de cadre juridique en une infraction qui ne relève pas des infractions mentionnées à l'article 139, paragraphe (2), du Code de procédure pénale. La question suivante se pose donc : les preuves obtenues par des moyens de surveillance technique peuvent-elles encore être utilisées dans l'affaire ou doivent-elles être exclues si le cadre juridique est modifié par la suite ?

987. Exclusion. Dans ce contexte, deux opinions se dégagent. Dans une première perspective[2906], on considère qu'il est nécessaire d'exclure les preuves obtenues, en raison du

[2904] T.V. Gheorghe, *op. cit*., p. 257.

[2905] En ce qui concerne la première hypothèse (les preuves ne pourraient être obtenues d'une autre manière ou leur obtention entraînerait des difficultés particulières qui nuiraient à l'enquête), nous soulignons qu'il n'existe pas de critères juridiques (comme c'est le cas pour la proportionnalité) permettant d'expliquer les « difficultés particulières », celles-ci devant être déterminées au cas par cas. Toutefois, la surveillance technique pourrait être refusée par le juge lorsqu'il constate que les mêmes preuves pourraient être fournies par un moyen non intrusif. En ce qui concerne la deuxième hypothèse (il existe un danger pour la sécurité des personnes ou des biens de valeur), il convient de noter que la nécessité de la surveillance technique ne réside pas dans l'impossibilité/la difficulté d'obtenir des preuves, mais plutôt dans le fait que l'utilisation d'autres moyens moins intrusifs nécessiterait un temps d'enquête plus long, ce qui pourrait entraîner certains risques pour la vie, l'intégrité physique ou la santé d'une personne ou pour la sécurité de biens de valeur. Dans ce cas également, nous soulignons que la loi ne fournit pas de repères pour comprendre l'expression « biens de valeur », cet aspect étant laissé à l'appréciation du juge qui examine l'opportunité d'ordonner la surveillance technique.

[2906] Dans ce sens, voir T.-V. Gheorghe, A.S. Uzlău, C.M. Chirița, dans N. Volonciu, A.S. Uzlău, R. Moroșanu, V. Văduva, D. Atasiei, C. Ghigheci, L.E. Holmanu, I.D. Samoilă, C. Voicu, G. Anghel-Tudor, T.-V. Gheorghe, C.M.

changement de cadre juridique d'une infraction prévue à l'article 139, paragraphe (2), en une infraction qui n'est plus prévue par cette disposition légale. La raison principale réside dans le fait que la loi a expressément prévu certaines conditions restrictives précisément afin de protéger la vie privée d'une personne. Or, dès lors qu'une situation empêchant le respect des conditions légales nécessaires à la mise en place de mesures de surveillance technique est survenue, les preuves obtenues antérieurement doivent être exclues. Dans le cas contraire, si les preuves pouvaient encore être utilisées après le changement de cadre juridique en une infraction non prévue par l'article 139, paragraphe (2), du CPP, les dispositions légales seraient contournées[2907].

988. Un argument supplémentaire à l'appui de ce point de vue, mis en évidence par la doctrine[2908], montre que la sanction d'exclusion des preuves repose sur le principe de causalité objective et non subjective. Par conséquent, que l'illégalité ait été ou non causée par la faute de l'autorité judiciaire, il suffit de démontrer que la preuve a été obtenue de manière illégale[2909].

989. **Utilisation légale.** Dans le deuxième avis, il est estimé que, malgré le changement de cadre juridique d'une infraction prévue à l'article 139, paragraphe (2), en une infraction qui n'est plus prévue par cette disposition, les preuves obtenues ne doivent pas être exclues, mais peuvent continuer à être utilisées[2910]. La justification réside dans le fait que l'admissibilité des mesures de surveillance technique est évaluée à la lumière de la situation au moment de l'autorisation,

---

Chirița, T. Manea, C. Marin, *Codul de procedură penală. Comentariu pe articole. Vol I. Partea generală*, 4e éd., Ed. Hamangiu, Bucarest, 2024, p. 548; B. Micu, R. Slăvoiu, A. Zarafiu, *Procedură penală*, 2e éd., Ed. Hamangiu, Bucarest 2024, p. 222-223.

[2907] R. Slăvoiu, *Protecția penală a vieții private*, Ed. Universul Juridic, Bucarest, 2016, p. 273.

[2908] M. Udroiu (coordonnateur) A.A. Bontaș, G. Bodoroncea, S. Bogdan, M. Bulancea, D-S Cherteș, I-P. Chiș, V. Constantinescu, D. Grădinaru, C. Jderu, I. Kuglay, C. Meceanu, I. Nedelcu, L. Postelnicu, S. Răduleţu, A-M. Sine, R. Slăvoiu, I. Tocan, A.-R. Trandafir, M. Vaiescu, G. Zlati, *Codul de procedură penală. Comentariu pe articole*, 2e éd., Ed. C.H. Beck, Bucarest, 2017, p. 664.

[2909] À l'appui de cette opinion, d'autres auteurs (T.-V. Gheorghe, A.S. Uzlău, C.M. Chirița, dans N. Volonciu, A.S. Uzlău, R. Moroșanu, V. Văduva, D. Atasiei, C. Ghigheci, L.E. Holmanu, I.D. Samoilă, C. Voicu, G. Anghel-Tudor, T.-V. Gheorghe, C.M. Chirița, T. Manea, C. Marin, *op. cit.*, 4e éd., Ed. Hamangiu, Bucarest, 2024, p. 548) soulignent que l'exigence d'une gravité abstraite minimale de l'infraction pour laquelle la surveillance technique peut être ordonnée a pour but même de limiter l'utilisation extensive et injustifiée, par les autorités judiciaires, des mesures de surveillance technique, car cela conduirait autrement à une surveillance excessive des citoyens.
Toutefois, il est admis qu'au moment de l'autorisation des mesures de surveillance technique et dans le cadre de leur exécution, toutes les conditions légales étaient remplies (y compris celle relative à la nature de l'infraction), de sorte que l'illégalité, du moins apparente, est analysée par rapport à ce moment, et non à un moment ultérieur, lorsque survient le changement de cadre juridique qui modifie les conditions. Cet aspect, soulignent les auteurs, est également mis en évidence par l'article 4, paragraphe (1), de la loi n° 255/2013 relative à la mise en œuvre du Code de procédure pénale, dont il résulte que les actes de procédure accomplis dans le respect des exigences légales en vigueur à la date de leur accomplissement restent valables. En revanche, les auteurs indiquent qu'en réalité « *le principe susmentionné n'est pas applicable, car si le cadre juridique de l'acte avait été correctement établie, l'utilisation de cette méthode spéciale de surveillance n'aurait pas été autorisée par la loi. Or, il serait absurde d'accepter l'utilisation d'une méthode probatoire restrictive autorisée par la loi dans un cas où le législateur l'a exclue, uniquement en raison du cadre juridique erroné de l'acte par l'autorité judiciaire* ».

[2910] Dans ce sens, R. Budăi, *Unele aspecte practice privind metodele speciale de supraveghere sau cercetare*, articol din 28 mai 2020, consulté sur https://www.juridice.ro/725634/unele-aspecte-practice-privind-metodele-speciale-de-supraveghere-sau-cercetare.html#_edn7; M. Suian, *Metode speciale de supraveghere sau cercetare*, Ed. Solomon, Bucarest, 2021, p. 54.

c'est-à-dire avant le changement de cadre juridique[2911]. En d'autres termes, lors de l'analyse du respect des conditions prévues par la loi pour la prise de mesures de surveillance technique, c'est la situation au moment de l'autorisation des mesures qui est prise en compte, la situation ultérieure étant sans importance.

990. C'est l'acte qui compte, pas le cadre juridique. À notre avis, nous considérons que les preuves obtenues avant le changement de cadre juridique (qui entraîne le non-respect de l'exigence de l'article 139, paragraphe 2, du CPP) ne doivent pas être exclues, sauf si le cadre juridique a été effectué de manière artificielle, manifestement illégale. Concrètement, le point de départ de la discussion devrait être les faits matériels décrits dans l'acte de saisine et vérifiés par les preuves obtenues avant le moment où une mesure de surveillance technique est demandée, et non le cadre en soi. Si, par exemple, le fait signalé et pour lequel une poursuite pénale *in rem* a été engagée concerne le simple vol d'une icône dans une église, dont l'auteur est connu, et que les autorités judiciaires qualifient cet acte d'infraction de corruption pour laquelle des mesures de surveillance technique peuvent être demandées, les résultats obtenus à la suite de l'utilisation de cette procédure probatoire intrusive dans la vie privée doivent être exclus du dossier de l'affaire. Toutefois, la question de l'exclusion des preuves pourrait également être examinée sous l'angle de la loyauté de leur administration, et pas seulement sous celui du changement de cadre juridique.

991. Analyse des preuves. La liberté d'analyse des preuves appartient évidemment au procureur, mais celui-ci doit respecter les principes de loyauté, de légalité et du droit à la défense. Si les faits pour lesquels une mesure de surveillance a été autorisée restent les mêmes, quelle que soit leur cadre juridique, les preuves ainsi obtenues peuvent servir précisément au nouveau cadre. Le motif du changement juridique ne peut en soi équivaloir à l'exclusion des preuves obtenues précédemment. Il est incontestable qu'il y a problème si, par exemple, un certain cadre juridique a porté atteinte au droit à la défense ou à un procès équitable.

Souvent, pour soutenir le contraire de notre opinion, on se réfère aux dispositions de l'article 142, paragraphe (5) du CPP, selon lesquelles « les données résultant des mesures de surveillance technique peuvent également être utilisées dans une autre affaire pénale si elles contiennent des données ou des informations concluantes et utiles concernant la préparation ou la commission d'une autre infraction parmi celles prévues à l'article 139, paragraphe (2) ». Nous estimons que, bien que la disposition mentionnée ne fasse pas référence à l'utilisation des données dans le même dossier, la raison de l'interdiction tient à la nature de l'infraction (qui doit être l'une de celles prévues à l'article 139, paragraphe 2, du CPP) et non au dossier dans

[2911] M. Suian, *op. cit.*, p. 54.

lequel l'infraction est instruite[2912]. Toutefois, nous continuons à estimer qu'en l'absence de précision expresse de la loi, les preuves obtenues par surveillance technique, avant le changement de cadre juridique, doivent être conservées, même s'il ne s'agit plus d'une infraction prévue à l'article 139, paragraphe (2) du CPP.

992. Avantage juridique. De même, la littérature spécialisée a identifié que l'opinion contraire est, dans certaines situations, « absurde », dans le contexte où « le changement de cadre juridique d'une infraction plus grave (n.n. infraction prévue à l'art. 139 paragraphe 2) en une infraction moins grave serait fondée sur les enregistrements effectués »[2913], ce avec quoi nous sommes tout à fait d'accord. Le changement de cadre juridique ne résulte pas nécessairement d'une erreur de la part de l'autorité judiciaire, mais peut être fondé sur le simple fait de la méconnaissance des preuves justifiant un certain cadre juridique. Toutefois, nous ne considérons pas notre opinion comme absolue, car dans certaines situations, on peut effectivement parler d'un cadre juridique manifestement incorrect, cas dans lequel les méthodes de surveillance technique pourraient être exclues.

993. Les preuves restent « acquises ». Par conséquent, nous estimons nécessaire une intervention *de lege ferenda* afin de clarifier cette question, mais, à ce stade, nous considérons que les preuves obtenues après un changement de cadre juridique (avec pour conséquence le non-respect de l'exigence prévue à l'article 139, paragraphe 2) restent « acquises » à la procédure pénale, étant donné qu'au moment de l'autorisation des mesures de surveillance technique (donc avant le changement de cadre juridique), les normes légales étaient respectées et que, par conséquent, les preuves ont été obtenues dans le respect de la loi.

b). Procédure de délivrance du mandat de surveillance technique

994. Le juge statue. La procédure de délivrance[2914] du mandat de surveillance technique est régie par l'article 140 du Code de procédure pénale. Conformément au paragraphe (1) de l'article 140, en principe, « celui-ci peut être ordonné au cours de l'enquête pénale »[2915], « pour une durée maximale de 30 jours, à la demande du procureur »[2916], par le juge des droits et des

[2912] M. Udroiu (coordonnateur) A.A. Bontaş, G. Bodoroncea, S. Bogdan, M. Bulancea, D-S Cherteş, I-P. Chiş, V. Constantinescu, D. Grădinaru, C. Jderu, I. Kuglay, C. Meceanu, I. Nedelcu, L. Postelnicu, S. Răduleţu, A-M. Sine, R. Slăvoiu, I. Tocan, A.-R. Trandafir, M. Vaiescu, G. Zlati, *op. cit.*, p. 695.
[2913] *Ibidem.*
[2914] A. Pintea, D.C. Pintea, A.C. Bălănescu, *Urmărirea penală. Aspecte teoretice şi practice, Modele de acte procesuale şi procedurale*, 2e édition révisée et augmentée, Ed. Universul Juridic, Bucarest, 2020, p. 228.
[2915] C.S. Paraschiv, *op. cit.*, p.82.
[2916] I. Neagu, M. Damaschin, *Tratat de procedură penală. Partea generală*, IVe édition révisée et augmentée, Universul Juridic, Bucarest, 2022, p. 557.

libertés de la juridiction qui serait compétente pour juger l'affaire en première instance ou par la juridiction de même rang dans le ressort de laquelle se trouve le siège du parquet dont relève le procureur qui a formulé la demande.

995. Exception – le procureur autorise. Il existe toutefois une exception à la règle ci-dessus, à savoir que, conformément à l'article 141, paragraphe (1), le procureur peut autoriser, pour une durée maximale de 48 heures, des mesures de surveillance technique lorsque plusieurs conditions cumulatives sont remplies :

- il y a urgence ;

- l'obtention du mandat de surveillance technique dans les conditions prévues à l'article 140 du Code de procédure pénale entraînerait un retard substantiel dans les enquêtes, la perte, l'altération ou la destruction des preuves ou mettrait en danger la sécurité de la personne lésée, du témoin ou des membres de leur famille ;

- les conditions prévues à l'article 139, paragraphes (1) et (2), du Code de procédure pénale sont remplies.

996. Demande motivée. Dans le cadre de la procédure commune, pour ordonner la délivrance d'un mandat de surveillance technique, le procureur doit formuler une demande indiquant les mesures de surveillance technique qu'il demande d'ordonner, le nom ou d'autres données d'identification de la personne contre laquelle la mesure est ordonnée, s'ils sont connus, l'indication des preuves ou des données qui donnent lieu à un soupçon raisonnable quant à la commission d'une infraction pour laquelle la mesure peut être ordonnée, l'indication de l'acte et de son cadre juridique, et, dans le cas d'une mesure de surveillance vidéo, audio ou photographique, si l'autorisation est également demandée aux autorités chargées des poursuites pénales de pénétrer dans les lieux privés indiqués afin d'activer ou de désactiver les moyens techniques qui seront utilisés pour l'exécution de la mesure de surveillance technique, la motivation du caractère proportionné et subsidiaire de la mesure.

997. Procédure secrète. Le procureur doit transmettre le dossier au juge des droits et des libertés[2917], qui statuera le jour même, en chambre du conseil, sans citer les parties, avec la participation obligatoire du procureur. S'il estime que la demande est fondée, le juge des droits et des libertés ordonne, par décision, l'admission de la demande du procureur et délivre immédiatement le mandat de surveillance technique, et s'il estime que les conditions prévues à

[2917] M. Udroiu (coordonnateur) A.A. Bontaş, G. Bodoroncea, S. Bogdan, M. Bulancea, D-S Cherteş, I-P. Chiş, V. Constantinescu, D. Grădinaru, A-V Iugan, C. Jderu, I. Kuglay, C. Meceanu, I. Nedelcu, M. Popa, L. Postelnicu, S. Răduleţu, A-M. Sine, R. Slăvoiu, I. Tocan, A.-R. Trandafir, M. Vaiescu, G. Zlati, *Codul de procedură penală – Comentariu pe articole*, 3e édition, Ed. C.H. Beck, Bucarest, 2020, p. 955-956.

l'article 139 et au paragraphe (1) de l'article 140 ne sont pas remplies, il ordonne, par décision, le rejet de la demande d'autorisation de la mesure de surveillance technique[2918].

998. Situations difficiles dans la pratique. Nous constatons qu'il existe une controverse fondée sur la situation suivante : lorsqu'une affaire implique plusieurs participants à la commission d'une infraction, certains ayant une qualité particulière qui relève de la compétence personnelle d'une autre juridiction que celle compétente en la matière, et que la surveillance technique est demandée à l'égard des participants sans qualité particulière. Dans ce cas, la question se pose de savoir quelle est la juridiction compétente pour délivrer le mandat de surveillance technique : celle qui est compétente matériellement (en fonction de l'infraction commise) ou celle qui est compétente personnellement (en fonction de la qualité du participant).

Il convient d'observer que les dispositions de l'article 140, paragraphe 1, du Code de procédure pénale attribuent généralement la compétence[2919] d'émettre un mandat de surveillance technique au juge des droits et des libertés « de la juridiction qui serait compétente pour juger l'affaire en première instance ». Ainsi, bien que le mandat de surveillance technique ne concerne pas le suspect qui a une qualité particulière qui relève de la compétence d'une certaine juridiction, mais les participants qui n'ont pas cette qualité, le juge de la juridiction compétente pour juger l'affaire en première instance sera néanmoins compétent pour délivrer le mandat. Ainsi, il sera tenu compte des particularités de l'ensemble de l'affaire pénale, y compris de la qualité des personnes.

Si le prévenu pour lequel aucun mandat de surveillance technique n'a été demandé est renvoyé devant le tribunal, les choses sont simples. La discussion se complique si nous nous trouvons dans une situation où la personne qui, naturellement, avait une qualité susceptible de relever de la compétence d'une juridiction hiérarchiquement supérieure, voire d'une juridiction militaire, n'est pas renvoyée devant le tribunal. Dans ce cas, au moment du renvoi en jugement, la compétence est établie en fonction de l'acte commis et non en fonction de la qualité de la personne qui a fait l'objet d'une enquête au cours de la phase de poursuites pénales.

999. Utilisateur inconnu. La surveillance technique peut être ordonnée à l'égard de toute personne[2920] ou même d'un numéro de téléphone donné (par exemple, celui correspondant à une carte prépayée, à un téléphone donné identifié par son numéro IMEI) ou d'un système informatique ou de communication donné, même si leur utilisateur n'est pas connu. En principe,

[2918] B. Micu, R. Slăvoiu, A. Zarafiu, *op. cit.*, p. 219.
[2919] I. Neagu, M. Damaschin, *op. cit.*, p. 580.
[2920] *Idem*, p. 561.

conformément à l'article 139, paragraphe (4) du CPP, la mesure de surveillance technique ne peut viser la relation entre l'avocat et son client, sauf à titre exceptionnel[2921].

1000. L'exécution du mandat est assurée par le procureur. Conformément à l'article 142, paragraphe (1) du Code de procédure pénale, l'exécution du mandat de surveillance technique est assurée par le procureur, qui peut déléguer cette opération aux organes d'enquête pénale ou à des agents spécialisés de la police. La version initiale de cet article, avant une intervention de la Cour constitutionnelle en 2016, prévoyait que le procureur pouvait déléguer l'exécution des mandats de surveillance technique à « d'autres organes spécialisés de l'État ». En complément, conformément au paragraphe (2) de l'article 142, les fournisseurs de réseaux publics de communications électroniques ou les fournisseurs de services de communications électroniques destinés au public ou de tout type de communication ou de services financiers sont tenus de coopérer avec les organes de poursuite pénale, respectivement avec les autorités prévues au paragraphe (1) de l'article 142, dans les limites de leurs compétences, pour l'exécution du mandat de surveillance technique.

1001. Accès des parties au dossier. En second lieu, nous tenons à préciser que, dans le cas où des enregistrements audio/vidéo ont été versés au dossier d'une affaire, afin de respecter le droit à la défense, le tribunal peut autoriser, à la demande des parties ou de la personne lésée, la délivrance de copies des informations contenues sur le support de stockage[2922]. Dans ce contexte, par la décision n° 630/2019[2923] de la Cour constitutionnelle relative au rejet de l'exception d'inconstitutionnalité des dispositions de l'article 139, paragraphe (1) lit. a) et c) et de l'article 282, paragraphe (1) du Code de procédure pénale, la Cour a constaté que « toute violation des règles relatives aux droits procéduraux, y compris en matière de preuve, peut entraîner une atteinte aux droits des parties ou des principaux sujets de la procédure, la preuve de l'atteinte par ceux-ci, ainsi que l'imposition, par la loi, d'autres exigences, telles que la fixation de délais ou de conditions procédurales, constituant une condition d'accès libre à la justice, justifiée par la restriction de la possibilité d'exercer de manière abusive le droit

---

[2921] T.-V. Gheorghe, *op. cit.*, p. 267. De même, un autre auteur (M. Udroiu, *Fişe de procedură penală. Partea generală. Teorie şi cazuri practice*, 3e éd., Ed. C.H. Beck, Bucarest, 2022, p. 288) indique que, à titre exceptionnel, la surveillance technique peut également être ordonnée dans le cadre de la relation entre l'avocat et son client, s'il existe des données indiquant que l'avocat commet ou prépare la commission d'une des infractions pour lesquelles la surveillance technique peut être ordonnée. À cet égard, il convient de rappeler les dispositions de l'article 34 de la loi n° 51/1995, republiée, qui prévoit que la relation entre l'avocat et la personne qu'il assiste ou représente ne peut faire l'objet d'une surveillance technique que s'il existe des données indiquant que l'avocat commet ou prépare la commission d'une infraction prévue à l'article 139, paragraphe (2) du Code de procédure pénale. « *Si, pendant ou après l'exécution de la mesure, il apparaît que les activités de surveillance technique ont également porté sur les relations entre l'avocat et le suspect ou l'accusé qu'il défend, les preuves obtenues ne peuvent être utilisées dans le cadre d'aucun procès pénal et doivent être détruites immédiatement par le procureur, qui informe le juge ayant ordonné la mesure de la destruction des preuves. Le juge ordonne ensuite que l'avocat soit informé* ».

[2922] M. Udroiu, *Fişe de Procedură penală Partea generală. Teorie şi cazuri practice*, Ed. C.H. Beck, Bucarest 2020, p. 277-278.

[2923] Publiée au Journal Officiel, Partie I nº 1024 du 19 décembre 2019.

d'invoquer la nullité relative, afin de garantir l'ordre juridique, indispensable à la valorisation de ses propres droits, dans le respect tant des intérêts généraux que des droits et intérêts légitimes des autres titulaires, auxquels l'État est tenu, dans une égale mesure, d'accorder sa protection »[2924].

B. Aspects controversés générés par l'expression « autres organes spécialisés de l'État »

1002. Implication personnelle du procureur. Au préalable, nous tenons à préciser que les dispositions de l'article 91[2], paragraphe (1), première phrase, du Code de procédure pénale de 1968 prévoyaient que le procureur procède personnellement aux interceptions et aux enregistrements ou peut ordonner qu'ils soient effectués par l'organe d'enquête pénale. Ainsi, les seuls organes pouvant participer à l'activité de surveillance étaient le procureur et les organes d'enquête pénale.

1003. Respect du droit à la vie privée. Comme l'indique la décision n° 51/2016[2925] de la Cour constitutionnelle, dans l'exposé des motifs de la loi n° 135/2010 relative au Code de procédure pénale, il est souligné que la surveillance technique doit respecter, d'une part, le droit à la vie privée et à la confidentialité de la correspondance et, d'autre part, les exigences d'accessibilité, de prévisibilité et de proportionnalité de la loi pénale. Il est évident que l'objectif d'une telle mesure est de découvrir la vérité dans l'affaire en question.

1004. Caractère exceptionnel. Il souligne également la nécessité, d'une part, de respecter le principe de subsidiarité[2926] en réglementant le caractère exceptionnel de la mise en place d'une surveillance technique (en raison des atteintes à la vie privée de la personne) et, d'autre part, du principe de proportionnalité de la mesure de surveillance technique avec la restriction du droit à la vie privée, en fonction de l'affaire concrète, de la pertinence des informations ou des preuves à obtenir ou de la gravité de l'infraction. L'exposé des motifs de la décision de la Cour « ne contient toutefois aucune explication concernant l'introduction dans la réglementation pénale actuelle, outre le procureur et les organes d'enquête pénale, des agents spécialisés de la police

[2924] Décision de la Cour Constitutionnelle nº 630/2019, par. 46.
[2925] Publiée au Journal Officiel, nº 190 du 14 mars 2016.
[2926] De même, au paragraphe 32 de la même décision, « *la Cour constate que l'illégalité de la décision, de l'autorisation, de l'enregistrement ou de l'administration de l'acte entraîne la sanction de la nullité absolue ou relative, selon les distinctions prévues aux articles 281 et 282 du Code de procédure pénale. Ainsi, la mise en œuvre de la surveillance technique, en tant que procédure probatoire, en violation des conditions légales prévues aux articles 138 à 146 du Code de procédure pénale, y compris celles relatives aux organes habilités à exécuter le mandat de surveillance, a pour effet la nullité des preuves ainsi obtenues et, par conséquent, l'impossibilité de les utiliser dans le cadre de la procédure pénale, conformément à l'article 102, paragraphe (3), du Code de procédure pénale* ».

et d'autres organes spécialisés de l'État, et encore moins une explication concernant les organes envisagés par le législateur lors de la réglementation de cette dernière expression »[2927].

1005. Procédure probatoire. Les actes accomplis directement par le procureur ou ceux accomplis par délégation constituent des procédures probatoires, et le procès-verbal consignant les résultats de l'activité de surveillance constitue le moyen de preuve[2928].

1006. Manque de clarté. Pour ces raisons, le législateur a inclus, dans l'article 142, paragraphe (1) du Code de procédure pénale, outre le procureur, l'organe d'enquête pénale et les agents spécialisés de la police et d'« autres organes spécialisés de l'État ». La Cour constate que ces organes spécialisés de l'État ne sont définis ni expressément, ni indirectement dans le Code de procédure pénale[2929].

La Cour relève que l'expression « ou d'autres organes spécialisés de l'État » semble manquer de clarté, de précision et de prévisibilité, empêchant les justiciables de comprendre quels sont ces organes habilités à prendre des mesures présentant un degré élevé d'intrusion dans la vie privée des personnes. Ainsi, la juridiction de contrôle constitutionnel indique que : « Compte tenu de ces arguments et du caractère intrusif des mesures de surveillance technique, (...) la norme constitutionnelle de protection de la vie intime, familiale et privée et du secret de la correspondance impose que leur limitation s'inscrive dans un cadre normatif qui établisse de manière expresse, de manière claire, précise et prévisible, quels sont les organes habilités à effectuer les opérations qui constituent des ingérences dans la sphère protégée des droits »[2930].

1007. Infrastructure technique. La note explicative accompagnant l'Ordonnance d'urgence n° 6/2016 du Gouvernement relative à certaines mesures visant à mettre en œuvre les mandats de surveillance technique ordonnés dans le cadre de procédures pénales[2931] prévoit que, en l'absence d'une infrastructure technique nécessaire à la mise en œuvre de ces méthodes spéciales de surveillance ou d'enquête, serait sérieusement compromise tant du point de vue de l'efficacité des actes de poursuite pénale que de l'administration d'une preuve complète sur la base de toutes les méthodes d'enquête prévues par la loi n° 135/2010 relative au Code de procédure pénale.

[2927] Décision de la Cour Constitutionnelle nº 51/2016, par. 27.

[2928] Décision de la Cour Constitutionnelle nº 51/2016, par. 34. Le même paragraphe précise également que, pour cette raison précisément, « *les seuls organes pouvant participer à leur réalisation sont les organes chargés des poursuites pénales, énumérés à l'article 55, paragraphe (1), du Code de procédure pénale, à savoir le procureur, les organes d'enquête pénale de la police judiciaire et les organes d'enquête pénale spéciaux* ».

[2929] Ainsi, conformément aux lois applicables, le Service Roumain de renseignement n'a de compétences que dans le domaine de la sécurité nationale, sans jouer aucun rôle dans le domaine judiciaire.

[2930] Décision de la Cour Constitutionnelle nº 51/2016, par. 48.

[2931] Consulté sur https://gov.ro/fisiere/subpagini_fisiere/NF_OUG_6-2016.pdf.

a). Protocoles inconstitutionnels entre le SRI et le Ministère Public concernant les interceptions

1008. Exécution des mandats relatifs à la sécurité nationale. Par ailleurs, une modification visant à introduire un nouveau paragraphe à l'article 57 a été proposée, selon lequel les organes d'enquête spéciaux procèdent, dans le cas d'infractions contre la sécurité nationale et d'infractions terroristes, à l'exécution des mandats de surveillance technique[2932]. Dans sa note explicative, l'initiateur a estimé que, afin de ne pas nuire à la coopération avec les autorités judiciaires dans le cadre des enquêtes et de la documentation relatives à ces infractions graves qui portent atteinte à la sécurité nationale, et afin de répondre aux critiques d'inconstitutionnalité, il est nécessaire d'attribuer le statut d'organe d'enquête pénale spéciale à certains cadres spécialisés du Service roumain de renseignement (SRI).

1009. Conflit de nature constitutionnelle. En 2019, un conflit juridique de nature constitutionnelle a éclaté entre le ministère public – le parquet près la Haute Cour de cassation et de justice, d'une part, et le Parlement roumain, la Haute Cour de cassation et de justice et les autres instances judiciaires, d'autre part, concernant l'exécution des mandats de surveillance technique. La principale question soumise à l'appréciation de la Cour constitutionnelle concernait le fait que le Ministère Public s'était arrogé le rôle de législateur en ajoutant à la loi, par le biais du contenu des « protocoles de collaboration », la Cour étant appelée à se prononcer sur les effets systémiques de ces protocoles sur les droits et libertés fondamentaux, dès lors qu'il est reproché que des moyens de preuve aient été obtenus en violation de la répartition constitutionnelle des compétences.

1010. Collaboration inconstitutionnelle. Par sa décision n° 26 du 16 janvier 2019[2933], la Cour a tranché le conflit constitutionnel susmentionné et a estimé que, dans le cadre de la procédure judiciaire, les mesures/actes que le procureur peut prendre/émettre sont expressément prévus par la loi. Elle a ainsi constaté l'existence de protocoles de collaboration conclus entre 2009 et 2016 entre le Ministère Public et le SRI qui, en réalité, conféraient aux agents du SRI des attributions spécifiques à des organes d'enquête pénale, alors qu'une telle possibilité n'était pas prévue par la loi. L'objectif déclaré de la conclusion de ces protocoles était de rendre plus efficace l'activité de poursuite pénale. En réalité, la Cour constitutionnelle a estimé que ces

[2932] La proposition était motivée par le fait que, au niveau du Service roumain de renseignement, il existe une base de données et d'informations importante concernant l'existence de menaces graves et imminentes pour la sécurité nationale, qui correspondent à des infractions de terrorisme, d'espionnage, de criminalité organisée transfrontalière et de criminalité informatique, que le service, en tant qu'organe d'enquête, est tenu de transmettre aux autorités chargées des poursuites pénales.
[2933] Publiée au Journal Officiel, nº 193 du 12.03.2019.

protocoles « suscitent des suppositions quant à une ingérence des services secrets dans le déroulement de l'activité de poursuite pénale et créent les conditions de leur subordination et, par conséquent, de l'activité de poursuite pénale aux structures d'un service secret, ce qui, sur le plan constitutionnel, remet en question la relation entre les parquets et les services de renseignement ».

1011. L'indépendance du procureur, en danger. En pratique, la Cour constitutionnelle a attiré l'attention sur le fait que la subordination des procureurs au SRI affectait l'indépendance de la justice. Or, ces protocoles complétaient la loi de manière cachée et conféraient des attributions supplémentaires et illégales à un service secret. Le pouvoir législatif appartient exclusivement au Parlement, et le Ministère Public a été accusé d'avoir outrepassé ses attributions constitutionnelles en établissant des règles contraires au Code de procédure pénale.

1012. Déclassifiés à la suite de la pression publique. Il est important de noter que ces protocoles ont été classifiés dès leur signature. Ils ont été déclassifiés en 2018, le sujet présentant un intérêt majeur pour la société roumaine, notamment dans le contexte de la protection du droit à la vie privée contre toute intrusion illégale de la part d'un acteur étatique. Dans un communiqué de presse[2934], le Ministère Public a annoncé que ces documents « ont cessé d'être applicables car ils sont devenus caducs à la suite de la décision n° 51/2016 de la Cour constitutionnelle roumaine ».

1013. Assistance technique ou activité de recherche ? La Cour a constaté que « les règles de procédure pénale, établies par la loi, ne prévoient pas que les procureurs, quel que soit leur niveau ou leurs fonctions, de conclure des « protocoles de collaboration » en rapport avec les affaires individuelles qu'ils instruisent »[2935] et que « l'assistance/le soutien/la collaboration technique ne peut être assimilé à une activité d'enquête pénale, propre aux organes de poursuite pénale »[2936]. Dans sa jurisprudence, la Cour a statué que « l'activité d'exécution du mandat de surveillance technique prévue à l'article 142, paragraphe (1), du Code de procédure pénale est réalisée par des actes procéduraux »[2937], et que leur réglementation relève du domaine du droit et entre dans le champ de compétence des autorités chargées des poursuites pénales.

b). Le médiateur: les interceptions réalisées par le SRI violent le droit à la vie privée

[2934] Voir le communiqué du 18.06.2018 : https://www.mpublic.ro/ro/content/c_18-06-2018-15-06.
[2935] Décision de la Cour Constitutionnelle nº 26/16.01.2019, par. 145.
[2936] Décision de la Cour Constitutionnelle nº 26/16.01.2019, par. 155.
[2937] Décision de la Cour Constitutionnelle nº 51/2016, par. 33.

1014. Les procureurs privés d'infrastructure technique. La décision 51/2016 de la Cour constitutionnelle a mis en difficulté le système judiciaire roumain, dans la mesure où ni le Ministère Public ni le Ministère de l'Intérieur (MAI) ne disposaient pas de l'infrastructure technique nécessaire pour procéder à l'interception des communications téléphoniques dans les affaires pénales pour lesquelles une autorisation avait été préalablement obtenue auprès du juge des droits et des libertés. La décision de la Cour constitutionnelle accordait un délai maximal de 45 jours au législateur pour remédier à la situation, et les procureurs ne pouvaient plus déléguer l'exécution des mandats de surveillance technique aux agents du SRI.

1015. OUG 6/2016. Dans ce contexte, l'Ordonnance d'urgence du Gouvernement (OUG) n° 6/2016 relative à certaines mesures pour l'exécution des mandats de surveillance technique ordonnés dans le cadre de procédures pénales a été adoptée, un acte normatif destiné à sauver la situation. Tout d'abord, le Code de procédure pénale a été modifié de manière à supprimer l'expression « ou d'autres organes spécialisés de l'État » du contenu de l'article 142, paragraphe 1. Dans le préambule de l'Ordonnance, l'urgence de son adoption est justifiée « compte tenu du fait que l'activité des parquets serait gravement affectée en l'absence d'un soutien technique et de ressources humaines spécialisées pour la gestion d'une infrastructure de communications ».

1016. Création du CNIC. Par l'Ordonnance d'urgence n° 6/2016 du Gouvernement, le « Centre national d'interception des communications au sein du Service roumain de renseignement » (CNIC) a été créé, bien qu'avant la publication de ladite ordonnance, aucun acte normatif n'ait été trouvé qui ait institué cette institution[2938]. Ce Centre fonctionne comme un département au sein du SRI et a pour objectif principal l'obtention, le traitement et le stockage d'informations dans le domaine de la sécurité nationale. Cependant, compte tenu du manque de moyens techniques pour mettre en œuvre les mesures de surveillance technique du Ministère Public, cette ordonnance a introduit une disposition qui a suscité de nouvelles controverses : « à la demande des organes de poursuite pénale, le Centre leur assure un accès direct et indépendant aux systèmes techniques afin de mettre en œuvre la surveillance technique prévue à l'article 138, paragraphe (1), point a), du Code de procédure pénale ». Concrètement, les autorités judiciaires pouvaient utiliser l'infrastructure technique du SRI pour effectuer des

[2938] Ainsi, il est soutenu que, par la promulgation de l'Ordonnance d'urgence du Gouvernement n° 6/2016, on a introduit dans la législation de la Roumanie une institution (C.N.I.C.) « *qui n'existe pas d'un point de vue juridique, en ce sens qu'elle n'a jamais acquis de personnalité juridique et n'a jamais été créée par un acte normatif public, ayant force de loi, opposable aux citoyens roumains. La légalisation d'une institution par une ordonnance d'urgence est de nature à violer l'article 115, paragraphe (6), de la Constitution, selon lequel : « Les ordonnances d'urgence ne peuvent être adoptées dans le domaine des lois constitutionnelles, elles ne peuvent affecter le régime des institutions fondamentales de l'État [...]* » (Décision de la Cour Constitutionnelle n° 55/2022, par. 68).

interceptions, et ce dernier n'exécutait plus les mandats, mais offrait uniquement un « soutien technique »[2939].

1017. Nouvelles critiques d'inconstitutionnalité. L'article 4, paragraphe 2, de l'OUG 6/2016[2940] a également suscité de vives controverses, car il autorisait la poursuite de la signature de protocoles de coopération entre le SRI et le Ministère Public, qui, dans les faits, permettaient aux agents du SRI de continuer à participer à des actes de poursuite pénale et même à l'élaboration de stratégies d'enquête pénale.

Une critique virulente a été formulée par le Médiateur, qui a saisi la Cour constitutionnelle le 19 novembre 2021. Il a été démontré que l'OUG 16/2016 a permis au C.N.I.C. et au S.R.I. de mener des activités portant atteinte à la vie privée et au droit à un procès équitable, car non seulement les dispositions de l'article 115, paragraphe (6) de la Constitution, qui interdit *expressis verbis* l'adoption d'un O.U.G. dans le domaine des lois constitutionnelles, des droits et libertés fondamentaux, mais aussi d'autres dispositions : l'article 21, paragraphe (3) concernant le droit à un procès équitable, l'article 26 concernant la vie privée, l'article 28 concernant le secret de la correspondance et l'article 61, paragraphe (1) de la Loi fondamentale.

1018. Arguments du Médiateur. Par la Décision n° 55 du 16 février 2022[2941], la Cour constitutionnelle s'est prononcée sur les arguments présentés par le Médiateur. Dans le contenu de la décision, il a été souligné que, selon le Médiateur, en ce qui concerne les critiques d'inconstitutionnalité extrinsèque de l'Ordonnance d'urgence du Gouvernement n° 6/2016, « conformément aux dispositions de l'article 147, paragraphe (4) de la Constitution, les décisions de la Cour constitutionnelle sont généralement obligatoires, de sorte que, dans le cas où la juridiction de contrôle constitutionnel a constaté l'inconstitutionnalité d'une certaine solution législative, celle-ci ne peut devenir partie intégrante du droit positif par le biais d'un autre acte normatif »[2942].

Le Médiateur estime que l'Ordonnance d'urgence du Gouvernement n° 6/2016 « entraîne des conséquences négatives en matière de garantie du droit à la vie intime, familiale et privée,

[2939] À cet égard, la Haute Cour de Cassation et de Justice, par sa Décision n° 64 du 2 octobre 2023, a établi que le Centre national d'interception des communications du Service roumain de renseignement, lorsqu'il met à disposition l'infrastructure nécessaire pour assurer les conditions techniques de l'exécution des mesures de surveillance technique, ne constitue pas une activité d'exécution du mandat de surveillance technique au sens de l'article 142 du Code de procédure pénale.

[2940] « Les organes du Service roumain de renseignement ne peuvent mener d'enquêtes pénales, ne peuvent procéder à des gardes à vue ou à des arrestations préventives et ne disposent pas de leurs propres locaux de détention. À titre exceptionnel, les organes du Service roumain de renseignement peuvent être désignés comme organes d'enquête pénale spéciaux conformément à l'article 55, paragraphes (5) et (6), du Code de procédure pénale pour l'exécution des mandats de surveillance technique, conformément aux dispositions de l'article 57, paragraphe (2), dernière phrase, du Code de procédure pénale. »

[2941] Publiée au Journal Officiel, nº 358 du 11.04.2022.

[2942] Décision de la Cour Constitutionnelle nº 55/2022, par. 4.

consacré par l'article 26 de la loi fondamentale »[2943] et que, compte tenu du caractère intrusif des mesures de surveillance technique, « il est impératif que les mesures de surveillance technique soient mises en œuvre dans un cadre normatif clair, précis et prévisible, tant pour la personne soumise à cette mesure que pour les organes de poursuite pénale et les tribunaux »[2944].

Le Médiateur estime également que l'introduction de l'article 30[1] dans la loi n° 304/2004 relative à l'organisation judiciaire vise à créer une apparence de légalité concernant l'exécution des mandats de surveillance technique dans le cadre des procédures pénales. Il estime que, de cette manière, la Haute Cour de Cassation et de Justice finirait par exercer un contrôle sur le C.N.I.C., violant ainsi le principe de la séparation des pouvoirs dans l'État.

1019. Clarté. Par ailleurs, il est avancé que le champ d'application de l'Ordonnance d'urgence n° 6/2016 du Gouvernement, à savoir les mesures visant à exécuter les mandats de surveillance technique ordonnés dans le cadre d'une procédure pénale, concerne des mesures qui affectent des droits fondamentaux et que, pour cette raison, les mesures de surveillance technique doivent être exécutées dans un cadre juridique aussi clair et précis que possible, non seulement pour la personne visée par la mesure de surveillance technique, mais aussi pour les autorités judiciaires.

1020. Objections d'inconstitutionnalité admises. Enfin, par décision du 16 février 2022, la Cour constitutionnelle admet les objections d'inconstitutionnalité formulées et, dans son argumentation, se réfère à une étude de droit comparé dont il ressort que dans la plupart des États membres de l'Union Européenne, la mise en œuvre des mesures de surveillance technique ne peut être effectuée que par les autorités judiciaires[2945].

La Cour a retenu que, « bien que six ans se soient écoulés depuis l'adoption de l'Ordonnance d'urgence n° 6/2016 du Gouvernement, le législateur, par la loi l'approuvant, s'est limité à approuver la « solution d'urgence » sans réglementer une procédure conforme aux normes constitutionnelles et a désigné la C.N.I.C. comme seule entité chargée d'exécuter tant les actes d'autorisation délivrés en vertu de l'article 13 de la loi n° 51/1991 relative à la sécurité nationale de la Roumanie que les mandats de surveillance technique délivrés conformément au Code de procédure pénale »[2946].

[2943] Décision de la Cour Constitutionnelle nº 55/2022, par. 9.

[2944] Décision de la Cour Constitutionnelle nº 55/2022, par. 16. De même, le Médiateur souligne que « dans le cas contraire, cela pourrait conduire à une violation aléatoire/abusive de certains droits fondamentaux essentiels dans un État de droit : la vie intime, familiale et privée ».

[2945] Par ailleurs, la Cour constitutionnelle souligne également que « s'agissant de l'exécution des mandats de surveillance technique, (...) le législateur a opté pour un système dualiste. D'une part, il réglemente la possibilité de mettre en place un système d'exécution des mandats de surveillance technique intégré à chaque unité du parquet et, d'autre part, il réglemente un système externe à ces unités, basé sur l'existence d'une seule entité par l'intermédiaire de laquelle les mandats de surveillance technique peuvent être exécutés » (Décision de la Cour constitutionnelle n° 55/2022, par. 200).

[2946] Décision de la Cour constitutionnelle n° 55/2022, par. 202.

En conclusion, la Cour a constaté que les dispositions de l'article II, point 1, et de l'article IV, point 1, troisième phrase, de l'Ordonnance d'urgence n° 6/2016 du Gouvernement relative à certaines mesures d'exécution des mandats de surveillance technique ordonnés dans le cadre de procédures pénales enfreignent les dispositions constitutionnelles, à savoir l'article 1, paragraphe (4), l'article 1, paragraphe (5), les articles 26, 28, 124, 126, 131 et 132 de la Constitution.

C. Information de la personne surveillée et de l'interlocuteur occasionnel

1021. La cessation de la mesure est notifiée par écrit. Conformément à l'article 145 du Code de procédure pénale, dans un délai maximal de 10 jours à compter de la cessation de la mesure de surveillance technique, le procureur informe par écrit chaque personne surveillée de la mesure de surveillance technique qui a été ordonnée à son égard[2947]. Le procureur a l'obligation procédurale positive d'informer[2948], par écrit, dans un délai maximal de 10 jours après la cessation de la mesure de surveillance technique, chaque personne visée par un mandat de la mesure de surveillance technique qui a été prise à son égard[2949].

1022. Report de l'information. Toutefois, le procureur peut ordonner, par ordonnance motivée, dans un délai de 10 jours à compter de la fin de la mesure de surveillance technique, le report de l'information ou, après l'information, le report de la présentation des supports sur lesquels sont stockées les activités de surveillance technique ou des procès-verbaux de restitution à la suite d'une demande de consultation du dossier, si cela pouvait entraîner : la perturbation ou la mise en danger du bon déroulement de l'enquête pénale en cause ; la mise en danger de la sécurité de la victime, des témoins ou des membres de leur famille ; des difficultés dans la surveillance technique d'autres personnes impliquées dans l'affaire.

Le report de la communication/présentation des supports sur lesquels sont stockées les activités de surveillance technique ou les procès-verbaux de restitution peut être ordonné au plus tard jusqu'à la fin de l'enquête pénale ou jusqu'au classement de l'affaire[2950].

[2947] I. Neagu, M. Damaschin, *op. cit.*, p.567.
[2948] A. Pintea, D.C. Pintea, A.C. Bălănescu, *op. cit.*, p.235.
[2949] G. Teodoru, I.-P. Chiș, *Tratat de Drept procesual penal*, 4e éd., Ed. Hamangiu 2020, p.440.
[2950] M. Udroiu, *Fişe de Procedură penală Partea generală. Teorie şi cazuri practice*, Ed. C.H. Beck, Bucarest, 2020, p. 278.

1023. Effets de l'omission. L'omission injustifiée de fournir les informations dans le délai prévu par la loi (lorsqu'aucun report n'a été ordonné) n'entraîne pas l'exclusion des preuves, car la légalité de leur obtention ou de leur administration n'est pas affectée[2951].

1024. Violation de la vie privée des interlocuteurs accidentels. Dans ce contexte, nous soulignons qu'avant la modification de l'article 145 du CPP par la loi n° 201/2023, conformément à l'article 145, paragraphe (2) du CPP, le droit d'être informé et d'examiner les résultats de la surveillance n'était reconnu qu'à la personne directement visée par le mandat, et non aux personnes qui ont communiqué ou ont eu des rencontres avec celle-ci et qui ont été enregistrées de manière fortuite. Cette omission réglementaire soulevait la question d'une éventuelle violation du droit à la vie privée des tiers dont les conversations avaient été interceptées et enregistrées dans le cadre de l'exécution du mandat de surveillance de la personne avec laquelle ils avaient dialogué.

1025. Saisine de la Cour Constitutionnelle. Bien avant la modification du Code de procédure pénale de 2023, la Haute Cour de Cassation et de Justice a saisi la Cour constitutionnelle d'une exception d'inconstitutionnalité, qui a donné lieu à la Décision n° 244 du 6 avril 2017[2952]. Dans l'exposé des motifs de l'exception d'inconstitutionnalité formulée, la Haute Cour souligne que la surveillance technique implique des procédures probatoires qui affectent de manière substantielle le droit à la vie privée, droit protégé non seulement par les articles 26 et 28 de la Loi fondamentale, mais aussi par la Convention européenne des droits de l'homme[2953].

1026. Garanties relatives à la vie privée. La Cour constitutionnelle a observé que la notion de vie privée est étroitement liée aux éléments visés par les méthodes de surveillance prévues à l'article 138, paragraphe (1) les points a) à d) et on considère que le contrôle *a posteriori* de ces éléments constitue une garantie de l'intimité de la vie privée, déterminant ainsi un niveau de proportionnalité entre la mesure de surveillance technique (compte tenu de son objectif et de sa nécessité) et la vie privée d'une personne.

1027. Recours effectif contre l'intrusion. Ainsi, la Cour a constaté que, « en matière de protection du droit constitutionnel à la vie privée, le législateur a l'obligation de prévoir un recours effectif permettant à la personne soumise à la mesure de surveillance technique »[2954] de

---

[2951] M. Udroiu (coordonnateur) A.A. Bontaş, G. Bodoroncea, S. Bogdan, M. Bulancea, D-S Cherteş, I-P. Chiş, V. Constantinescu, D. Grădinaru, A-V Iugan, C. Jderu, I. Kuglay, C. Meceanu, I. Nedelcu, M. Popa, L. Postelnicu, S. Răduleţu, A-M. Sine, R. Slăvoiu, I. Tocan, A.-R. Trandafir, M. Vaiescu, G. Zlati, *op. cit.*, p.1003.

[2952] Publiée au Journal Officiel de la Roumanie, Partie I, nº 529 du 6 juillet 2017.

[2953] Selon l'article 13 de la Convention, « toute personne dont les droits et libertés reconnus dans la présente Convention ont été violés a le droit de saisir efficacement un tribunal national, même si la violation a été commise par des personnes agissant dans l'exercice de leurs fonctions officielles ». De même, conformément à l'article 21, paragraphe (1) de la Constitution, toute personne peut saisir la justice pour défendre ses droits, ses libertés et ses intérêts légitimes.

[2954] Décision de la Cour constitutionnelle nº 244/2017, par. 73.

faire cesser les éventuelles violations des droits et libertés fondamentaux et d'obtenir une réparation appropriée des conséquences de la violation contestée. Dans ces conditions, dans le cadre d'une procédure pénale, la contestation de la légalité de la mesure de surveillance technique peut être effectuée tant par le prévenu - dans le cadre de la procédure de chambre préliminaire, après le renvoi en jugement, ainsi que dans le cadre de la procédure de chambre préliminaire lorsque la plainte contre la décision de classement est tranchée, si une action pénale a été engagée dans l'affaire, et par les personnes qui n'ont aucune qualité dans le dossier pénal ou qui ont la qualité de suspect, donc de « personne concernée » par cette mesure.

1028. Dispositions inconstitutionnelles. La Cour constitutionnelle a admis l'exception d'inconstitutionnalité et a constaté que l'article 145 est une disposition inconstitutionnelle, car il ne permet pas à d'autres personnes que le prévenu de contester la légalité des mesures de surveillance technique. Par ailleurs, nous précisons que, selon la doctrine, « il n'est pas nécessaire, pour ordonner la mesure de surveillance technique, que le procureur ait ordonné la poursuite de l'enquête pénale à l'encontre du suspect »[2955].

1029. Contrôle *a posteriori*. À la suite de l'admission de l'exception d'inconstitutionnalité, la Loi n° 201/2023 modifiant et complétant la Loi n° 135/2010 relative au Code de procédure pénale, ainsi que d'autres actes normatifs, entrée en vigueur le 9 juillet 2023, a inséré un nouvel article - l'article 145[1] - précisément pour permettre l'exercice d'un contrôle *a posteriori* sur la surveillance technique par des personnes autres que le suspect ou l'accusé.

1030. Incohérences. Cette règle stipule que « toute personne faisant l'objet d'une mesure de surveillance technique et qui n'a pas acquis la qualité de partie dans cette affaire, ainsi que le prévenu à l'égard duquel il a été décidé de renoncer aux poursuites pénales ou de classer l'affaire, peut former une plainte contre la mesure et son mode d'exécution ».

Bien que la nouvelle disposition soit, en substance, bienvenue et louable, nous soulignons qu'elle n'est pas exempte de questions controversées[2956], de formulations pour le

[2955] G. Teodoru, I.-P. Chiș, *op. cit.*, p. 421.

[2956] Ces aspects sont également confirmés dans la littérature spécialisée (M.V. Tudoran, « Analiza modificărilor aduse de Legea nr. 201/2023 în materia supravegherii tehnice », dans la revue *Dreptul*, n° 1/2025), la disposition légale n'est pas exempte d'incohérences critiquables. Tout d'abord, d'un point de vue logique, les paragraphes (1) et (2) devraient être inversés, car ce n'est qu'après le prononcé de l'acte d'accusation ou de l'ordonnance de classement ou de renonciation à la poursuite pénale que la personne à l'encontre de laquelle une mesure de surveillance technique a été ordonnée ou confirmée saura si elle a la qualité d'une des personnes du paragraphe (1) et, en plus, il y a une « organisation consécutive logique » entre le paragraphe (1) et le paragraphe (2) de l'article 145[1] du CCP. En deuxième lieu, conformément à l'article 145, paragraphe (3)-disposition qui impose à l'autorité judiciaire l'obligation d'informer la personne surveillée des mesures de surveillance ordonnées à son encontre, le procureur peut reporter la communication écrite ou la présentation du contenu des supports sur lesquels sont stockées les activités de surveillance technique ou les procès-verbaux de restitution « au plus tard jusqu'à la résolution de l'affaire ». Une nouvelle intervention législative est donc nécessaire pour remédier à cette incohérence législative regrettable.

moins regrettables et d'incohérences entre les différentes règles de procédure[2957], l'utilité de la règle étant ainsi contrecarrée par la « négligence » du législateur[2958]. Il est donc nécessaire que les incohérences mises en évidence soient corrigées lors des prochaines révisions législatives.

Conclusions du Chapitre 1

Le chapitre reconstitue, à partir des expériences française, roumaine et européenne, la ligne de démarcation juridique entre les prérogatives de l'État en matière de surveillance et les limites imposées par le droit à la vie privée. Partant de la justification théorique de l'intrusion et des premières contraintes juridiques applicables aux autorités (Semayne, premières réglementations du mandat de perquisition), l'analyse montre que l'intervention coercitive dans l'espace privé n'est pas un donné naturel de la souveraineté, mais le résultat d'une construction normative progressive, qui conditionne l'accès des forces publiques au domicile et aux conversations privées.

L'évolution des réglementations relatives à l'interception des communications, avec des repères tels que Malone c. Royaume-Uni, le rapport Birkett, la loi britannique de 1985 ou la loi allemande G10, confirme la même logique : la surveillance technique n'est admise que sur la base de critères clairs de légalité, de délimitation matérielle et de contrôle externe, et les différences de traitement entre citoyens et étrangers, les collaborations entre services et les transferts de données soulèvent des problèmes autonomes de compatibilité avec les exigences de la Convention européenne. La formule politique selon laquelle on ne peut garantir à la fois

[2957] À cet égard, une autre incohérence que nous soulignerons concerne la rédaction du paragraphe (7) et du paragraphe (8) point b) de l'article 145[1] du CPP. Ainsi, le paragraphe (7) précise que le juge de la chambre préliminaire vérifie la légalité de la mesure de surveillance technique et son mode d'exécution, tandis que le paragraphe (8) stipule que le juge peut admettre la plainte et constater l'illégalité de la mesure de surveillance technique. Ainsi, le premier texte de loi entraînerait une séparation entre la mesure de surveillance technique et son mode d'exécution, tandis que le second texte de loi suggère la vérification de la mesure de surveillance technique, qui inclurait également son mode d'exécution. Comme le montre l'auteur susmentionné (M.V. Tudoran, « Analiza modificărilor aduse de Legea nr. 201/2023 în materia supravegherii tehnice », dans la revue *Dreptul*, n° 1/2025), en fait, « ce qui est exécuté, au sens strict, c'est le mandat de surveillance technique ».

[2958] En conclusion, les modifications apportées par la loi n° 201/2023 étaient nécessaires car, comme l'a constaté la Cour constitutionnelle, les mesures de surveillance technique constituent « une ingérence dans la vie privée des personnes soumises à ces mesures » et, par conséquent, « il doit y avoir un contrôle a posteriori de l'autorisation et de la mise en œuvre de la surveillance technique ». Comme le constate un auteur (M.V. Tudoran, « Analiza modificărilor aduse de Legea nr. 201/2023 în materia supravegherii tehnice », dans la revue *Dreptul*, n° 1/2025), « Il apparaît donc nécessaire d'imposer une obligation positive de la part de l'État visant à réglementer, dans le cadre de la législation interne, un « recours effectif » permettant de remédier à d'éventuelles violations des droits et libertés fondamentaux. En ce qui concerne les personnes soumises à des mesures de surveillance technique, autres que le prévenu, l'État n'a pas respecté son obligation positive de réglementer une forme de contrôle a posteriori, à laquelle la personne concernée peut avoir accès afin de vérifier le respect des conditions et, implicitement, la légalité de cette mesure ».

« 100 % de sécurité » et « 100 % de vie privée » n'est pas reprise comme règle juridique, mais comme avertissement sur la nécessité d'un équilibre normatif précis.

La partie consacrée à la surveillance technique en France et en Roumanie décrit concrètement les risques résultant du décalage entre la pratique et la réglementation. En France, le retard de l'intervention législative, le rôle étendu de la jurisprudence, le régime des interceptions judiciaires et administratives, l'absence de voies de recours efficaces et les constatations de la CNCTR concernant les collectes sans autorisation préalable montrent que la simple existence d'un mandat n'est pas suffisante si l'architecture des procédures favorise l'opacité. En Roumanie, l'extension de la formule « autres organes spécialisés de l'État », les protocoles déclarés inconstitutionnels, l'implication des services de renseignement dans les activités de poursuite pénale et les problèmes liés à l'information des personnes concernées dessinent un modèle dans lequel les instruments spéciaux peuvent dégénérer en un mécanisme de surveillance permanente.

En matière d'ingérence gouvernementale, le droit pénal et la procédure pénale doivent fonctionner comme une barrière et non comme un simple canal technique de validation de la volonté étatique. Les mandats de perquisition, l'interception des communications, l'accès aux données et la coopération entre les services ne sont légitimes que dans la mesure où ils sont encadrés par des règles claires, un contrôle juridictionnel effectif, des limitations temporelles et matérielles, une transparence a posteriori et l'interdiction d'utiliser des mécanismes secrets parallèles. Tout écart par rapport à ces exigences transforme les instruments d'enquête exceptionnels en une ingérence structurelle incompatible avec la protection de la vie privée.

Chapitre 2
SURVEILLANCE ÉLECTRONIQUE

1031. Qu'est-ce que la surveillance électronique (SE) ? La surveillance électronique est un terme général qui fait référence aux formes de surveillance par lesquelles l'emplacement, le mouvement et le comportement spécifique des individus[2959]sont surveillés. Au fil du temps, les technologies de localisation ont évolué de la radiofréquence au GPS (système de positionnement global). Ce dernier, actuellement utilisé dans les systèmes de surveillance électronique, utilise le principe de la triangulation et, à l'aide d'un réseau satellitaire, fournit des emplacements précis, assurant une surveillance continue en temps réel dans divers environnements géographiques[2960].

1032. Stigmatisation des personnes surveillées. L'une des principales controverses sur la surveillance électronique est ses implications dans la vie privée, la tendance à étendre (au lieu de remplacer) l'incarcération, la stigmatisation possible des personnes surveillées, le contrôle qu'il peut exercer sur le comportement, et l'impact sur les familles ou les proches[2961].

En ce qui concerne les droits de l'homme[2962], l'utilisation de l'UE peut être réalisée :

- Article 3 : " nul ne sera soumis à la torture ni à des peines ou traitements inhumains ou dégradants "
- Article 5 – droit à la liberté et à la sécurité
- Article 8 - "le droit au respect de la vie privée et familiale".

1033. Utilisation modérée de l'EM. Les droits de l'homme en détention remontent d'abord à 1955 par l'ONU[2963], puis de manière beaucoup plus avancée dans les règles Mandela en 2015[2964]. Au niveau européen, le Conseil de l'Europe a élaboré des règles pénitentiaires

---

[2959] T. Alhmiedat, M. Aborokbah, *Social distance monitoring approach wearable smart tags*, Electronics, vol.10, 2021. p.2435

[2960] E. Kaplan, C. Hegarty(eds), *Understanding GPS : principles and application*. 2nd ed., MA : Artech House Inc, 2006.

[2961] Nellis, M. (2013) « Surveillance, Stigma and Spatial Constraint : The Ethical Challenges of Electronic Monitoring » in : Nellis, M., Beyens, K. and Kaminski, D. (eds.) Electronic Monitoring Punishment : International and Critical perspectives, Oxon : Routledge : 193-210
https ://www.taylorfrancis.com/chapters/edit/10.4324/9780203103029-13/surveillance-stigma-spatial-constraint-mike-nellis?context=ubx

[2962] Convention européenne des droits de l'homme
https ://www.echr.coe.int/documents/d/echr/Convention_RON

[2963] *Ensemble de règles minima pour le traitement des détenus*, accepté par le premier Congrès des Nations Unies pour la prévention du délit et le traitement des délinquants, tenu à Genève en 1955, et approuvées par le Conseil économique et social par ses résolutions 663 C (XXIV) du 31 juillet 1957 et 2076 (LXII) du 13 mai 1977. https ://www.unodc.org/pdf/criminal_justice/UN_Standard_Minimum_Rules_for_the_Treatment_of_Prisoners.pdf

[2964] *Ensemble de règles minima des Nations Unies pour le traitement des détenus* (*règles Nelson Mandela*). https ://www.unodc.org/documents/justice-and-prison-reform/Nelson_Mandela_Rules-E-ebook.pdf

européennes[2965]. Sur la base de ces règlements, ils ont été jugés au fil du temps comme des violations des droits de l'homme et des sanctions communautaires, de la stigmatisation et de l'humiliation, des mesures intrusives dans la vie privée, telles que la surveillance électronique[2966]. Dans ce contexte, il est nécessaire d'élaborer des règles pour la bonne utilisation du SME, ce qui est fait par le Conseil de l'Europe en 2010, par les règles de probation - Recueil (2010)1[2967] et en 2014 sous la forme de la Recommandation cm/Rec(2014)4[2968]. Ce document souligne clairement le caractère intrusif (avec un impact sur la vie privée) de l'UE, soulignant (dans le principe de base n° 1) la nécessité d'une réglementation nationale de son utilisation. Il recommande également de l'utiliser modérément, avec prudence, afin de ne pas étendre inutilement et illégalement le réseau de contrôle pénal (règles no.2 et 16).

Section 1**. LA SURVEILLANCE ÉLECTRONIQUE: UNE MESURE SUBSTITUTIVE À L'INCARCÉRATION ET SES ARGUMENTS JUSTIFICATIFS**

Bien que plusieurs définitions aient été données au système de surveillance, elles convergent toutes vers le contenu et la signification stipulés par le Comité des Ministres du Conseil de l'Europe 2014 : « Un terme général désignant les formes de surveillance utilisées pour surveiller la localisation, les déplacements et le comportement spécifique des personnes soumises à la justice pénale ». Les formes actuelles de surveillance électronique sont basées sur la technologie de suivi radio, barométrique ou par satellite. Ils comprennent généralement un dispositif amovible attaché à la personne concernée[2969].

§1. MÉTHODE ALTERNATIVE À L'INCARCÉRATION. ARGUMENTS EN FAVEUR DE LA SURVEILLANCE ÉLECTRONIQUE

1034. Comme alternative à la prison classique, la surveillance électronique des personnes pendant les procédures judiciaires et dans l'exécution des sanctions pénales est mise en œuvre

[2965] E. Steinerte, D. van Zyl Smit, S. Snacken, *Principles of European Prison Law and Policy : Penology and Human Rights*, Human Rights Law Review, vol. 11, no. 2, 2011. P.417 – 420. https ://doi.org/10.1093/hrlr/ngr008
[2966] F. Dünkel, „*Electronic Monitoring in Europe – a Panacea for Reforming Criminal Sanctions Systems? A Critical Review"*, Kriminologijos studijos, vol.6, 2018, pp.58-77. 10.15388/CrimLithuan.2018.6.3.
[2967] *Recommendation CM/Rec(2010)1 of the Committee of Ministers to member states on the Council of Europe Probation Rules*. https ://cep-probation.org/wp-content/uploads/2018/10/CoE-probation-rules-recommendation.pdf
[2968] *Recommendation CM/Rec(2014)4 of the Committee of Ministers to member states on electronic monitoring*. http ://www.europeanrights.eu/public/atti/2014_-_4__ing.pdf
[2969] J. Bonta, W. Capretta, S. Rooney, *A quasi-experimental evaluation of an intensive rehabilitation supervision program*, Criminal Justice and Behavior, vol.27, 2000. p.312-329.

au niveau européen depuis environ deux décennies. Une enquête menée en 2013 dans les pays européens a montré que la surveillance électrique comme méthode alternative d'incarcération est de plus en plus utilisée, son utilisation variant d'un État à l'autre en fonction du contexte juridique et de l'infrastructure disponible[2970].

A. Les fondements théoriques et pratiques

1035. Principaux avantages. Utilisée soit pour prévenir la surpopulation carcérale et réduire les coûts, soit pour offrir des sanctions plus accessibles avec un certain respect de la vie privée, les partisans de cette mesure espèrent atteindre et réduire le taux de rechute et, implicitement, le taux de criminalité[2971]. En 2005, un rapport est publié dans le Journal of Experimental Criminology, qui souligne la possibilité de réduire les rechutes avec l'aide du me, en particulier si la mise en œuvre de programmes de réadaptation et de conseils[2972]est ajoutée à cette mesure.

Une enquête menée en 2010 à l'étranger (les États-Unis étant le premier État à mettre en œuvre une surveillance électronique, vers 80), montre que la surveillance électronique a réduit le risque de rechute (jusqu'à 31%) et facilité la réintégration. Du point de vue des personnes surveillées, cette mesure procure un sentiment de liberté, leur permettant de poursuivre leur vie personnelle et professionnelle. Cependant, des effets négatifs tels que la stigmatisation sont également signalés, ce qui entraîne des effets psychologiques et sociaux négatifs[2973].

1036. Problèmes liés à l'intrusion dans la vie privée. En 1993, la Nouvelle-Zélande a introduit la détention à domicile contrôlée électroniquement pour les infractions légères à moyennes. L'évaluation qui a suivi a révélé de nombreux aspects positifs, tels que la réduction des coûts, la facilitation de l'intégration dans la société ou la réduction du pourcentage de rechutes. Les principaux défis auxquels ils étaient confrontés à l'époque étaient la difficulté de surveiller efficacement, compte tenu de la technologie disponible à l'époque[2974]. Une évaluation plus récente du même pays ne se concentre plus sur les problèmes liés à la technologie, mais

[2970] Report Mike Nellis – *Survey of Electronic Monitoring in Europe*, EuroPris, 2017 https ://www.europris.org/file/report-mike-nellis-survey-of-electronic-monitoring-in-europe/?download=1

[2971] P. Conway, „*Survey of Agencies Using Electronic Monitoring Reveals a Promising Future",* Journal of Offender Monitoring, vol.16.2, 2003.

[2972] M. Renzema, E. Mayo-Wilson, *Can electronic monitoring reduce crime for moderate to high-risk offenders?,* J Exp Criminol, 2005, p.215–237. https ://doi.org/10.1007/s11292-005-1615-1

[2973] B. Balles, K. Mann, T. Blomberg, et al., *A quantitative and qualitative assessment of electronic monitoring*, U.S. Department of Justice, 2010.http ://criminology.fsu.acsitefactory.com/sites/g/files/upcbnu3076/files/2021-03/A-Quantitative-and-Qualitative-Assessment-of-Electronic-Monitoring.pdf

[2974] A Church, S Dunstan, *Home Detention, The Evaluation of the Home Detention Pilot Program, 1995-1997,* U.S. Department of Justice, 1997. https ://www.ojp.gov/ncjrs/virtual-library/abstracts/home-detention-evaluation-home-detention-pilot-programme-1995-1997

sur ceux liés à l'intrusion dans la vie privée, les personnes concernées ressentant un stress psychologique majeur compte tenu de la pression d'une surveillance continue[2975].

1037. Utilisation de l'EM en médecine. Abordant un domaine de niche, en 2023, des chercheurs britanniques explorent l'utilisation de l'EM dans les établissements de santé mentale médico-légale[2976] au Royaume-Uni[2977], concluant que la méthode est utile pour accélérer la reproductibilité, réduire les coûts et accroître la sécurité publique. Les principales controverses ont été juridiques pour le respect des droits de l'homme, en particulier lors du recours au MEM sur le long terme[2978]. Toujours au Royaume-Uni, un programme pilote sur l'utilisation de l'UE a été introduit en 2014 pour vérifier si les criminels se conforment à une interdiction d'alcool imposée par les tribunaux[2979]. Le programme s'est avéré efficace, associant un taux de rechute plus faible, une réduction des comportements antisociaux et un impact positif sur la qualité de vie des participants[2980]. La surveillance électronique a évolué régulièrement au Royaume-Uni au cours de la dernière décennie. Utilisée à l'origine en 1999 pour les criminels sous surveillance, la méthode s'étend désormais à de nombreux types de crimes, permettant des poursuites en temps réel et contribuant à une surveillance communautaire efficace[2981].

En particulier, la motivation sociale devrait prévaloir dans l'introduction d'un système de surveillance comme alternative à l'emprisonnement classique, qui constitue une forme de sanction plus humaine, moins restrictive, offrant la possibilité de rester dans la famille et de conserver leur emploi. Elle est certes perçue comme une méthode de réinsertion, mais comme un revers de la médaille, les personnes qui ont expérimenté une telle méthode de suivi parlent de limitation significative de la liberté de mouvement, de surveillance constante conduisant à un sentiment de perte d'autonomie et à une pression psychologique importante[2982].

[2975] A. Gibbs, D. King, *Home Detention with Electronic Monitoring: The New Zealand Experience,* Criminology & Criminal justice, vol.3, 2003, p.199-211. https ://www.researchgate.net/publication/240721402_Home_Detention_with_Electronic_MonitoringThe_New_Zealand_Experience

[2976] Les établissements de santé mentale médico-légale du Royaume-Uni s'occupent de patients souffrant de problèmes de santé mentale qui posent un risque pour la sécurité publique.

[2977] Le Royaume-Uni est le premier pays d'Europe à utiliser la surveillance électronique en 1980.

[2978] S. Malek, D. Hearn, T. Fahy, J. Tully, T. Exworthy, *Legal and human rights issues in the use of electronic monitoring (using GPS „tracking" technology) in forensic mental health settings in the UK*, Medecine, Science and the Law, vol.63(4), 2023. p.309-315. https ://journals.sagepub.com/doi/10.1177/00258024231174820#body-ref-bibr3-00258024231174820

[2979] J. Cattell, T. Kenny, C. Lord, M. Wood, *Community Orders with Punitive Requirements: Results from the Offender Management Community Cohort Study*, London: Ministry of Justice, 2014.

[2980] Z. Hobson, A. Harrison, L. Duckworth, *Alcohol abstinence monitoring requirement: a review of process and performance from year 2*, MOPAC, Evidence and Insight, 2018. https ://www.london.gov.uk/sites/default/files/aamr_final_process_performance_y2_report_final.pdf

[2981] UK Ministry of Justice, *Electronic monitoring caseload*, Justice Data, 2024. https ://data.justice.gov.uk/contracts/electronic-monitoring

[2982] D. Vanhaelemesch, T. Vander Beken, S. Vandelvelde, *Punishment at home : offenders experiences with electronic monitoring*, European Journal of Criminology, vol.11, issue 3, 2013. https://journals.sagepub.com/doi/10.1177/1477370813493846

1038. Avantages économiques. La littérature mentionne également des aspects de la motivation économique, qui fait référence à « moins de personnes dans les prisons et à des coûts plus bas, en raison du fait qu'une journée en prison coûte plus cher qu'une journée de surveillance électronique »[2983]. Comparant les pays en Europe, les coûts de moi varient considérablement, d'environ 5 euros en Pologne à 100 euros dans la péninsule scandinave, étant inférieur aux coûts de l'emprisonnement traditionnel[2984]. Il est évident que même si le but principal de la surveillance électronique est de réduire les rechutes, certains de ces programmes ont également été créés pour réduire les coûts du système carcéral, ce qui procure un avantage économique important. En général, les coûts moins élevés associés à la surveillance électronique en font une alternative plus avantageuse à l'incarcération[2985].

Par conséquent, l'utilisation de la surveillance électronique dans l'environnement juridique vise à réduire les rechutes, à éviter le surpeuplement des pénitenciers et à apporter une solution plus humaine, éthique, respectueuse de la vie privée et moins coûteuse que les prisons traditionnelles. Cependant, les experts dans le domaine soulignent que le succès de cette méthode dépend de facteurs tels que la nature du soutien familial initial du crime, la capacité de[2986] l'individu à se réinsérer dans la société.

a). Surveillance électronique dans la lutte contre la violence domestique

1039. L'UE est également utilisée par les États membres dans le cadre de la mise en œuvre de la convention d'Istanbul[2987] dans les cas de violence domestique/violence à l'égard des femmes, dans les ordonnances d'interdiction d'urgence, les ordonnances de non-communication ou les ordonnances de protection (dans un contexte pénal ou civil). L'un des principes fondamentaux

---

[2983] Standards and Ethics in electronic monitoring, *Handbook for professionals responsible for the establishment and the use of Electronic Monitoring*, Conseil de l'Europe, 2015. p.15 https ://rm.coe.int/handbook-standards-ethics-in-electronic-monitoring-eng/16806ab9b0

[2984]F. Dünkel, *Electronic Monitoring in Europe – A Panacea for Reforming Criminal Sanctions Systems? A Critical Review,* Kriminologijos Studijos, 2018. p.69 https ://www.journals.vu.lt/kriminologijos-studijos/article/view/12674/11279

[2985] T. Kyckelhahn, *Direct Expenditures by Criminal Justice Funtion, 1982–2007 : Technical Report*, Bureau of Justice Statistics, 2011.

[2986] M. Finn, S. Muirhead-Steves, *The effectiveness of electronic monitoring with violent male parolees*, Justice Quarterly, vol.19, 2002. p.293-312. https ://www.researchgate.net/publication/248966595_The_effectiveness_of_electronic_monitoring_with_violent_male_parolees

[2987] *La Convention d'Istanbul*, officiellement connue sous le nom de *Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique*, est un instrument européen juridiquement contraignant visant à prévenir, protéger et combattre la violence à l'égard des femmes et la violence domestique. Il a été signé à Istanbul en 2011, d'où son nom vient. https ://rm.coe.int/168008482e. La Roumanie l'a ratifiée en 2016, par la *loi n° 30/2016*. https ://anes.gov.ro/wp-content/uploads/2017/09/2.-LEGE-Nr-30-din-2016-Conventia-de-la-Istanbul.pdf

de la Convention susmentionnée, conformément à l'article 7 de celle-ci, est « l'approche centrée sur la victime et fondée sur les droits ». L'approche de l'moi centrée sur la victime signifie que la victime doit toujours être informée des limites de la surveillance électronique et des mesures qu'elle doit prendre dans les situations d'urgence. Le droit à l'information est énoncé à l'article 19 de la Convention d'Istanbul, les informations transmises doivent inclure des détails sur le fonctionnement du matériel, l'attitude des autorités, les dysfonctionnements éventuels, ce qui se passe à la fin de la période de surveillance.

1040. Surveillance électrique bilatérale. Dans le cas de la violence familiale, outre la surveillance électronique de l'agresseur, la surveillance électronique de la victime peut parfois être exigée, ce qu'on appelle la surveillance électronique bilatérale. Actuellement, la surveillance électronique bilatérale est utilisée aux États-Unis, en Espagne et au Portugal, en particulier pour l'exécution des ordonnances de protection[2988].

Le respect des droits et des besoins de la victime, y compris le droit à la vie privée, est également essentiel. Le respect des droits et de la liberté de l'agresseur est tout aussi important, et les mesures du SME doivent être mises en œuvre de manière légale et proportionnée, en tenant compte[2989] du niveau de risque pour la victime. Cependant, certains inconvénients ont été identifiés pour les victimes dans les situations où le port du bracelet ou de la surveillance peut parfois être une source de stress, ou dans les situations où l'alarme se déclenche trop souvent, les victimes éprouvant un fort sentiment de peur et de panique.

1041. Efficacité de l'EM, prouvée dans des études. Selon des études américaines, l'utilisation du me dans de tels cas s'avère extrêmement efficace, permettant de surveiller les mouvements des agresseurs ainsi que d'alerter les autorités en cas de violation du périmètre, ce qui permet une intervention rapide. Dans ces circonstances, la méthode donne un sentiment de sécurité à la victime et en même temps réduit le risque de rechute[2990]. Une autre étude montre que la surveillance électronique accroît le sens des responsabilités chez les hommes violents, en étant conscients de la détection immédiate de toute inconduite. Il en résulte moins de violations des restrictions imposées et une réinsertion plus facile de ces types de criminels, surtout si la méthode est accompagnée de programmes de conseil et de réadaptation[2991].

[2988] Scottish Government, *Electronic Monitoring: Uses, Challenges & Successes*, Research and Analysis, 2019. https ://www.gov.scot/binaries/content/documents/govscot/publications/research-and-analysis/2019/04/electronic-monitoring-uses-challenges-successes/documents/electronic-monitoring-uses-challenges-successes/electronic-monitoring-uses-challenges-successes/govscot%3Adocument/electronic-monitoring-uses-challenges-successes.pdf

[2989] *Fact sheet Istanbul Convention*, Wave network, 2016. https ://fileserver.wave-network.org/researchreports/2016_WAVEFactSheetIC.pdf

[2990] E. Erez, et al., *Monitoring Technologies and Domestic Violence: An Evaluation Study*, NCJRS Report, 2012. https ://www.ojp.gov/pdffiles1/nij/grants/238910.pdf

[2991] M.A. Finn, S. Muirhead-Steves, *The effectiveness of electronic monitoring with violent male parolees*, Justice Quarterly, vol.19(2), 2002, p.293-312. https ://doi.org/10.1080/07418820200095251

Les analyses sur ce sujet montrent également que la surveillance électronique a entraîné une augmentation de la sécurité des femmes victimes de violence conjugale, bien que le taux de rechute soit resté le même que dans le cas de la prison traditionnelle (50 %)[2992].

1042. Instrument complémentaire dans le système pénal. Si elle est analysée de ce point de vue, il est vrai que la surveillance électronique pourrait conduire à moins de personnes dans les prisons, à une réduction des coûts, à une plus grande sécurité pour les victimes de violence domestique, à de meilleurs liens sociaux pour les criminels, etc. Cependant, certaines voix soulignent que la surveillance électronique ne devrait pas être utilisé comme panacée pour résoudre les problèmes du système judiciaire. Bien qu'il présente de nombreux avantages, vu comme un exemple de bonne volonté technologique, il doit être considéré comme un instrument complémentaire dans le système pénal et l'obtention des résultats escomptés nécessite une utilisation combinée à d'autres formes d'intervention et de soutien[2993].

b). Inconvénients de la surveillance électronique – « prison électronique »

1043. EM, soutenue par l'ONU. Au niveau mondial, l'Office des Nations Unies contre la drogue et le crime (ONUDC)[2994] promeut des mesures alternatives à l'emprisonnement, y compris au sein de l'UE. Les arguments de l'organisation sont que cette méthode permet de réduire les coûts, d'éviter la congestion des prisons et de protéger les droits de l'homme[2995].

1044. Critiques adressées à l'EM. Mais il y a aussi des voix qui critiquent la mesure, soulignant les inconvénients tels que stigmatiser et humilier les personnes surveillées, étendre la surveillance et le contrôle des autorités sur la population, avec un impact important sur la vie privée de l'utilisateur et de sa famille[2996]. Dans une étude de 2014 sur l'impact de l'EMI sur les

---

[2992] R. Winter, E. Herrlander Birgerson, R. Julian, R. Frey, P. Lucas, K. Norris, M. Matthewson, *Evaluation of Project vigilance : Electronic Monitoring of Family Violence Offenders* , Tasmanian Institute of Law Enforcement Studies (TILES), 2021. https ://www.police.tas.gov.au/uploads/Final-TILES-Report-V.2-Project-Vigilance.pdf

[2993] M. DeMichele, *Electronic Monitoring : It is a Tool, not a Silver Bullet*, Criminology & Public Policy, vol.13, 2014, p.393-400. https ://doi.org/10.1111/1745-9133.12089

[2994] L'ONUDC est une organisation mondiale qui lutte contre la drogue, la criminalité internationale et le terrorisme, élabore et met en œuvre des programmes adaptés aux besoins spécifiques des pays, promouvant la santé, la justice et la sécurité dans le monde entier. Elle a été fondée en 1997 et a son siège à Vienne. https ://www.unodc.org/unodc/en/about-unodc/contact-us.html

[2995] ONUDC. Handbook of basic principles and promising practices on alternatives to imprisonment. https ://www.unodc.org/documents/justice-and-prison-reform/crimeprevention/Handbook_of_basic_principles_and_promising_practices_on_Alternatives_to_Imprisonment.pdf

[2996] P. de Andrés, M. N. Rodríguez, *L'utilisation de bracelets électroniques de surveillance comme mesure alternative à l'emprisonnement au Panama.* Avis consultatif technique no. 002/2013, adressée au Ministère public et au Ministère du Gouvernement du Panama, Office des Nations Unies contre la drogue et le crime, Bureau régional pour l'Amérique centrale et les Caraïbes, 2013. http ://www.antoniocasella.eu/nume/Unodc_electronic_Panama_2013.pdf

personnes surveillées, les auteurs ont conclu que, bien que l'alternative soit perçue comme plus douce que la prison, elle peut causer une détresse psychologique comme l'anxiété, l'isolement social et l'isolement social, un manque d'intimité ou manque de contrôle sur sa vie quotidienne aussi fort que l'emprisonnement traditionnel[2997]. Aussi, en analysant l'utilisation de la surveillance électronique pour la surveillance et le suivi des immigrants aux États-Unis, les experts ont montré que cette mesure n'était pas neutre ou objective, mais une forme de contrôle social, qui a contribué à leur marginalisation et stigmatisation. La surveillance électronique est considérée comme une « punition étendue » qui porte atteinte au droit à la vie privée des migrants[2998] et provoque des inégalités structurelles.

1045. Risque d'intrusion dans la vie privée. Il y a aussi des voix qui soutiennent qu'au lieu de réduire le nombre de personnes incarcérées, la surveillance électronique peut mener à la surveillance et au contrôle d'un nombre beaucoup plus important de personnes, y compris celles qui autrement ne seraient pas soumises à une telle surveillance (par exemple, la famille ou les proches des criminels sous la surveillance électronique).[2999]. Cependant, la population incarcérée, en augmentation continue jusqu'au début du XXIe siècle, est actuellement en baisse, en particulier en Europe centrale et orientale, l'explication la plus pertinente étant probablement la baisse des taux de criminalité[3000].

L'intrusion dans la vie privée et les effets psychologiques qui peuvent me causer restent un sujet d'actualité. Certaines voix soutiennent que la réforme de la justice devrait être fondée sur la prévention de la criminalité et la promotion d'un jugement équitable plutôt que sur des mesures punitives et une surveillance coercitive[3001].

1046. Naissance du terme « prison électronique ». Cette « prison électronique », comme l'appelle Weisbury, entraîne de sévères restrictions à la liberté de mouvement, à la vie privée. En outre, il peut conduire à de nouvelles sanctions, des données de déficiences techniques ou administratives du système de suivi (par exemple, la perte du signal GPS), qui ne sont pas des

---

[2997] B.K. Payne, D.C. May, P.B. Wood, *The „pains" of electronic monitoring: a slap on the wrist or just as bad as prison?,* Criminal Justice Studies, vol.27(2), 2014. p.133–148. https ://doi.org/10.1080/1478601X.2014.885755

[2998] M.G. Martinez-Aranda, *Extended punishment: criminalising immigrants through surveillance technology,* Journal of Ethics and Migration Studies, vol.48(1), 2020, p.74–91. https ://doi.org/10.1080/1369183X.2020.1822159

[2999] F. Dünkel, *Electronic monitoring–Some critical issues*, Liber Amicorum Gerben Bruinsma. The Hague: Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR*)*, 2017, p.108-117. https ://scholar.google.com/scholar_lookup?title=Electronic+monitoring+%E2%80%93+Some+critical+issues&author=F+D%C3%BCnkel&publication_year=2017&pages=108-117

[3000] F. Duenkel, *European penology : The rise and fall of prison population rates in Europe in times of migrant crises and terrorism,* European Journal of Criminology, vol.14, 2017. p.629-653. https ://www.researchgate.net/publication/321132730_European_penology_The_rise_and_fall_of_prison_population_rates_in_Europe_in_times_of_migrant_crises_and_terrorism

[3001] C. Lum, D. S. Nagin, „*Reinventing American Policing"*, Crime and Justice vol.46 (1), 2017. p.339–93. https ://www.journals.uchicago.edu/doi/full/10.1086/688462

actes criminels, mais peuvent apporter de nouvelles accusations ainsi que[3002] l'extension de la période de peine.

En 2023, dans la recherche sur l'efficacité de la surveillance électronique, les avantages évidents tels que la présentation des défendeurs au procès ou la diminution des rechutes ont été mis en évidence, mais les effets négatifs tels que la surveillance intrusive avec des implications psychologiques et sociales importantes ont également été mis en évidence. L'étude suggère que la décision de surveiller la surveillance électronique devrait être utilisée avec discernement, adaptée individuellement à chaque accusé et proportionnée au délit concerné[3003].

Il existe une multitude d'avantages et de inconvénients dans la mise en œuvre de bracelets électroniques à partir de différentes perspectives, allant des meilleures pratiques et réglementations internationales actuelles (européennes et nationales) jusqu'aux possibilités offertes par les progrès actuels de l'électronique par rapport au niveau des ressources financières publiques allouées à ces fins par les décideurs des gouvernements nationaux[3004]. La prévention des risques dus aux limitations technologiques implique une augmentation significative des ressources financières, du personnel hautement qualifié et des plans alternatifs aux lacunes susmentionnées Tout cela rend parfois les décideurs réservés à la mise en place de tels systèmes de surveillance.

B. Utilisation de la surveillance électronique dans les États européens

1047. Leviers législatifs. Deux grandes lignes pour l'UE des délinquants à haut risque sont actuellement adoptées au niveau international : une ligne législative, qui exige et réglemente l'utilisation de cette technologie, et une ligne budgétaire, qui met en évidence les économies et l'efficacité de cette méthode par rapport à la prison traditionnelle.

En ce qui concerne la législation, la surveillance électronique est réglementée à grande échelle en Europe, aux États-Unis et en Australie, avec une large application : dans les différentes étapes d'un procès criminel, comme condition de libération sous caution, comme méthode alternative à une peine privative de liberté, pour la surveillance des criminels après leur libération de prison, comme moyen de protection, etc.[3005] Les premières tentatives

[3002] K. Weisbury, et all., *Electronic prisons: The Operation of Ankle Monitoring in the Criminal Legal System,* GWU Law School Public Law Research Paper No.41, 2021. Available at SSRN : https ://ssrn.com/abstract=3930296

[3003] R. Rivera, *Release, detain or surveil? The Effects of electronic monitoring on Defender Outcomes*, Unpublished manuscript, Columbia University, 2023. https ://www.columbia.edu/~rgr2122/romanrivera_jmp.pdf

[3004] J. Belur, A. Thornton, I. Tompson, M. Manning, A. Sidebottom, K. Bowers, *A systematic review of the effectiveness of the electronic monitoring of offenders*, Journal of Criminal Justice, 2020. p.68.

[3005] R. Geoghegan, *Future of corrections: Exploring the use of electronic monitoring,* Policy Exchange, 2012. https ://www.academia.edu/6593718/Future_of_Corrections_Exploring_the_use_of_Electronic_Monitoring

d'utilisation de moi ont eu lieu au début de 90 au Royaume-Uni, suivi par la Suède et les Pays-Bas[3006]. Actuellement, la Belgique et l'Angleterre sont parmi les pays qui ont le programme Best me, étant extrêmement efficace pour réduire la population incarcérée[3007]. Le rapport de 2014 de l'UE sur l'utilisation de la surveillance électronique place l'Angleterre et le pays de Galles au premier rang en Europe et aux deux tiers dans le monde après les États-Unis, avec un nombre de 105 000 nouveaux cas[3008].

a). Conseil de l'Europe : méthode alternative aux peines privatives de liberté

1048. Justice pénale. L'utilisation de la surveillance électronique dans les systèmes de justice pénale est réglementée par le Conseil de l'Europe par la Recommandation CM/Rec(2014)4[3009]. Elle encourage le recours à la surveillance électronique comme méthode alternative aux peines privatives de liberté, tout en fixant des limites claires aux droits fondamentaux des personnes concernées, y compris le droit à la dignité et à la vie privée.

Une façon de protéger les droits fondamentaux est de réglementer le consentement. CM/Rec(2014)4 recommande le consentement et la coopération avec la personne à surveiller électroniquement ou le consentement de la victime (si une mesure de protection est impliquée), mais permet la mise en œuvre conformément à la législation nationale[3010]. Dans la plupart des pays, le consentement est requis, mais la manière et le moment de l'obtenir diffèrent, parfois il n'y a pas de réelle possibilité de refuser de le signer, ce qui soulève des questions sur le caractère « librement informé » (qui est également obligatoire pour tout type de consentement). Le seul pays qui n'exige pas le consentement de l'UE est l'Allemagne, car ce type de surveillance n'est utilisé que pour les délits très graves[3011].

[3006] M. Nellis, *Understanding the electronic monitoring of offenders in Europe: expansion, regulation and prospects,* Crime Law Soc Change, vol.62, 2014. p.489–510. https ://doi.org/10.1007/s10611-014-9540-8

[3007] A. Hucklesby, K. Beyens, et al., *Electronic Monitoring in Europe: Uses, Challenges & Successes*, Brussels, 2016. https ://www.europris.org/wp-content/uploads/EM-in-EU-summary-report.pdf

[3008] *Rapport de l'UE sur l'utilisation de la surveillance électronique des délinquants*, Journal officiel de l'Union européenne, 2014. https ://www.justice.gov.md/public/files/file/reforma_sectorul_justitiei/proiecte/proiect_de_asist_tehn_4/Electronic_Monitoring_ROM.pdf

[3009] *Recommendation CM/Rec(2014)4 of the Committee of Ministers to member States on electronic monitoring*. http ://www.europeanrights.eu/public/atti/2014_-_4__ing.pdf

[3010] Ibidem, page 6.

[3011] A. Hucklesby, K. Beyens, M. Boone, F. Dünkel, G. McIvor, H. Graham, *Creativity and Effectiveness in the use of electronic monitoring: a case study of five jurisdictions*, Conseil de l'Europe, 2016. https ://dspace.stir.ac.uk/bitstream/1893/23603/1/Electronic%20Monitoring%20Comparative%20Synthesis%20Report.pdf

b). Rapport GREVIO sur la mise en œuvre de la surveillance électronique

1049. La violence envers les femmes, un problème social d'une grande importance. Une attention particulière est accordée en Europe à l'utilisation de l'EM pour prévenir et combattre la violence à l'égard des femmes. Par conséquent, outre la mise en œuvre de la Convention d'Istanbul de 2011 (mentionnée ci-dessus), le Conseil de l'Europe approuve également la mise en place d'un mécanisme de suivi de la mise en œuvre de cette Convention dans chaque Etat membre Ce mécanisme est connu sous le nom de GREVIO (groupe d'experts contre la violence à l'égard des femmes et la violence domestique)[3012]. L'objectif principal du GREVIO est d'analyser les progrès réalisés contre la violence à l'égard des femmes dans chaque pays. À l'instar de la recommandation du Conseil de l'Europe, le GREVIO souligne également l'importance du consentement, qui est essentiel pour protéger les droits des victimes. Dans ce cas, on peut parler d'un double consentement : un de la victime et un de l'agresseur. En outre, il insiste pour que la victime soit informée de manière correcte et transparente des capacités et des limites de la technologie afin de pouvoir agir en connaissance de cause. Les réglementations varient d'un pays à l'autre[3013]. Par exemple, le consentement de la victime est obligatoire en Roumanie, et le consentement de l'auteur de l'infraction uniquement lorsque l'EM est utilisée comme mesure de détention alternative. En Allemagne et en France, le consentement de l'agresseur n'est pas requis. En Espagne, qui dispose de l'un des meilleurs systèmes de moi, seul le consentement de la victime est requis.

1050. Progrès dans la lutte contre la violence à l'égard des femmes. Dans le rapport GREVIO sur la Roumanie de juin 2022, les efforts considérables déployés par le pays pour mettre en place une législation adéquate sont reconnus, parmi les progrès notables figurent l'amélioration de la *loi n° 217 du 22 mai 2003*[3014], l'introduction d'ordonnances de protection et l'inclusion de la cyberviolence en tant que forme de violence domestique. Toutefois, le rapport souligne également la nécessité de disposer de ressources financières suffisantes pour mettre en œuvre les mesures prévues par[3015] la loi.

[3012] *Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique*, Chapitre 9, article 66, Istanbul, Conseil de l'Europe, 2011. https ://rm.coe.int/168008482e

[3013] GREVIO, *Mid-term Horizontal Review of GREVIO baseline evaluation reports*, Conseil de l'Europe, 2022. https ://edoc.coe.int/en/violence-against-women/11030-mid-term-horizontal-review-of-grevio-baseline-evaluation-reports.html

[3014] *Loi n° 217 du 22 mai 2003* (*republiée*)
https ://legislatie.just.ro/Public/DetaliiDocument/44014

[3015] *Rapport d'évaluation (de référence) du GREVIO sur les mesures législatives et autres donnant effet aux dispositions de la Convention du Conseil de l'Europe sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique* (Convention d'Istanbul) ROUMANIE https ://rm.coe.int/final-report-on-romania/1680a6e439

Au 31 janvier 2023, selon l'analyse SPACE II[3016], environ 1 300 000 personnes étaient en probation[3017] (ce qui correspond à un taux de 164 personnes pour 100 000 habitants). Les taux les plus élevés sont observés en Pologne (700/100 000 habitants), en Turquie et en Moldavie, et les plus faibles en Macédoine du Nord (9,7/100,00 habitants) et en Grèce[3018].

c). L'Allemagne, réticente à utiliser la surveillance électronique

1051. Accélération législative. En Allemagne, la justice est réticente à me faire appel, probablement parce qu'elle ne fait pas face à une surpopulation carcérale et dispose d'un service de probation efficace[3019]. En général, la surveillance électronique n'est pas une forme de fraude, mais selon le Code pénal, il peut être utilisé pour la surveillance des délinquants à haut risque, après avoir purgé leur peine (article 68b 1) n° 12), pour la suspension de la peine (article 56c), pour la libération anticipée (articles 57, 57a),[3020] comme mesure alternative d'arrestation préventive (Article 116 du Code de procédure pénale)[3021]. En 2008, la CEDH a examiné l'affaire M. c. Allemagne (no 19359/04)[3022], dans laquelle un criminel à haut risque accuse l'État de violer son droit à la liberté (garanti par l'article 5 de la CEDH), prolongeant la détention préventive pour une période prolongée après l'exécution de sa peine initiale. La CEDH surmonte le cas du requérant et crée un précédent, l'Allemagne devant libérer plusieurs criminels dangereux en détention provisoire. C'est le moment où le pays de Goethe accélère la mise en œuvre et la réglementation de la surveillance électronique[3023].

[3016] Les statistiques criminelles annuelles du Conseil de l'Europe (SPACE) sont une série d'analyses sur les prisons et les institutions pénales (SPACE I) ou sur les mesures et sanctions impliquant une privation de liberté (SPACE II). https ://wp.unil.ch/space/

[3017] Selon la *Recommandation CM/Rec (2010)1* du Conseil de l'Europe, la probation est définie comme « *la mise en œuvre dans la communauté de sanctions et de mesures définies par la loi et imposées à un criminel* ». Ces sanctions comprennent la surveillance électronique accompagnée de programmes de réadaptation. La définition de la probation figure à l'annexe I de la présente Recommandation. https ://cep-probation.org/wp-content/uploads/2018/10/CoE-probation-rules-recommendation.pdf

[3018] F. Marcelo, L. Molnar, E. Cocco*, Probation and Prisons in Europe, 2023 : Key findings of the SPACE reports*, Conseil de l'Europe, 2024. https ://wp.unil.ch/space/files/2024/06/Key-Findings_Prisoners-and-Probationers-SPACE_240625.pdf

[3019] F. Dünkel, C. Thiele, J. Treig, *« You'll never stand-alone » : Electronic monitoring in Germany,* European Journal of Probation, vol.9(1), 2017, p.28-45. https ://doi.org/10.1177/2066220317697657

[3020] *German Criminal Code (Strafgesetzbuch – StGB)* https ://www.gesetze-im-internet.de/englisch_stgb/

[3021] *German Code of Criminal Procedure (Strafprozeßordnung-StPO*) https ://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

[3022] *M. c. Germany, no. 19359/04,* 1er juillet 2008.

[3023] F. Dünkel, C. Thiele, J. Treig, *Electronic Monitoring in Germany*, CEP, 2016. http ://www.antoniocasella.eu/nume/Dunkel_2016.pdf

d). La Norvège n'utilise la SE que dans les cas de violence conjugale

1052. Prisons norvégiennes et réhabilitation. Réglementé avec beaucoup de controverse en 2008[3024], l'utilisation de la SE en Norvège est de nature limitée et est plus orientée vers les cas de violence domestique. Entre 2013 et 2018, il n'y a eu que 14 peines impliquant un contrôle électronique. Une raison pourrait être donnée par les coûts de mise en œuvre, qui étaient parmi les plus élevés de toute l'Europe (environ 5 millions d'euros)[3025]. La mesure n'a peut-être pas trouvé sa place également en raison de la politique scandinave d'exceptionnalisme déjà pratiquée dans les prisons norvégiennes. Il est centré sur le respect des droits fondamentaux, sur des conditions décentes, avec un accent sur les mesures de réhabilitation et de réinsertion des criminels[3026].

e). En Suède, la SE réduit la récidive et facilite la réinsertion sociale

1053. En Suède, la mesure de la surveillance électronique a été introduite en 1994, et le pays travaille depuis 80 à l'élaboration et à la mise en œuvre de mesures alternatives aux prisons traditionnelles. Le nombre d'utilisateurs de la SE a augmenté d'année en année, atteignant 3000 criminels[3027] en 2012. Une étude sur les avantages de l'utilisation de la surveillance électronique a conclu que c'est une méthode efficace pour réduire les rechutes et faciliter la réinsertion sociale, fournissant un bénéfice humain net aux personnes libérées. Il réduit également les coûts du système judiciaire. L'analyse montre toutefois que le succès de la mesure dépend du soutien social, économique et familial apporté aux personnes surveillées[3028].

f). Belgique : Réduction la surpopulation carcérale

[3024] *Loi relative à l'exécution des peines* etc. (The Execution of Sentences Act) *Chapitre 1. Le champ d'application de la loi et les principes généraux de l'exécution des peines, al.16, paragraphe 2* https ://www.regjeringen.no/en/dokumenter/Act-relating-to-the-execution-of-sentences-etc-/id420593/

[3025] M.K. Øster, T. Rokkan, „*The Norwegian Approach to Electronic Monitoring: Changing the System and Making a Difference",* Federal Sentencing Reporter, vol.31, no.1, 2018. pp.75-84. https ://www.jstor.org/stable/26586189.consulté le 28 nov 2024.

[3026] A. Eriksson, J. Pratt, *In defence of Scandinavian exceptionalism*, Routledge, 2012. https ://www.researchgate.net/publication/259610240_In_defence_of_Scandinavian_exceptionalism

[3027] J. Bungerfeldt, *Old and New Uses of electronic monitoring in Sweden*, Centre for Crime and Justice studies, 2015. https ://www.crimeandjustice.org.uk/sites/crimeandjustice.org.uk/files/09627251.2014.902193_0.pdf

[3028] F. Marklund, S. Holmberg, *Effects of early release from prison using electronic tagging in Sweden*, J Exp Criminol vol.5, 2019. p.41–61 https ://doi.org/10.1007/s11292-008-9064-2

1054. Réduction la surpopulation carcérale. En Belgique, la surveillance électronique a été mise en œuvre à la fin des années 1990 dans le but de réduire la surpopulation carcérale[3029] et d'encourager la réinsertion, une mesure qui s'inscrivait initialement dans un cadre de réhabilitation plus large. Au fil du temps, cependant, il y a une transition dans l'utilisation de la SE et sa transformation en sanction autonome[3030]. En 2016, l'Europe loue l'approche proactive ainsi que l'utilisation généralisée de la SE dans ce pays[3031].

g). Différence de vision entre l'Europe et les États-Unis sur l'utilisation de la surveillance

1055. Respect de la vie privée. Le 19 février 2014, lors de la 1192e réunion des délégués des Ministres, l'Union Européenne a publié un ensemble de recommandations sur l'utilisation de la surveillance électronique dans les procédures pénales[3032]. L'objectif de la recommandation est d'encourager le recours à la surveillance électronique comme alternative à la détention, tout en maintenant un équilibre entre la sécurité publique et le respect des droits fondamentaux. Parmi les principes de base de ce type de surveillance figurent le respect de la proportion de délits et de peines et, en même temps, le respect de la vie privée de la personne surveillée[3033].

Par rapport à la réglementation d'outre-mer, nous constatons la grande importance que le Conseil de l'Europe accorde au respect de la vie privée dans l'utilisation de la surveillance électronique[3034]. En Europe, elle est considérée comme une alternative à l'incarcération, dans le but d'éviter la surpopulation carcérale et de faciliter la réinsertion sociale, tandis qu'aux États-Unis, la technologie est principalement utilisée pour étendre la surveillance. La législation

[3029] E. Maes, B. Mine, *Some Reflections on the Possible Introduction of Electronic Monitoring as an Alternative to Pre-trial Detention in Belgium*, Howard Journal, vol.52(2), 2013. p.144-165. https ://onlinelibrary.wiley.com/doi/full/10.1111/hojo.12008

[3030] K. Beyens, M. Roosen, *Electronic monitoring and reintegration in Belgium*, European Journal of Probation, vol.9(1), 2017, p.11-27. https ://doi.org/10.1177/2066220317704132

[3031] A. Hucklesby, K. Beyens, et al., *Electronic Monitoring in Europe: Uses, Challenges & Successes*, EuroPris, European Commission Research, 2016. https ://www.europris.org/wp-content/uploads/EM-in-EU-summary-report.pdf

[3032] *Recommendation CM/Rec(2014)4* of the Committee of Ministers to member States on electronic monitoring (Adopted by the Committee of Ministers on 19th February 2014, at the 1192nd meeting of the Ministers' Deputies http ://www.europeanrights.eu/public/atti/2014_-_4__ing.pdf

[3033] M. Nellis, *Standards and Ethics in electronic monitoring, Handbook for professionals responsible for the establishment and the use of Electronic Monitoring*, Conseil de l'Europe, 2015. https ://rm.coe.int/handbook-standards-ethics-in-electronic-monitoring-eng/16806ab9b0

[3034] M. Mayer, R. Haverkamp, R. Levy(Eds.), *Will electronic monitoring have a future in Europe,* Frieburg , Max Planck Institute, 2003.
https ://www.ojp.gov/ncjrs/virtual-library/abstracts/will-electronic-monitoring-have-future-europe

européenne exige également le consentement de la personne surveillée, alors qu'aux États-Unis, il peut être appliqué de manière coercitive, sans évaluer[3035] l'impact sur la vie privée.

§2. LA SURVEILLANCE ÉLECTRONIQUE DANS LES SYSTÈMES JURIDIQUES FRANÇAIS ET ROUMAIN

1056. Considérations éthiques sur la surveillance électronique. Il existe actuellement de nombreux débats nationaux/internationaux sur les implications éthiques de l'IME. Le sujet est abordé dans la Recommandation du Conseil de l'Europe sur la surveillance électronique cm/Rec (2014)4, qui interdit l'utilisation de l'EM pour causer des souffrances physiques ou mentales au suspect/délinquant. Cela signifie que des éléments tels que l'âge, le sexe et les handicaps éventuels doivent être pris en compte avant de recourir à ce type de surveillance. En outre, compte tenu des évolutions technologiques, il est nécessaire d'éviter toute intrusion injustifiée dans[3036] la vie privée des personnes concernées. Les chercheurs ont défini deux principes éthiques en matière de surveillance électronique : « éthique de la punition, du contrôle et des soins » et « éthique du changement technologique »[3037], principes qui s'appliquent en particulier dans les cas de violence domestique ou de harcèlement.

Une étude de 2009 a examiné les aspects sociaux et psychologiques qui influent sur le respect par les criminels des ordonnances d'arrestation à domicile contrôlées électroniquement. Il suggère que le SME peut être efficace s'il est encadré dans un système d'éthique qui inclut le soutien social, le soutien familial, de bonnes relations avec les autorités, le plein respect des conditions d'arrestation[3038].

1057. La sensation de « punition invisible ». Une autre considération éthique est la liberté « illusoire » que certains prisonniers ressentent lorsqu'ils sont soumis à une surveillance électronique comme alternative à l'emprisonnement traditionnel. Une étude menée en Belgique en 2012 montre que la surveillance électronique est d'une part une opportunité de liberté, d'intégration dans la société, de maintien des relations sociales et familiales, mais d'autre part

[3035] J.R. Lilly, *The 2014 Council of Europe recommendation on electronic monitoring : an American perspective,* Crime Law Soc Change, vol.62, 2014. p.511–513 https ://link.springer.com/article/10.1007/s10611-014-9539-1#Bib1

[3036] Ibidem, page 6-7

[3037] M.Nellis, *Standards and Ethics in electronic monitoring: Handbook for professionals responsible for the establishment and the use of Electronic Monitoring*, Council of Europe, 2015. https ://rm.coe.int/handbook-standards-ethics-in-electronic-monitoring-eng/16806ab9b0

[3038] A. Hucklesby, „*Understanding Offenders Compliance: A Case Study of Electronically Monitored Curfew Orders"*, Journal of Law and Society, vol.36, no.2, 2009. pp.248-71. http ://www.jstor.org/stable/40206889. Consulté le 29 novembre 2024.

une forme de contrôle permanent générant anxiété et stress[3039]. Une autre étude, également menée en Belgique, a donné des résultats similaires. Bien que la surveillance électronique soit évidemment plus facilement acceptée que la prison traditionnelle, étant perçu comme une « punition invisible », de nombreux criminels ont signalé des tensions et des conflits avec les membres de leur famille, principalement en raison de leur présence constante à la maison et de la perception que la « maison » est devenue un lieu de punition[3040].

Certains auteurs ont étudié d'un point de vue éthique l'impact que la facturation d'un parent a sur les enfants, montrant un impact négatif sur leur éducation et leur avenir. L'impact est déterminé par l'instabilité familiale, la stigmatisation sociale et les difficultés économiques résultant de l'incarcération[3041]. Ces phénomènes, bien qu'ils ne puissent pas être entièrement combattus, peuvent être réduits en utilisant moi comme méthode alternative d'incarcération[3042].

A. Roumanie - Loi no. 146/2021 sur la surveillance électronique

1058. La Roumanie, en tant qu'État membre, a progressivement adopté des mesures pour se conformer aux principes de la Recommandation européenne CM/Rec (2014)4. C'est pourquoi, en 2021, il a adopté la loi n° 146 sur le contrôle électronique dans les procédures pénales judiciaires et d'exécution[3043]. Il réglemente la mise en place, l'organisation et le fonctionnement du système numérique de la surveillance électronique (SIME) en Roumanie. Conformément à la loi ci-dessus, la surveillance électronique en Roumanie peut être appliquée dans les cas suivants :

Assignation à résidence/contrôle judiciaire, surveillance électronique assurant l'interdiction de quitter le domicile ou un certain périmètre établi[3044]

Ordonnance de protection/interdiction dans certains domaines, garantissant l'interdiction pour le défendeur de s'adresser à la victime[3045]

[3039] D. Vanhaelemesch, T. Vander Beken, „*Electronic Monitoring: Convicts' Experiences in Belgium*", Social Conflicts, Citizens and Policing, vol.6, Maklu, 2012. p.77-96. http ://hdl.handle.net/1854/LU-3135529

[3040] D. Vanhaelemesch, T. Vander Beken, *Punishment at home/ Offenders' experiences with electronic monitoring*, European Journal of Criminology, vol.11(3), 2014. p.273-287. https ://doi.org/10.1177/1477370813493846

[3041] C. Arteaga, *Parental Incarceration and Children's Educational Attainment*, The Review of Economics and Statistics, vol.105 (6) : 2023 . p.1394–1410. deux : https ://doi.org/10.1162/rest_a_01129

[3042] J. Grenet, H. Grönqvist, S. Niknami, *The effects of electronic monitoring on offenders and their families,* Journal of Public Economics, vol.230, 2024. 10.1016/j.jpubeco.2023.105051

[3043] *Loi n° 146 du 17 mai 2021 relative au contrôle électronique dans les procédures judiciaires et pénales d'exécution*.

[3044] Code de procédure pénale du 1er juillet 2010 (loi no 135/2010).

[3045] *Loi n° 217 du 22 mai 2003 (*republiée*) pour la prévention et la lutte contre la violence domestique.* https ://legislatie.just.ro/Public/DetaliiDocumentAfis/231227

Surveillance à distance de l'exécution des différentes peines[3046] : libération conditionnelle/service d'intérêt général.

L'application de la décision de protection européenne, qui assure la protection des personnes en danger lorsqu'elles se déplacent ou s'installent dans un État de[3047] l'Union Européenne.

1059. Mise en œuvre de l'EM en Roumanie. Dans la première phase, à compter du 1er octobre 2022, le contrôle électronique a été appliqué dans un système pilote de décisions de protection (y compris le respect de la décision de protection européenne)[3048]. Par la suite, depuis le 1er octobre 2024, il a également appliqué dans l'exécution du contrôle judiciaire et des mesures d'assignation à résidence (conformément à l'article 40 de la loi n° 146 du 17 mai 2021)[3049].

Conformément à l'article 33 de la loi 146/2021, dans le cadre du contrôle électronique, l'organe de contrôle ainsi que l'organe judiciaire ont accès aux données de localisation, tandis que l'article 45 réglemente l'accès aux « documents, images, enregistrements audio-vidéo ou tout autre document »[3050], qui évidemment, cela soulève des questions sur l'intrusion dans la vie privée. En ce qui concerne le respect de la vie privée du point de vue de la protection des données personnelles, la loi n° 146/2021, dans son article 37, stipule clairement le respect des dispositions légales. En outre, les données personnelles seront conservées pendant une période de 2 ans après la fin du suivi électronique au sein du SIME, après quoi elles seront supprimées par une procédure irréversible.

1060. Le système numérique de surveillance électronique (SIME) est un ensemble de systèmes d'information qui utilisent des dispositifs de surveillance électronique permettant le suivi en temps réel des personnes surveillées[3051]. Après avoir été initialement mis en œuvre dans plusieurs comtés pilotes, à partir du 1er octobre 2024, il s'est étendu à 18 autres comtés. En ce qui concerne la protection des intérêts de la personne, la loi garantit le droit de la personne

---

[3046] *Loi no 254 du 19 juillet 2013 relative à l'exécution des peines et mesures privatives de liberté ordonnées par les organes judiciaires au cours du procès pénal.* https ://legislatie.just.ro/Public/DetaliiDocumentAfis/220250

[3047] *Loi n° 151 du 13 juillet 2016 sur la décision de protection européenne, modifiant et complétant certains actes normatifs*. https ://legislatie.just.ro/Public/DetaliiDocumentAfis/180244

[3048] *Ordonnance d'urgence n° 14 du 23 février 2022 modifiant la loi n° 146/2021 relative au contrôle électronique dans les procédures judiciaires et pénales d'exécution.* https ://legislatie.just.ro/Public/DetaliiDocumentAfis/251898

[3049] *Ordonnance d'urgence n° 61 du 13 juin 2024 modifiant et complétant la loi n° 146/2021 relative au contrôle électronique dans les procédures judiciaires et pénales d'exécution*. https ://legislatie.just.ro/Public/DetaliiDocumentAfis/284040

[3050] *Loi n° 146 du 17 mai 2021 relative au contrôle électronique dans les procédures judiciaires et exécutoires pénales* (promulguée le 18 mai 2021 par le Décret n° 626/2021), articles 33 et 45. https ://snppc.ro/uploads/fisiere/articole/204910-Legea-146-2021.pdf

[3051] *Loi sur la surveillance électronique dans les procédures judiciaires et pénales, ainsi que modifiant et complétant certains actes normatifs*. https ://webapp.mai.gov.ro/frontend/documente_transparenta/222_1563289097_proiect%20Lege%20SIME_08072019%20negru.pdf

à la vie privée, compte tenu de[3052] la nature personnelle des informations qui sont diffusées. SIME s'aligne sur le RGPD en respectant « la vie privée dès la conception ». Ce concept, essentiel dans la protection des données à caractère personnel, implique le respect des méthodes de protection de la vie privée à toutes les étapes[3053] du développement d'un système et pendant toute la durée – de la collecte, du stockage à l'utilisation et après suppression. Le concept de protection des données « dès la conception » est garanti par l'article 25 et le considérant 78 du RGPD[3054].

a). De la violence domestique aux procédures pénales

1061. En fait, en Roumanie, la possibilité de surveillance électronique a été réglementée il y a quelque temps. En 2003, la loi no 217 sur la prévention et la lutte contre la violence familiale prévoit son utilisation comme mesure de protection en cas de violence familiale[3055]. En 2007, elle est réglementée pendant le procès ou pendant l'enquête pénale[3056]. En 2010, le nouveau Code de procédure pénale prévoit la surveillance électronique et l'assignation à résidence[3057], de sorte qu'à partir de 2013, elle peut également être utilisée en cas de libération pour travaux d'intérêt général[3058]. En ce qui concerne l'intrusion dans la vie privée, le Parlement roumain a souligné en 2021 que la surveillance électronique est une ingérence dans le droit à la vie privée, qui est toutefois nécessaire pour assurer la sécurité et atteindre les objectifs de la justice[3059].

Toutefois, des investissements importants dans les ressources humaines et l'équipement sont nécessaires en raison du fait que la technologie GPS est utilisée pour surveiller les criminels à haut risque. Il faut aussi beaucoup d'efforts pour adapter la législation et former à la fois le personnel et le personnel du système judiciaire. C'est probablement l'une des raisons

---

[3052] *Loi sur la surveillance électronique dans les procédures judiciaires et pénales, ainsi que modifiant et complétant certains actes normatifs,* expunere de motive. https ://www.cdep.ro/proiecte/2020/100/20/9/em180.pdf, page 26

[3053] *What does data protection „by design" and „by default" mean?*, European Commission. https ://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organizations/obligations/what-does-data-protection-design-and-default-mean_en

[3054] *Article 25 and Recital 78 of the GDPR*

[3055] *Loi n° 217 du 22 mai 2003 (*republiée*) pour la prévention et la lutte contre la violence domestique*. https ://legislatie.just.ro/Public/DetaliiDocument/44014

[3056] *Ordonnance d'urgence no 60 du 6 septembre 2006 modifiant et complétant le Code de procédure pénale, ainsi que d'autres lois.* https ://legislatie.just.ro/Public/DetaliiDocumentAfis/74920

[3057] *Loi no 135 du 1er juillet 2010 portant Code de procédure pénale, article 221*. https ://legislatie.just.ro/Public/DetaliiDocumentAfis/120609

[3058] LOI no 254 du 19 juillet 2013 relative à l'exécution des peines et mesures privatives de liberté ordonnées par les organes judiciaires au cours du procès pénal https ://legislatie.just.ro/Public/DetaliiDocument/150699

[3059] Parlement roumain, 2021, exposé des motifs de la loi sur la surveillance électronique dans les procédures judiciaires et pénales exceptionnelles, ainsi que pour modifier et compléter certains actes normatifs https ://www.cdep.ro/proiecte/2020/100/20/9/em180.pdf

pour lesquelles en Roumanie, bien que la législation la réglemente depuis un certain temps, ce n'est qu'au début de 2024 que la méthode est devenue viable et étendue à l'échelle nationale.

B. Utilisation des bracelets électroniques en France

L'utilisation de bracelets électroniques comme alternative à la détention traditionnelle est née de la nécessité de moderniser le service pénitentiaire, suggérée pour la première fois en 1989 par Gilbert Bonnaison[3060]. La suggestion réapparaît en 1995, lorsque le sénateur Pierre-Guy Cabanel, inspiré des pratiques étrangères[3061], propose le recours à cette technique de détention.

1062. Surveillance statique et mobile. La surveillance électronique a été testée pour la première fois en 90 avant sa généralisation progressive. Actuellement, 1 500 personnes ont un bracelet électronique « fixe ». Cela permet la surveillance statique (à la maison - bracelet électronique fixe) et la surveillance mobile (bracelet électronique mobile). Les deux types de surveillance peuvent être utilisés à n'importe quel stade du procès pénal (à la fois dans la phase des poursuites et dans la phase du procès). Cela leur permet également d'éviter la prison[3062]. Le bracelet fixe permet de vérifier qu'ils ne quittent la maison qu'aux heures autorisées par le juge (par exemple, pour aller travailler). Le bracelet électronique mobile est un nouveau dispositif destiné aux prisonniers jugés dangereux, condamnés à plus de 7 ans de prison Les prisonniers peuvent se déplacer sous surveillance. Ce dispositif vise à les aider à se réintégrer tout en contrôlant leurs mouvements pour éviter la récidive[3063]. S'il est mis en œuvre dans la phase de poursuite, le niveau de surveillance doit être proportionnel à la gravité des infractions, ne doit pas être intrusif et doit respecter la vie privée de la personne. En outre, elle doit être complétée par des mesures d'intégration socio-économique[3064].

a). Historique de la réglementation juridique de 2000 à 2024

[3060] G. Bonnaison, *La modernisation du service public pénitentiaire*, rapp. au Premier Ministre et au garde des Sceaux, Min. Justice, 1989.
[3061] P.G. Cabanel, *Pour une meilleure prévention de la récidive*, rapp. au Premier ministre, Doc. fr., *« Rapports officiels* », 1996.
[3062] A. Kensey, et al., « *Le développement de la surveillance électronique en France et ses effets sur la récidive* », Criminologie, vol.43, no.2, 2010. p.153-178. https ://doi.org/10.7202/1001773ar
[3063] G. Fenech, *Le placement sous surveillance électronique*, *Rapport de la mission confiée par le Premier Ministre à Monsieur Georges Fenech, député du Rhône*, Ministère de la Justice, 2005. http ://www.antoniocasella.eu/nume/Fenech_PSEM_2005.pdf
[3064] M. Herzog-Evans, *Droit de l'exécution des peines*, Paris : Dalloz, 2023/2024. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=DAEXPEINES

1063. Principales règles relatives à l'assignation à résidence. En examinant l'évolution législative, nous constatons que le règlement sur le placement à domicile sous surveillance électronique a subi de nombreuses modifications.

Le 15 juin 2000, la loi sur[3065] la présomption d'innocence est adoptée et, conformément à l'article 144-2 du Code de procédure pénale, la détention provisoire peut être obtenue par le biais d'un contrôle électronique à domicile.

En 2002, la loi n° 2002-1138 a instauré la surveillance électronique à domicile sous le contrôle judiciaire[3066].

En 2004, la loi n° 2004-204 accroît les possibilités de recours à la mesure de surveillance électronique[3067]. Conformément au Code de procédure pénale[3068], l'autorité judiciaire peut décider :

- Dans le cadre du suivi socio-judiciaire, à titre de mesure de sécurité, des adultes condamnés à une peine privative de liberté d'une durée de sept ans ou plus,
- Dans le cadre de la libération conditionnelle, pour les personnes reconnues coupables d'un crime ou d'un délit pour lequel la mesure de contrôle socio-judiciaire a été prise,
- En matière de contrôle judiciaire, pour les personnes condamnées à une peine privative de liberté d'une durée égale ou supérieure à 10 ans pour lesquelles un contrôle socio-judiciaire est effectué.

En 2009, la loi no 2009-1436[3069], également appelée loi pénitentiaire, a été adoptée, qui a favorisé l'adoption de mesures visant à adapter la peine, réglementant l'assignation à résidence sous contrôle électronique. Depuis 2010 (conformément à la loi no 2010-242[3070]), cette forme d'arrestation peut être appliquée aux mineurs, la surveillance électronique devenant ainsi une mesure éducative. La loi a suscité des discussions, d'une part l'initiative de modernisation et de gestion de la surpopulation carcérale a été appréciée, mais d'autre part, l'application inégale et

---

[3065] *Loi n° 2000-516 du 15 juin 2000 renforçant la protection de la présomption d'innocence et les droits des victimes*
https ://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000765204

[3066] *Loi n° 2002-1138 du 9 septembre 2002 d'orientation et de programmation pour la justice* . https ://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000775140

[3067] *Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité*. https ://www.legifrance.gouv.fr/jorf/id/JORFSCTA000000894222

[3068] *Code de procédure pénale, Section 6 : Du placement sous surveillance électronique (Articles 723-7 à 723-13-1)*.https ://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000006167536/#LEGISCTA000006167536

[3069] *Loi n° 2009-1436 du 24 novembre 2009 pénitentiaire.* https ://www.legifrance.gouv.fr/loda/id/JORFTEXT000021312171/

[3070] *Loi n° 2010-242 du 10 mars 2010 tendant à amoindrir le risque de récidive criminelle et portant diverses dispositions de procédure pénale* . https ://www.legifrance.gouv.fr/jorf/id/JORFTEXT000021954436

les inégalités qui en résultent ont été critiquées[3071]. Il convient de mentionner qu'à l'époque, le placement sous contrôle électronique n'était effectué qu'avec le consentement de la personne concernée, et ce en présence d'un avocat[3072].

Le 15 août 2014, la loi n° 2014-896[3073], qui abroge les dispositions de la loi de 2009, est approuvée. Sollicité par les recommandations de l'ONU[3074], ainsi que par leur mise en œuvre dans d'autres états, le législateur continue de concentrer son attention sur les mesures visant à ajuster la peine. Ainsi, il établit la procédure de « libération sous contrainte », une procédure de libération forcée sous contrôle électronique.

Afin de moderniser et de réformer le système judiciaire français, la loi n° 2018-2022-222 relative à la programmation et à la réforme du système judiciaire pour la période 2 est approuvée[3075]. Elle réglemente spécifiquement la détention à domicile sous contrôle électronique pour les peines de courte durée ou dans la phase finale des peines plus longues, dans le but d'une réinsertion progressive.[3076]

b). Tensions entre le droit européen et le droit français au sujet des bracelets électroniques

1064. Les préoccupations éthiques du Conseil de l'Europe. Au niveau européen, le Conseil de l'Europe publie les recommandations cm/Rec (2014)4[3077], qui établissent des lignes directrices pour l'utilisation de la surveillance électronique par les États membres L'Europe met l'accent sur les principes éthiques, le respect des droits fondamentaux, la vie privée, la dignité humaine et la prévention de la stigmatisation ou de la discrimination.

Les incompatibilités entre la réglementation européenne et le droit français concernent principalement les libertés individuelles et la sécurité du porteur du bracelet électronique. Par

---

[3071] M. Herzog-Evans, *Application des peines : la prétendue « bonne partie » de la loi pénitentiaire*, AJ pénal, 2009. p.483 https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=AJPEN/CHRON/2009/0100

[3072] *Code de procédure pénale Art. 723-7*. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CPRP029030

[3073] *Loi n° 2014-896 du 15 août 2014 relative à l'individualisation des peines et renforçant l'efficacité des sanctions pénales*. https ://www.legifrance.gouv.fr/jorf/id/JORFTEXT000029362502/

[3074] UNODC, *Manuel d'introduction pour la prévention de la récidive et la réinsertion sociale des délinquants*, Série de manuels sur la justice pénale, 2012. https ://css.unodc.org/documents/justice-and-prison-reform/UNODC_SocialReintegration_FRE_LR_final_online_version.pdf

[3075] *Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice* https ://www.legifrance.gouv.fr/jorf/id/JORFARTI000038261740

[3076] *Décret n° 2020-81 du 3 février 2020 relatif à la peine de détention à domicile sous surveillance électronique, au assis probatoire, aux conversions de peines et au mandat de dépôt à effet différé,* pris en application de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.

[3077] *Recommendation CM/Rec(2014)4 of the Committees of Ministers to member States on electronic monitoring,* Committee of Ministers, 2014. http ://www.europeanrights.eu/public/atti/2014_-_4__ing.pdf

exemple, le droit français ne tient pas compte du droit de la famille, bien que le consentement de la personne concernée soit nécessaire, il est plus formel[3078]. De plus, rien n'est stipulé concernant l'âge, le sexe ou les handicaps éventuels que le porteur d'un bracelet électronique peut présenter[3079].

1065. Période d'utilisation des bracelets électroniques. La durée d'application des bracelets électroniques mobiles est de deux ans, selon la loi « pénitencier » du 24 novembre 2019[3080]. En outre, aux articles 730-2 et 730-2-1 du Code de procédure pénale, la durée maximale d'utilisation peut atteindre 3 ans.

Une étude suédoise a montré que les meilleurs résultats sont obtenus lorsque la durée de la surveillance électronique est comprise entre 2 et 3 mois[3081]. En France, il a été observé que les longues périodes de détention à domicile ont des effets négatifs, augmentant le risque de rechute ou de violation des obligations pendant la détention[3082] [3083].

Actuellement, en ce qui concerne l'assignation à résidence sous contrôle électronique, si elle est effectuée pendant l'enquête, elle ne peut dépasser la durée de l'enquête elle-même. L'article 142-7 du Code de procédure pénale[3084] dispose que cette mesure ne peut être ordonnée pour une durée supérieure à six mois, avec possibilité de prolongation jusqu'à un maximum de deux ans (conformément à l'article 142-6[3085]). Si elle est exécutée dans le cadre de la peine, la durée ne peut excéder un an.

1066. Les avantages de la surveillance électronique. La mise sous surveillance électronique mobile permet :

- Déterminer le lieu où se trouvent les personnes concernées et recueillir des informations sur leurs déplacements ;
- Vérifier si les obligations et interdictions auxquelles ils sont soumis pendant le voyage sont respectées et si leur non-respect est immédiatement détecté ;
- Prévention des rechutes ;

[3078] M. Herzog-Evans, *Droit de l'exécution des peines, Chapitre 443 - Placement restreint en milieu libre : bracelet électronique*, Dalloz, 2023/2024. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=DZ/ACTION/EXECUTION-PEINES/2022/NIVO/L04-T44-C443

[3079] A. Hucklesby, „*Vehicles of desistance? The impact of electronically monitored curfew orders",* Criminology and Criminal Justice, vol.51, no 8(1), 2008.

[3080] *L'assignation à résidence sous surveillance électronique (ARSE)* est prévue par le *Code de procédure pénale*, art. 137, 142-5 s., 394 s., et a fait l'objet d'une décision importante : Cass. crim., *3 octobre 2012, n° 12-84.863.* https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=DZ/OASIS/001857

[3081] CNCDH, *Alternatives à la détention : du contrôle judiciaire à la libération conditionnelle*, Doc. fr., 2007. (audition de M. Norman Bishop, 4 avr. 2006)

[3082] V.P. Gendreau(dir.), *Choosing Correctional Options that Work*, Sage Publications, 1996.

[3083] J. Bonta, D.A. Andrews, *The Psychology of Criminal Conduct*, 6e éd., Routledge, 2017.

[3084] *Code de procédure pénale, Sous-section 2 : De l'assignnation à résidence avec surveillance électronique (articles 142-5 à à 142-13).*

[3085] *Ibidem*.

- Promouvoir la réinsertion en soutenant et en surveillant le respect des obligations imposées par le service d'intégration et de probation pénitentiaire ;
- C'est un outil complémentaire utile pour une bonne investigation.

c). Moindres coûts pour la surveillance à l'aide du bracelet électronique

A noter qu'en France, le coût d'un bracelet électronique est d'environ 30 euros/jour, contre 60 euros/jour d'emprisonnement[3086]. Une étude réalisée en France en 2016 a révélé que l'utilisation de la surveillance électronique réduit le taux de rechute, facilitant ainsi l'accès au travail et la réinsertion sociale[3087].

1067. Avantages et inconvénients de la surveillance à domicile. Cependant, la raison principale pour laquelle la France a utilisé ce temps de surveillance, en plus d'éviter les effets de désocialisation de l'emprisonnement, était la surpopulation carcérale[3088]. La surveillance électronique des délits légers a été introduite en 1997-2000. Bien que la surpopulation carcérale ait diminué au départ, depuis 2001, la surpopulation carcérale s'est accélérée, les raisons étant à la fois politiques[3089] et dues à des dispositifs de surveillance rudimentaires et peu fidèles, ce qui a entraîné de nombreux problèmes éthiques et de violation de la vie privée. Cela se produit également dans d'autres pays, avec une étude britannique montrant que le taux de rechute tous les deux ans chez les personnes sous surveillance électronique à domicile était de 73%[3090].

Entre octobre 2000 et mai 2002, une analyse du cadre juridique, des étapes de mise en œuvre et de l'impact ultérieur de la mise en œuvre de la surveillance électronique est réalisée en France. La conclusion du rapport est d'étendre l'utilisation de ce mode de surveillance, mais avec l'approbation de réformes continues pour plus d'efficacité[3091] .

[3086] J. Belur, Thornton, A., Tompson, L., Manning, M., Sidebottom, A., Bowers, K. (2020), *A systematic review of the effectiveness of the electronic monitoring of offenders,* Journal of Criminal Justice, 2020. https ://doi.org/10.1016/j.jcrimjus.2020.101686.

[3087] A. Henneguelle, B. Monnery, A. Kensey, *Better at Home than in Prison? The Effects of Electronic Monitoring on Recidivism in France.* The Journal of Law and Economics, vol.59, 2016. p.629-667. https ://doi.org/10.1086/690005.

[3088] R. Lévy, A. Pitoun, *Electronic Monitoring in France and Lessons Learned (2001-2004)*, Déviance et Société, vol.28(4), 2004, p.411-437. https ://shs.cairn.info/journal-deviance-et-societe-2004-4-page-411?lang=en.

[3089] R. Lévy, *Pardons and Amnesties as Policy Instruments in Contemporary France*, In M. Tonry (Ed.), *Crime, Punishment, and Politics in Comparative Perspective (551-590),* Chicago University Press, 2007.

[3090] D. Sugg, L. Moore, P. Howard, « *Electronic Monitoring and Offending Behavior — reconviction results for the second year of Trials of curfew Orders »,* Home Office Online Report, vol.59/04, 2001.

[3091] A. Kensey, A. Pitoun, R. Lévy, P.V. Tournier, *Sous surveillance électronique. La mise en place du « bracelet électronique » en France (octobre 2000-mai 2002),* Ministère de la Justice, Direction de l'administration pénitentiaire, 2003.

d). De l'expérience à l'usage généralisé

1068. Expérimentation. En France, il y a eu une étape d'expérimentation avant de généraliser ce processus. Depuis juillet 2006, la mise sous surveillance électronique mobile a fait l'objet, avant sa généralisation sur l'ensemble du territoire national, d'une expérimentation selon les étapes suivantes.

- Une première phase sur une période de 6 mois débutant en juillet dans deux sites pilotes : Les services pénitentiaires régionaux de Lille et de Rennes. Le placement de bracelets mobiles n'a été appliqué que dans le contexte d'une libération conditionnelle ;
- Une deuxième phase d'une durée de 18 mois (de décembre 2006 à mai 2008) dans quatre lieux pilotes : les directions régionales des services pénitentiaires de Lille, Rennes, Paris et Marseille. Le bracelet mobile sera ensuite appliqué dans le cadre de la libération conditionnelle, du contrôle judiciaire et du suivi socio-judiciaire
- La troisième étape de généralisation de l'application de la mesure des bracelets électroniques à partir de mai 2008.

1069. Localisation GPS permanente. La personne en question porte un bracelet, généralement attaché à la cheville, et une boîte à la ceinture la taille d'un téléphone mobile, qui est un émetteur mobile. Grâce à un système de surveillance par satellite (GPS), l'administration pénitentiaire peut localiser la personne à tout moment et ainsi surveiller ses déplacements. Lorsque la personne s'approche d'une zone qui lui est interdite (la maison de la victime, l'école, etc.), elle reçoit immédiatement un SMS sur son appareil pour l'alerter. Un autre récepteur est installé au domicile de la personne condamnée et récupère les données du boîtier mobile. Le récepteur fixe permet de vérifier que la personne est chez elle aux heures fixées par le juge[3092].

1070. Le logiciel de surveillance électronique mobile permet de programmer :

- Zones d'inclusion et zones d'exclusion : lieux autorisés vs lieux interdits
- Zones tampons autour de chaque lieu interdit permettant au personnel de surveillance d'alerter la personne localisée et de lui donner les instructions nécessaires
- Heures d'accès à un emplacement spécifique.

[3092] *Detention à domicile sous surveillance électronique (DDSE),* Citoyens & Justice. https ://www.citoyens-justice.fr/post-sententiel/amenagements-de-la-peine-demprisonnement/detention-a-domicile-sous-surveillance-electronique.html

1071. Surveillance à domicile, également disponible pour les personnes détenues. Depuis juillet 2006, les personnes détenues dans des unités relevant de la compétence de certaines cours d'appel (Caen et Douai) peuvent bénéficier, si elles remplissent et respectent les conditions, d'une libération conditionnelle accompagnée d'une surveillance électronique mobile. Ils ont contacté l'assistante sociale du service de probation et d'intégration pénitentiaire pour la préparation du dossier. La demande a ensuite été transmise à la juridiction chargée de l'exécution des peines. Un avocat, élu ou nommé par le tribunal, peut assister le condamné dans sa procédure. Le travailleur social effectue ensuite une étude de faisabilité pour déterminer si le placement est possible (famille, professionnel, situation familiale, consentement des personnes partageant le logement, suivi de la personne par un thérapeute, etc.). Parallèlement, un psychiatre devait examiner la personne pour évaluer le niveau de danger et les risques de rechute, cette expertise étant obligatoire. Le dossier complet est ensuite transmis à la juridiction responsable de l'exécution des sanctions. S'il accepte d'accorder une libération conditionnelle accompagnée du port d'un bracelet électronique, les obligations à respecter (programmes, lieux interdits, travail, etc.) seront définies en fonction de la situation de la personne.

e). Détention à domicile sous surveillance électronique

1072. Détention à domicile sous surveillance électronique peut être imposée dans les situations suivantes :

- Détention à domicile sous surveillance électronique comme peine de substitution à la détention traditionnelle
- Détention à domicile sous surveillance électronique en tant qu'adaptation à une peine de privation de liberté
- Détention à domicile sous surveillance électronique en tant que mesure de détention provisoire[3093]. Cette possibilité est renforcée par l'article 142-5 du Code de procédure pénale, qui permet au juge d'accorder cette mesure d'office, et le refus du suspect peut conduire à une mesure d'arrestation provisoire[3094].

Le recours à la détention à domicile sous contrôle électronique comme méthode de modification de la peine peut être décidé soit par le tribunal au moment de la condamnation (et

[3093] *Code de procédure pénale, Sous-section 2 : De l'assignnation à résidence avec surveillance électronique (articles 142-5 à à 142-13)*

[3094] V. D. Miranda, *Détention provisoire et surpopulation carcérale*, AJ pénal, 2018. p.341 https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=RSC/CHRON/2019/0407. Le nombre d'assignation à résidence sous surveillance électronique est assez faible en raison de la concurrence de la mesure de contrôle judiciaire

ici il s'agit d'un ajustement ab initio de la peine), soit par un juge de condamnation au moment de la condamnation.

1073. Réglementation de l'assignation à résidence. Actuellement, le placement sous contrôle électronique est régi par le Code pénal, par l'article 131-4-1 et par le Code de procédure pénale, par l'article 723-7[3095]. Conformément à l'article 131-4-1 du Code pénal, tel que modifié par la loi sur la réforme de la justice, lorsqu'une infraction pénale est passible d'une peine d'emprisonnement, le tribunal peut appliquer une peine de détention à domicile sous contrôle électronique pour une période de quinze jours à six mois, ne pas dépasser la durée de la peine d'emprisonnement[3096]. L'article R57-10 du Code de procédure pénale dispose que cette mesure est appliquée selon des procédures et conditions strictes prévues par la loi[3097].

La détention à domicile sous surveillance électronique peut également viser des personnes incarcérées, la loi autorisant, sous certaines conditions, la transformation d'une peine de prison en cours d'exécution en une peine de détention à domicile sous surveillance électronique.

Les interdictions et obligations ainsi que les prestations destinées à favoriser la réinsertion, dont bénéficie la personne surveillée à domicile, sont énoncées dans les articles 132-44 et 132-45 du Code pénal [3098].

f). Utilisation de la SE, une punition évolutive qui protège le droit à la vie privée

1074. S'inscrivant dans le concept de châtiment évolutif, le principal avantage de ce type de détention est d'éviter les effets négatifs de l'emprisonnement sur l'individu[3099]. Par ailleurs, dans le rapport de 2005 du Ministère de la Justice, il est souligné que cette mesure est moins intrusive, protégeant dans une certaine mesure le droit à la vie privée, facilitant la réinsertion sociale, tout en évitant la surpopulation carcérale[3100]. Ce dernier est une préoccupation actuelle, puisque la capacité des prisons en France est légèrement supérieure à 59.000 et que le nombre de détenus

---

[3095] *Code de procédure pénale, section 6 : du placement sous surveillance électronique (articles 723-7 à 723-13-1)*

[3096] *Code pénal, Sous-section 2 : Des peines correctionnelles (articles 131-3 à 131-9), article 131-4-1*

[3097] *Code de procédure pénale, Titre III : du placement sous surveillance électronique (articles R57-10 à R57-30-1)*

[3098] *Code pénal, Paragraphe 2 : Du régime de la probation (articles 132-43 à 132-46*)
https ://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006117596/#LEGISCTA000006117596

[3099] V. Peltier, *Le placement sous surveillance électronique et l'environnement du condamné », colloque Environnement et peine privative de liberté*, l'Institut de Sciences criminelles et de la Justice de Bordeaux, Cujas, n°2, 2013, p.176.

[3100] G. Fenech, *Le placement sous surveillance électronique mobile*, Ministère de la justice, 2005.
https ://www.vie-publique.fr/rapport/27394-le-placement-sous-surveillance-electronique-mobile

dépasse fréquemment les 70.000[31013102]. Cela peut entraîner des conséquences néfastes pour la France, et elle peut être accusée de violations de l'article 3 de la CEDH, qui interdit les traitements dégradants ou inhumains[3103]. Par exemple, dans l'affaire Canali c. France, la CEDH a jugé que la France ne respectait pas les droits fondamentaux du détenu[3104], étant privée de sa vie privée et de conditions d'hygiène adéquates. Les cas de ce type sont multiples, en 2018, la CEDH concluant, à la suite de l'analyse d'une vingtaine de cas, que la Roumanie, à travers les conditions de détention nationales, viole l'article 3 de la CEDH[3105].

1075. Mise en œuvre de l'assignation à résidence en France. En France, la détention à domicile sous contrôle électronique est l'une des peines les plus fréquentes décidées par les tribunaux. Le 1er mai 2004, le placement sous contrôle électronique était mis en œuvre dans 112 tribunaux de haute Cour (sur un total de 181) avec un total de 2312 mesures prononcées. De ce nombre, 126 (5,4 %) étaient des échecs dus soit à la non-conformité, soit à de nouveaux délits (comportement inapproprié, évasions)[3106]. En 2014, la loi no. 2014-896 a été adoptée[3107] qui, attirant l'attention sur la surpopulation des établissements pénitentiaires, réglemente l'octroi de mesures visant à modifier la peine, y compris la détention à domicile sous surveillance électronique[3108].

1076. Les avantages de l'assignation à résidence. Une adaptation de la peine de détention à domicile sous contrôle électronique peut être décidée pour permettre à la personne en particulier :

- Exercice d'une activité professionnelle
- Pour suivre un stage ou une formation
- Pour chercher un emploi
- Afin de participer aux dépenses et à la vie familiale
- Pour traitement médical ou soins spéciaux

[3101] *Rapport d'activité 2012 du Contrôleur général des lieux de privation de liberté*, Dalloz, 2013

[3102] A. Jego, *Les conséquences de la surpopulation en détention*, AJ pénal, 2018. p.344 https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=AJPEN/CHRON/2018/0235

[3103] Cour européenne des droits de l'homme, 4e section, *22 octobre 2009, n° 17599/05,* Jurisprudence Dalloz, 2009. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CEDH_LIEUVIDE_2009-10-22_1759905

[3104] CEDH, *Canali c. France, req. n°40119/09, 25 avril 2013*. https ://www.revuegeneraledudroit.eu/blog/decisions/cedh-25-avril-2013-canali-contre-france-req-n40119-09/

[3105] Cour européenne des droits de l'homme, *3 mai 2018 / n° 67449/14,* Dalloz, 2018. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CEDH_LIEUVIDE_2018-05-03_6744914

[3106] René Lévy, A. Pitoun, « *L'expérementation du placement sous surveillance électronique en France et ses renseignements (2001-2004)* », Déviance et Société, no.4, vol. 28, 2004. p.411-437.

[3107] *Loi n° 2014-896 du 15 août 2014 relative à l'individualisation des peines et visant l'efficacité des sanctions pénales.* https ://www.legifrance.gouv.fr/loda/id/JORFTEXT000029362502

[3108] M. Giacopelli, *La loi du 15 août 2014 relative à l'individualisation des peines et visant l'efficacité des sanctions pénales : un rendez-vous manqué*, AJ pénal, 2014. p.448 https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=AJPEN/CHRON/2014/0246

- Afin d'entreprendre tout projet qui favoriserait leur intégration.

1077. Statistiques du Ministère de la Justice en France. Si nous regardons les statistiques du ministère de la Justice, nous constatons que 12,3% des détenus purgent des peines allant jusqu'à 6 mois et 17,3% ont des peines allant de 6 mois à 1 an[3109]. La surveillance électronique peut remplacer entièrement des peines allant jusqu'à 6 mois de prison. En résumé, le placement sous surveillance électronique à la maison peut être prononcé dans :

- Adaptation de la peine (art. 723-7 du Code de procédure pénale)[3110]
- Ab initio, conformément à l'article 132-26-1 du Code pénal
- En contrôle judiciaire (art. 138 du Code de procédure pénale)
- Aveu préalable de culpabilité. (Article 495-8 du Code pénal).

g). Moyens de surveillance à l'aide du bracelet électronique

1078. Supervision après l'exécution de la peine. Elle a été introduite en tant que mesure de sécurité en 2005, puis modifiée par la loi no. 2011-1862 du 13 décembre 2011 et est régie par l'article 763-10 du Code de procédure pénale. Il cible les criminels dangereux à haut risque de rechute et aussi ceux qui seront interdits pendant une période après la condamnation de se rendre dans certains lieux. La mesure est controversée et considérée comme très intrusive dans les droits fondamentaux de la personne, en particulier la vie privée[3111].

1079. Supervision administrative. Cela est dû au besoin de sécurité généré par les récents attentats terroristes en France. Ainsi, la loi n°[3112] 30-2017 sur la sécurité nationale et la lutte contre le terrorisme prévoit également des dispositifs de surveillance électronique. Il peut être utilisé pour surveiller les personnes soupçonnées de terrorisme, même après l'exécution de la peine pénale, afin d'assurer la sécurité publique[3113].

Ainsi, conformément à l'article L.855-1 du Code de la sécurité nationale, les agents pénitentiaires peuvent recourir à des mesures telles que la surveillance électronique pour recueillir des informations sur les suspects[3114].

[3109] *Le plan pénitentiaire*, Ministère de la Justice, 2018. http ://www.justice.gouv.fr/art_pix/dp_plan_penitentiaire_20180912.pdf, page 3

[3110] *Code de procédure pénale, Section 6 : Du placement sous surveillance électronique (articles 723-7 à 723-13-1)*

[3111] P. Beauvais, *La nouvelle surveillance pénale*, 1er éd., coll. Droit & Justice, PUF, 2022. p. 264.

[3112] *Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme* https ://www.legifrance.gouv.fr/jorf/id/JORFTEXT000035932811/

[3113] H. Mastopoulou, *La transposition dans le droit des principales mesures de l'état d'urgence - à propos de la loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme*, JCP, 2017. Doctr. 1268.

[3114] *Code de la sécurité intérieure, Titre V bis: du renseignement de sécurité pénitentiaire, article L855-1)*

Dans ce contexte, cependant, la Cour européenne des droits de l'homme (CEDH) déclare que ces mesures restrictives sur la vie privée ne peuvent être prises uniquement sur la base de soupçons. Par exemple, dans l'affaire S., V., A. c. Danemark, la Cour européenne des droits de l'homme examine si, par des mesures restrictives à l'encontre des trois citoyens danois soupçonnés de terrorisme, il n'y a pas eu violation des dispositions de l'article 5 de la Convention[3115]. En l'espèce, la CEDH a conclu qu'un simple soupçon ne suffit pas pour recourir à des mesures privatives de liberté, qui exigent des preuves concrètes et justifiées.

h). Le caractère obligatoire du consentement a été exclu

1080. Consentement, même formel, afin de réduire la perception d'intrusion dans la vie privée. Dans un pays où l'on met l'accent sur la vie privée, la discussion sur l'installation d'un dispositif de surveillance domestique suscite la controverse, rappelant le principe du « grand frère » dans le livre de George Orwell[3116]. Le bracelet électronique peut être perçu comme une restriction de la vie personnelle, d'autant plus que la surveillance se déroule dans l'espace privé de l'individu. Cependant, il est préférable, devant la prison, car il permet à la personne de rester dans la communauté En outre, la nécessité de consentement (même formel) de la personne concernée diminue[3117] la perception de violation de la vie privée.

Cependant, depuis 2019 (loi n° -22 du 23 mars 2019)[3118] la France renonce à l'obligation de consentement, abrogeant l'article 132-26-1 du Code pénal (remplacé par l'article 131-4-1) et avec elle la faible défense de la liberté individuelle et de la protection de la vie privée[3119].

Conclusions Chapitre 2 - sur l'utilisation de la surveillance électronique

1081. Les systèmes de surveillance électronique sont un outil de surveillance accrue des criminels dans le cadre d'un régime de surveillance de la justice pénale. Cette technologie peut

---

[3115] Cour européenne des droits de l'homme, grande chambre *22 octobre 2018 N° 35553/12 36678/12 36711/12 Affaire S., V., A. c. Danemark*, Dalloz Jurisprdence, 2018. https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CEDH_LIEUVIDE_2018-10-22_3671112

[3116] B. Harcourt*, 1. Le Big Brother de George Orwell. La Société d'exposition Désir et désobéissance à l'ère numérique*, Le Seuil, 2020. p. 39-58 https ://shs-cairn-info.docelec.u-bordeaux.fr/la-societe-d-exposition-desir-et-desobeissance-a-l-ere-numerique--9782021372977-page-39?lang=fr.

[3117] M. Peretti*, Le bracelet électronique : « boulet moderne » ou outil d'insertion ?*, AJ pénal, 2007. p.468 https ://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=AJPEN/CHRON/2007/0091

[3118] *Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice.* https ://www.legifrance.gouv.fr/jorf/id/JORFARTI000038261740

[3119] *Décret n° 2020-81 du 3 février 2020 relatif à la peine de détention à domicile sous surveillance électronique, au assis probatoire, aux conversions de peines et au mandat de dépôt à effet différé*, pris en application de la loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice. https ://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041521121

être utilisée à différents stades du processus judiciaire : détention préventive, libération conditionnelle et régime de sanctions communautaires, en fonction de chaque système national.

La SE permet aux autorités de surveiller et de vérifier la localisation des personnes impliquées dans des procédures judiciaires, augmentant ainsi la probabilité que toute violation du régime de surveillance soit détectée et que des sanctions soient imposées.

SE devient attrayante parce qu'elle est moins chère que la détention, mais elle offre également une surveillance supplémentaire par rapport à la probation traditionnelle. En général, deux formes de SE sont prédominantes : la surveillance par radiofréquence (FR) et le système de positionnement global (GPS). FR surveillance mesure si un sujet actif de procédure judiciaire se trouve à une certaine distance de l'émetteur fixe, est utilisé presque exclusivement dans les peines et les régimes restrictifs de détention à domicile, et la surveillance GPS suit les mouvements des criminels en temps réel.

Ce chapitre montre que la surveillance électronique s'est imposée, au niveau européen, comme une véritable alternative à la détention, justifiée par des objectifs concrets : réduire la surpopulation carcérale, prévenir la récidive, protéger les victimes – en particulier en matière de violence domestique – et faciliter la réinsertion sociale. Les expériences des États analysés montrent toutefois que cette solution n'est pas neutre : elle transforme l'espace de vie en un lieu contrôlé en permanence, proche de l'idée de « prison électronique », et soulève des questions directes quant à la proportionnalité de l'ingérence par rapport à l'objectif poursuivi.

En droit roumain, la loi n° 146/2021 marque le passage de l'utilisation de la surveillance électronique exclusivement dans les cas de violence domestique à son intégration dans les procédures pénales, ce qui exige des conditions claires concernant la durée, l'objectif et le contrôle judiciaire de la mesure. En droit français, l'évolution de la réglementation, l'extension progressive du champ d'application, l'utilisation dans le cadre de l'assignation à résidence et l'exclusion du consentement comme condition préalable obligatoire révèlent un renforcement de la surveillance électronique en tant que forme autonome d'exécution de la peine. Dans le même temps, les tensions signalées par rapport aux exigences européennes en matière de dignité et de vie privée confirment la nécessité d'une justification individualisée de chaque mesure et de garanties effectives contre les abus.

Il en résulte que la surveillance électronique n'est acceptable que dans la mesure où elle reste une mesure strictement réglementée, proportionnée, soumise à un contrôle judiciaire effectif et assortie de critères transparents concernant la sélection des personnes concernées, les moyens techniques utilisés et les limites de la surveillance. En l'absence de ces conditions, cet instrument conçu comme une alternative à l'incarcération risque de devenir une forme extensive de contrôle de la vie privée, incompatible avec son statut de sanction moins intrusive

Chapitre 3
VIE PRIVÉE VERSUS MÉDECINE MODERNE

1082. L'influence de l'évolution technologique dans le domaine médical. La médecine de précision offre des perspectives prometteuses pour une meilleure santé, en tenant compte des caractéristiques génétiques, de l'individu, de l'environnement et du style de vie. Cette approche continuera à révolutionner les soins de santé au cours de la prochaine décennie, conduisant à des diagnostics affinés, à des traitements plus rationnels et à une prévention plus efficace, en s'étendant à des domaines clés tels que l'intelligence artificielle[3120], la génétique moléculaire et l'interrogation génétique phénotypique[3121]. Dans ce contexte, en 2011, le Conseil national de la recherche des États-Unis a appelé à une nouvelle taxonomie des maladies humaines basée sur la médecine de précision[3122]. Actuellement, l'analyse génétique est limitée au dépistage de maladies rares ou de certains cancers, mais à l'avenir, elle deviendra routinière[3123], avec le séquençage du génome entier des personnes analysé de manière routinière. L'ADN deviendra certainement un pilier du dépistage[3124].

Section 1. PROTECTION DES CARACTÉRISTIQUES GÉNÉTIQUES

Aujourd'hui, des questions telles que la procréation assistée, la gestation pour autrui, la recherche sur les cellules souches embryonnaires, les tests ADN, le séquençage de l'ADN, la copie de l'ADN, l'isolement du génome personnel, l'euthanasie, sont d'actualité et font l'objet de débats intenses, impliquant deux sphères d'intérêt majeures : d'une part, la médecine et, d'autre part, la sphère juridique, en ce qui concerne la protection de la vie privée et la protection des « libertés de vivre ».[3125] Dans le contexte médical, les tests génétiques sont utilisés pour détecter les prédispositions aux maladies héréditaires en identifiant des mutations spécifiques, pour évaluer les risques génétiques en proposant ensuite des traitements personnalisés basés sur le profil génétique des patients, pour effectuer des tests prénataux afin de détecter des anomalies

[3120] L. Alexandre*, La mort des médecins.* Les Tribunes de la santé, no.54 2017/1, p.43-47. https://shs.cairn.info/revue-les-tribunes-de-la-sante1-2017-1-page-43?lang=fr.
[3121] F. Lemaitre, et all., *Comment entrer la médecine de précision dans la décision thérapeutique de routine au lit du malade ?* Therapies, vol 79, 2024, p.1-11.
[3122] National Research Council, *Toward Precision Medicine : Building a Knowledge Network for Biomedical Research and a New Taxonomy of Disease*. National Academies Press, 2011. [PubMed] [Google Scholar].
[3123] S. Ayme S. *La médecine prédictive vingt ans après*. Actualite Et Dossier En Sante Publique(100) : 13-16, 2017.
[3124] J.C. Denny, F.S. Collins, *Precision medicine in 2030 – seven ways to transform healthcare*. Cell., 2021.
[3125] P. Muzny, *La liberté de la personne sur son corps,* DALLOZ, 2010.

fœtales (syndrome de Down ou autres anomalies génétiques). Ces tests sont essentiels pour la mise en œuvre de la médecine personnalisée et pour améliorer les résultats cliniques[3126].

1083. L'intrusion de la génétique dans la vie privée. La génétique se distingue des autres spécialités médicales[3127] par son intrusion dans la vie privée de l'individu[3128]. Elle soulève également de nombreuses questions éthiques et juridiques, en particulier avec les développements technologiques continus et rapides de la cartographie du génome humain[3129].

L'examen des caractéristiques génétiques à des fins médicales et scientifiques est régi par un vaste cadre juridique national et international, qui vise à protéger les droits des personnes concernées, à garantir la confidentialité des données génétiques et à définir les modalités d'utilisation de ces informations[3130].

§1. LE CADRE JURIDIQUE DE LA PROTECTION DES CARACTÉRISTIQUES GÉNÉTIQUES

La France promeut une recherche responsable en génétique en veillant à ce que toutes les études soient menées conformément à des normes éthiques strictes et en respectant la confidentialité des données génétiques[3131]. Ce cadre juridique solide garantit que la recherche contribue au progrès scientifique sans compromettre les droits individuels.[3132]

Ces derniers temps, avec le développement de la médecine et de la technologie modernes, les domaines médicaux et scientifiques, si bénéfiques et en même temps si menaçants en termes de protection de la vie privée, ont fait l'objet d'une attention juridique accrue. Des préoccupations telles que la stigmatisation, l'exclusion ou l'inconvenance vis-à-vis de l'individu sont de plus en plus soulevées.[3133] C'est pourquoi, avec l'aide de la justice, on tente

---

[3126] F. Ewald. *Les Normes de Protection des Données Génétiques en France*. Revue de Droit Sanitaire et Social, vol. 60, no. 3, 2018.

[3127] T.H., Murray, "*Genetic Exceptionalism and 'Future Diaries' : Is Genetic Information Different from Other Medical Information?"* in M.A., Rothstein(ed), *Genetic Secrets : Protecting Privacy and Confidentiality in the Genetic Era,* Yale University Press, 1997. Google Scholar.

[3128] A. Claeys, J.S., Vialatte, *Les progrès de la génétique : vers une médecine de précision ? Les enjeux scientifiques, technologiques, sociaux et éthiques de la médecine personnalisée*, Office Parlementaire d'Evaluation des Choix Scientifiques et Technologiques, 2014. https://www.senat.fr/fileadmin/import/files/fileadmin/Fichiers/Images/opecst/quatre_pages/4_pages_medecine_perso_def.pdf.

[3129] D. Lacombe. *Génétique médicale et éthique*, Journal International de Bioéthique, vol.23, 2012/2. p.95-102. https://shs.cairn.info/revue-journal-international-de-bioethique-2012-2-page-95?lang=fr.

[3130] S. Bernatchez, *La Protection des Données Personnelles et la Recherche Scientifique en France*, Éditions Dalloz, 2019.

[3131] M. Perrine. *Les techniques de séquençage de nouvelle génération Questions éthiques en pratique clinique*. *Laennec,vol.64,* 2016/3. p.6-17. https://shs.cairn.info/revue-laennec-2016-3-page-6?lang=fr

[3132] J-P. Costa. *Les Droits de 'Homme et la Bioéthique*, Éditions La Découverte, 2019.

[3133] E. Abrahams, G.S Ginsburg, M. Silver, *The Personalized Medicine Coalition : goals and strategies*. Am J Pharmacogenomics, 2005.

de maintenir un équilibre entre les droits et les intérêts, apparemment avec des effets opposés sur l'individu.[3134]

Un bref aperçu du cadre législatif relatif à la confidentialité et à la protection des données génétiques comprend le règlement général sur la protection des données (GDPR) de l'Union Européenne, mis en œuvre en 2018, qui comporte des dispositions strictes sur la collecte, le stockage et le traitement des données génétiques[3135]. En vertu du GDPR, version 2.0[3136] (adopté en 2021), les données génétiques sont considérées comme des données sensibles et leur traitement nécessite le consentement explicite de la personne concernée. Cela inclut les examens génétiques à des fins médicales et de recherche scientifique, interdisant l'accès non autorisé ou l'utilisation abusive. Le GDPR est appliqué dans tous les pays de l'UE, y compris la France et la Roumanie[3137].

A. Loi de la bioéthique en France

1084. Réglementation des données génétiques dans la recherche. En France, la Loi de Bioéthique a été adoptée pour la première fois en 1994 et a ensuite fait l'objet de plusieurs révisions.[3138] Elle réglemente l'utilisation des données génétiques pour la recherche et le traitement médical, en prévoyant des droits clairs pour les patients et des responsabilités strictes pour les chercheurs et les médecins en ce qui concerne la protection de ces données.[3139] La dernière révision majeure a eu lieu en 2021 et a été adoptée, après de longs débats, le 2 août 2021 par un effort conjoint de l'Académie de Médecine, de l'Institut du Droit et de la Santé de l'Université Paris Cité et du Comité Éthique et Cancer.[3140] Pour gérer les questions éthiques,

---

[3134] E. Derieux, *Vie privée et données personnelles - Droit à la protection et « droit à l'oubli » face à la liberté d'expression*, Les Nouveaux Cahiers du Conseil constitutionnel*,* no.48*,* 2015/3, p.21-33 https://shs.cairn.info/revue-les-nouveaux-cahiers-du-conseil-constitutionnel-2015-3-page-21?lang=fr.

[3135] Le GDPR définit les données génétiques comme « les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne, résultant de l'analyse d'un échantillon biologique prélevé sur la personne concernée, notamment de l'analyse des chromosomes, de l'acide désoxyribonucléique (ADN) ou de l'acide ribonucléique (ARN), ou de l'analyse d'un autre élément fournissant des informations équivalentes ».

[3136] Guidelines *07/2020 on the concepts of controller and processor in the GDPR*, Version 2.0, 2021. https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2021/07/guidelines_2020-07.pdf

[3137] *Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (Règlement Général sur la Protection des Données - RGPD*), Publié au Journal Officiel de l'Union Européenne, L 119, le 4 mai 2016, ce règlement est également applicable en France et régit la protection des données génétiques. Disponible sur le site officiel d'EUR-Lex : www.eur-lex.europa.eu.

[3138] D. Turpin. *20 ans de lois de bioéthique, chapitre 1. Les lois françaises de bioéthique ont 20 ans !,* Journal international de bioéthique et d'éthique des sciences, vol.26, 2015. p.27-36. https://stm.cairn.info/revue-journal-international-de-bioethique-et-d-ethique-des-sciences- 2015-3?lang=fr

[3139] *LOI n° 2021-1017 du 2 août 2021 relative à la bioéthique* sur l'utilisation des données génétiques à des fins scientifiques et médicales. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043884384

[3140] C. Esper, *Introduction du colloque « Loi de bioéthique du 2 août 2021. Quel impact sur nos vies ?* Organisé par l'Institut Droit et Santé (INSERM UMR_S 1145) de l'Université Paris Cité, le Comité éthique et cancer, l'Académie nationale de médecine. Journal du Droit de la Santé et de l'Assurance - Maladie (JDSAM*), no.32,*

juridiques et sociales[3141] liées à l'utilisation des données génétiques dans la recherche, le don d'organes ou les techniques de reproduction, l'Agence de la Biomédecine a été créée en 2004, avec pour objectif principal de se conformer à la loi de bioéthique en vigueur.[3142] D'après l'Art. L. 1131-3 du Code de la Santé Publique**,** seuls les praticiens autorisés par l'Agence de la Biomédecine peuvent procéder à des examens des caractéristiques génétiques[3143].

Une telle attention à l'égard de cette réglementation est justifiée et nécessite une réévaluation et une mise à jour constantes pour suivre le rythme des nouvelles technologies qui sont si utiles dans le domaine de la santé et qui ont un si grand impact sur la société.[3144] Il suffit de citer la technologie **Crisp-Cas9[3145]**, capable de modifier l'ADN pour prévenir des pathologies telles que l'anémie filiforme et la thalassémie.[3146] En 2020, elle a valu le prix Nobel de chimie à la chercheuse française Emmanuelle Charpentier et à l'Américaine Jennifer Doudna, qui l'ont découverte.[3147]

a). Droit à l'oubli génétique

Un terme relativement nouveau, qui s'est imposé avec le développement des tests génétiques, est le « droit à l'oubli génétique »[3148]. Cette réglementation vise à empêcher que des individus soient discriminés sur la base de leur profil génétique, notamment dans le domaine des assurances ou par les employeurs. Ainsi, en vertu de cette loi, les personnes concernées ne sont pas obligées de divulguer les résultats de leurs tests génétiques aux assureurs vie ou santé ou aux employeurs (surtout s'ils indiquent un risque de développer des maladies graves)[3149].

2022/2. p.8-11 https://droit.cairn.info/revue-journal-du-droit-de-la-sante-et-de-l-assurance- maladie-2022-2-page-8?lang=fr.

[3141] I. de Lamberterie, *« Débat éthique et juridique relatif à l'accès aux données génétiques* », Éthique publique vol. 6, n° 2 | 2004. URL : http://journals.openedition.org/ethiquepublique/2027, https://doi.org/10.4000/ethiquepublique.2027.

[3142] A. Courrèges. *L'Agence de la biomédecine, un modèle original au service de la loi de bioéthique*, Dalloz, 2021 https://www.dalloz-actualite.fr/flash/l-agence-de-biomedecine-un-modele-original-au-service-de-loi-de-bio.

[3143] Code de la santé publique - Art. L. 1131-3, Journal Officiel https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CSPU000199.

[3144] H. Chneiweiss. *Modification du génome : quels enjeux éthiques ?,* Sciences Sorbonne Université, 2021. https://sciences.sorbonne-universite.fr/actualites/modification-du-genome-quels-enjeux- ethiques.

[3145] F. Ewald. *Les Technologies CRISPR et Leur Application dans les Maladies Génétiques*, Revue de Droit Sanitaire et Social, vol. 60, nr. 3, 2019.

[3146] Z., Meilin. *Jennifer Doudna and Emmanuelle Charpentier's Experiment About the CRISPR/cas 9 System's Role in Adaptive Bacterial Immunity (2012).* Embryo Project Encyclopedia, 2017. https://hdl.handle.net/10776/12998.

[3147] E. Charpentier, J.A. Doudnam *The Nobel Prize in Chemistry 2020 – Genetic scissors: a tool for rewriting the code of life,* Nobel Prize Outreach,2020. https://www.nobelprize.org/prizes/chemistry/2020/press-release/.

[3148] C. Crichton. *Le « droit à 'oubli » sur les moteurs de recherche : état des lieux.* 2019, Dalloz- etudiant https://actu.dalloz-etudiant.fr/a-la-une/article/droit-a-loubli-sur-les-moteurs-de-recherche-etat-des-lieux/h/917f05c286a69786043c0e31cdaaa2737.html.

[3149]B. M.-Bricout, T. Favario. *L'identité, un singulier au pluriel*, Dalloz, n°1, 2015. https://bibliotheque-lefebvre-dalloz-fr.docelec.u-bordeaux.fr/ouvrage/themes- commentaires/identite-singulier-pluriel_9782247160181.

1085. Réglementation du droit à l'oubli. La France est l'un des premiers pays à mettre en œuvre une loi sur le droit à l'oubli génétique[3150], adoptée en 2016 et incluse dans la loi de bioéthique[3151]. Dans sa forme initiale, la loi prévoyait que les patients chez qui un cancer avait été diagnostiqué avant l'âge de 21 ans pouvaient le dissimuler 5 ans après la fin du traitement. Si le néoplasme a été diagnostiqué après l'âge de 21 ans, le droit à l'oubli s'applique 10 ans après la fin du traitement.[3152] En 2022, la loi sur l'oubli a été révisée dans le but de la rendre plus claire, plus efficace et plus facile à appliquer. Ainsi, à partir du 17 février 2022, le droit à l'oubli a été fixé à 5 ans, en excluant le critère de l'âge.[3153]

Dans l'Union Européenne, les discussions sur cette question ont commencé en 1995, avec l'adoption de la directive 95/46/CE du Parlement Européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[3154]. En 2014, la Cour de Justice de l'Union Européenne (CJUE) a précisé que les informations obtenues lors de recherches en ligne constituent un traitement de données à caractère personnel et que le responsable du traitement est tenu de supprimer, dans certaines circonstances, ces informations, établissant ainsi le droit à l'oubli[3155]. En 2019, la CJUE valide la loi susmentionnée dans l'ensemble de l'Union Européenne, en l'incluant dans le Règlement Général sur la Protection des Données (RGPD) et abroge la directive initiale - 95/64/CE[3156].

Au niveau de l'UE, le droit à l'oubli n'est pas aussi bien défini qu'en France, le droit à l'oubli étant associé au droit à l'effacement des données et, comme indiqué ci-dessus, est régi par l'article 17 du Règlement Général sur la Protection des Données (RGPD), qui donne à la

---

[3150] RANQUET Marie. Le droit à l'oubli : vers un nouveau droit fondamental de l'individu ? *Communications,* 2019/1 No 104, p.149-159. DOI : 10.3917/commu.104.0149. URL : https://shs.cairn.info/revue-communications-2019-1-page-149?lang=fr.

[3151] *Les questions de bioéthique: chronologie 1983-2023*, Vie publique, 2023 https://www.vie-publique.fr/eclairage/19234-les-questions-de-bioethique-la-chronologie-de-1983-2023.

[3152] M. Moliner-Dubost. *Le Droit à l'Oubli Génétique*, Journal International de Bioéthique et d'Éthique des Sciences, vol. 31, n° 2, 2019.

[3153] *Réduction du délai de droit à l'oubli pour faciliter l'accès au crédit pour les anciens malades du cancer*, Ministère des Solidarités et de la Santé, Communique de Presse, Paris, 2022. https://sante.gouv.fr/archives/archives-presse/archives-communiques-de-presse/article/reduction-du-delai-de- droit-a-l-oubli-pour-faciliiter-l'-acces-au-credit-pour-les.

[3154] Directive 95/46/CE du Parlement Européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A31995L0046.

[3155] P. Hustinx , *EU Data Protection Law : The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, European University Institute's Academy of European Law, 2013. https://www.statewatch.org/media/documents/news/2014/sep/eu-2014-09-edps-data-protection-article.pdf

[3156] *Le droit à l'oubli sur internet*, EUR-Lex 2022. https://eur-lex.europa.eu/RO/legal-content/summary/right- to-be-forgotten-on-the-internet.html.

personne concernée le droit de demander l'effacement de ses données à caractère personnel, y compris de ses données génétiques[3157].

À l'instar de la France, le Parlement Européen a proposé en 2022 une résolution sur le droit à l'oubli des patients atteints de cancer, qui devrait entrer en vigueur au plus tard en 2025 : tous les États membres de l'UE doivent offrir aux citoyens la possibilité de faire effacer leurs informations néoplasiques dans un délai de 5 ou 10 ans après la fin du traitement, en fonction de l'âge de la personne concernée. Mais ce droit est assez difficile à mettre en œuvre, car il n'est pas directement stipulé dans la législation actuelle, les limites du GDPR à ce sujet étant présentée plus haut.[3158] Le droit à « être oublié » reste la solution ultime pour protéger la vie privée face aux développements numériques de plus en plus intrusifs, mais il est en conflit avec le besoin de la société de documenter correctement son histoire[3159].

b). Médecine personnalisée et tests génétiques

1086. L'influence des tests génétiques sur la vie privée. La médecine personnalisée[3160] et les tests génétiques utilisés pour guider les traitements sont légaux, mais nécessitent un consentement éclairé et la protection des données génétiques[3161]. Toute violation de ces règles peut entraîner une responsabilité pénale ou civile en vertu de la législation sur la protection des données. Les tests génétiques prénataux sont disponibles et légaux dans la plupart des pays européens, y compris en France[3162] et en Roumanie[3163] [3164], avec une attention accrue (en particulier en France[3165]) pour prévenir les abus (sélection génétique contraire à l'éthique). Les

---

[3157] Article 17 du GDPR. Droit à l'effacement des données (« droit à l'oubli »)/Article 17 GDPT. Right to erasure ("right to be forgotten") https://gdpr-text.com/ro/read/article-17.

[3158] European Parliament resolution of 16 February 2022 on strengthening Europe in the fight against cancer – towards a comprehensive and coordinated strategy 2020/2267(INI) https://www.europarl.europa.eu/doceo/document/TA-9-2022-0038_EN.html.

[3159] F. Pellegrini, A. Vitalis. *L'ère du fichage généralisé* , Le Monde diplomatique, 2018. p.3 https://www.monde-diplomatique.fr/2018/04/PELLEGRINI/58551.

[3160] Approche médicale dans laquelle l'attitude thérapeutique est basée sur les caractéristiques génétiques de chaque patient. Elle diffère de la médecine traditionnelle en ce sens qu'elle n'applique pas un traitement général, mais personnalise les interventions, maximisant ainsi l'efficacité et minimisant les risques ou les effets secondaires.

[3161] R. Picard, R. *Médecine personnalisée : de quoi parle-t-on? une vision prospective*. Annales des Mines - Réalités industrielles vembre 2014. (https://shs.cairn.info/revue-realites-industrielles1-2014-4-page- 99?lang=fr

[3162] Le Code civil - Chapitre III : De l'examen des caractéristiques génétiques d'une personne et de l'identification d'une personne par ses empreintes génétiques (Articles 16-10 à 16-13) https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070721/LEGISCTA000006136513/#LEGISCTA000006136513

[3163] *LOI no 95 du 14 avril 2006 (**republiée**) relative à la réforme du système de santé*. https://legislatie.just.ro/Public/DetaliiDocument/71139

[3164] *LOI no. 46 du 21 janvier 2003 droits des patients*. https://legislatie.just.ro/Public/DetaliiDocumentAfis/41483

[3165] Le Code Pénal - *Section 6 : Des atteintes à la personne résultant de l'examen de ses caractéristiques génétiques ou de l'identification par ses empreintes génétiques (Articles 226-25 à 226-30)* https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165397/#LEGISCTA000006165397

tests génétiques de prédisposition à certaines maladies doivent être effectués avec un consentement explicite et éclairé. Selon la Loi sur la Bioéthique[3166] et le GDPR, les patients doivent être informés de la finalité du test, de la durée de conservation des données et de la possibilité de demander la suppression des données à tout moment[3167] [3168]. La gestion des résultats des tests génétiques est une autre question éthique importante. Il est nécessaire de déterminer qui peut accéder à ces informations et dans quelles conditions. Dans certaines situations, les données génétiques peuvent avoir un impact sur la personne testée, ainsi que sur les membres de sa famille, ce qui soulève la question de leur information en cas de découverte de risques génétiques partagés[3169] [3170].

B. Discrimination génétique

1087. Données génétiques : risque de discrimination. Le terme de discrimination génétique est utilisé depuis le siècle dernier, les experts en la s'essayant à plusieurs définitions. Par exemple, Apse et al. la définissent comme une situation dans laquelle des décisions injustes sont prises à l'égard d'une personne en bonne santé sur la base de ses informations génétiques.[3171] Plus récemment, la discrimination génétique est définie par certains auteurs[3172] comme le refus de droits, de privilèges, d'opportunités ou d'un autre traitement en raison d'informations génétiques, y compris les antécédents familiaux ou les résultats de tests génétiques.

a). Discrimination génétique en France

[3166] V. Depadt-Sebag, L Chambaud. *La nouvelle loi de bioéthique en question(s) -Sur quels principes s'établit le droit relatif à la bioéthique?,* Presses de l'EHESP, 2021. P.27-39. https://shs.cairn.info/la-nouvelle-loi-de-bioethique-en-questions--9782810907922?lang=fr .

[3167] *Loi de bioéthique - LOI n° 2021-1017 du 2 août 2021 relative à la bioéthique*, sur l'utilisation des données génétiques à des fins scientifiques et médicales https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043884384

[3168] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (Règlement Général sur la Protection des Données - RGPD), Publié au Journal officiel de l'Union Européenne, L 119, le 4 mai 2016, ce règlement est également applicable en France et régit la protection des données génétiques. Disponible sur le site officiel EUR-Lex : www.eur-lex.europa.eu.

[3169] P.-H. du Chène. *La Bioéthique et le Droit en France*, Presses Universitaires de France, 2020.

[3170] François Ewald. *Les Normes de Protection des Données Génétiques en France*, Revue de Droit Sanitaire et Social, vol. 60, nr. 3, 2018.

[3171] L. Geller, J. Alper, P. Billings, Barash C, Beckwith J, Natowicz M. *Individual, family, and societal dimensions of genetic discrimination : a case study analysis*. Sci Eng Ethics. 1996, 2 : 71-88. 10.1007/BF0262639319.

[3172] C. Erwin, Williams JK, Juhl AR, Mengeling M, Mills JA, Bombard Y, Hayden MR, Quaid K, Shoulson I, Taylor S, Paulsen JS, *I-RESPOND-HD Investigators of the Huntington Study Group: Perception, experience, and response to genetic discrimination in Huntington disease*: *the international RESPOND-HD study*, Am J Med Genet B Neuropsychia Genet. 2010.

Le problème de la discrimination[3173] se pose dans le monde entier, surtout avec le développement de la technologie. Au 19e siècle, bien que caractérisé par un développement prodigieux, avec des découvertes et des innovations phénoménales dans divers domaines, l'abolition de l'esclavage et du servage,[3174] le plus célèbre écrivain anglais, Oscar Wilde, a été accusé d'homosexualité et condamné à 2 ans de prison dure. 5 ans plus tard, le génie irlandais meurt des suites de l'immense discrimination dont il a été victime[3175].

Dans le contexte du développement de la technologie, avec la possibilité de réaliser divers algorithmes, en France, le Médiateur ainsi que la CNIL (Commission nationale de l'informatique et des libertés) tentent de prévenir la discrimination en appelant à une prise de conscience collective et à l'adoption de mesures pour l'éviter.[3176]

1088. Tests génétiques disponibles: avantages, restrictions. Des études génétiques sont désormais possibles, qui permettent d'estimer avec précision la probabilité d'un grand nombre de maladies[3177] telles que les maladies oncologiques, mais aussi des affections comme la maladie Huntington, cardiomyopathie hypertrophique, hyperlipémie etc. De nombreuses études démontrent et analysent l'existence d'une discrimination génétique, le domaine le plus touché par cet épineux problème au fil des ans étant l'assurance-vie.[3178]

1089. Synthèse législative: pénal, civil, codes connexes. Il existe des restrictions à l'utilisation de ces tests par les employeurs ou les compagnies d'assurance afin de prévenir la discrimination génétique.[3179] La France a adopté des mesures législatives strictes pour prévenir la discrimination fondée sur l'information génétique.[3180]]. Dans le Code Pénal, cette notion est définie aux articles 225-1[3181] et 225-2, et les personnes reconnues coupables de discrimination

---

[3173] F. Dubet, *« Ce que les discriminations font aux individus et aux sociétés »,* Mélanges de la Casa de Velázquez, 2017. consulté le 16 septembre 2024. URL:http://journals.openedition.org/mcv/7719 ,DOI:https://doi.org/10.4000/mcv.7719.

[3174]J. Feldman *L'idée de science au XIXè siècle*, Editions L'Harmattan, *2006* https://www.librairiedalloz.fr/ebook/9782296157804-l-idee-de-science-au-xixe-siecle-jacqueline-feldman/.

[3175] S Neil McKenna. *Secret Life of Oscar Wilde*. Arrow, 2024.

[3176] Declaration of the Defender of Rights. Algorithmes, prévenir l'automatisation des discriminations May 2020 https://juridique.defenseurdesdroits.fr/index.php?lvl=notice_display&id=32665&opac_view=-1.

[3177] E. Uffelmann, et al. "*Genome-wide association studies"*. Nature Reviews Methods Primers 1.1, 2021. 59. https://www.nature.com/articles/s43586-021-00056-9.

[3178] Y. Joly, Ngueng Feze, I., Simard, J. *Genetic discrimination and life insurance : a systematic review of the evidence*. BMC Med, 2013. https://doi.org/10.1186/1741-7015-11-25.

[3179] C. Byk, *L'utilisation des tests génétiques dans le domaine de l'assurance en droit français et européen : une affaire d'assurance et de politique publique*. In : L. Khoury, A. Blackett, L. Vanhonnaeker(eds) *Genetic Testing and the Governance of Risk in the Contemporary Economy Ius Comparatum* - Global Studies in Comparative Law, vol 34. Springer, 2020. Cham. https://doi.org/10.1007/978-3-030-43699-5_8.

[3180] S. Bernatchez, *La Protection des Données Personnelles et la Recherche Scientifique en France*, Éditions Dalloz, 2019.

[3181] « Constitue une discrimination toute différence de traitement appliquée aux personnes physiques en base de l'origine, le sexe, la situation de famille, la grossesse, l'apparence physique, la particulière vulnérabilité résultant de la situation économique apparente ou connue de son auteur, le patronyme, le lieu de résidence, l'état de santé, la perte d'autonomie, le handicap, les caractéristiques génétiques, les mœurs, l'orientation sexuelle, l'identité de genre, l'âge, les opinions politiques, les activités syndicales, le statut de lanceur d'alerte, de facilitateur ou de personne liée à un lanceur d'alerte, en application de l'article 6 et de l'article 6-1 de la Loi n°2016-1691 du 9 décembre 2016

sont passibles d'une peine de trois ans d'emprisonnement et d'une amende de 45.000 euros.[3182] Parallèlement, l'article R.625-7 du Code Pénal établit également une peine contraventionnelle pour la discrimination et l'incitation à la discrimination, si l'action a lieu dans un lieu non public.[3183]

Le Code Civil interdit la discrimination (Art. 16-13 – « Nul ne peut être discriminé en raison de ses caractéristiques génétiques »)[3184] dans le domaine de l'assurance et de l'emploi sur la base des résultats de tests génétiques. Ceci est essentiel pour s'assurer que les individus ne sont pas désavantagés en raison de leur profil génétique[3185].

L'article L.1141-1 du Code de la Santé Publique stipule que nul ne peut faire l'objet d'une discrimination fondée sur des informations génétiques. Les assureurs et les employeurs ne sont pas autorisés à demander ou à utiliser les informations génétiques d'une personne pour prendre des décisions en matière de police d'assurance ou d'emploi.[3186] [3187]

À l'ère de la technologie, prévoyant l'évolution continue de l'analyse du génome[3188], la France renforce le droit du patient à la vie privée, ainsi que la protection contre la discrimination ou la protection des données génétiques personnelles, en adoptant en 2002 la Loi n° 2002-303**,** également connue sous le nom de loi Kouchner[3189], du nom de son fondateur[3190].

---

relative à l'égalité des devant la loi. 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique, la capacité à s'exprimer dans une langue autre que le français, l'appartenance ou la non-appartenance, vraie ou supposée, à une ethnie, une nation, une prétendue race ou une religion déterminée.
Est également considérée comme une discrimination toute différence de traitement appliquée à des personnes morales en raison des caractéristiques de leurs membres ou de certains d'entre eux, telles que l'origine, le sexe, la situation de famille, la grossesse, l'apparence physique, la vulnérabilité économique, le nom, la résidence, l'état de santé, la perte d'autonomie, le handicap, l'orientation sexuelle, l'identité de genre, l'appartenance ethnique, nationale, religieuse ou linguistique, telles que définies par le droit applicable ».

[3182] Le Code Pénal - Chapitre V, Section 1 : Des discriminations (articles 225-1 à 225-4).

[3183] « La provocation non publique à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance ou de leur non-appartenance, vraie ou supposée, à une ethnie, une nation, une prétendue race ou une religion déterminée est punie de l'amende prévue pour les infractions de la classe 5.
La même peine s'applique à la provocation non publique à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur sexe, de leur orientation sexuelle, de leur identité de genre ou de leur handicap, ainsi qu'à la provocation non publique aux discriminations visées aux articles 225-2 et 432-7 ».

[3184] Code Civil, Chapitre III : De l'examen des caractéristiques génétiques d'une personne et de l'identification d'une personne par ses empreintes génétiques (articles 16-10 à 16-13) https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006419313/2019-04-19.

[3185] O. Huez. *La Non-Discrimination Génétique : Perspectives Juridiques*. Cahiers de Droit Européen,vol.57, no.1. 2020.

[3186] J.-P. Costa, *Les Droits de 'Homme et la Bioéthique*, Éditions La Découverte, 2019.

[3187] Code du Travail, Section 7 : Discriminations (articles L112-45 à L112-45-5) https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006646204/2006-03-24.

[3188] Q. Gerard, A. De Paor, P. Blanck(eds.), *Genetic discrimination : transatlantic perspectives on the case for a European level legal response*, Routledge, 2014.

[3189] M.A. Shampon, R.A. Kyle, *Bernard Kouchner - Founder of doctors without borders.* Mayo Clin Proc, 2011. https://pmc.ncbi.nlm.nih.gov/articles/PMC3012640/.

[3190] *La loi du 4 mars 2002 dite « loi Kouchner »* https://shs.cairn.info/revue-les-tribunes-de-la-sante1-2014-1-page-27?lang=fr&tab=texte-integral.

Dans certains cas, les données génétiques collectées à des fins médicales ou scientifiques peuvent être demandées par les autorités judiciaires[3191]. Cependant cela est strictement encadré afin de ne pas porter atteinte aux droits des personnes concernées. En France, par exemple, le Code de Procédure Pénale et le règlement du FNAEG (fichier génétique) sont très stricts quant à l'utilisation des données génétiques dans le cadre d'enquêtes pénales[3192].

b). Discrimination génétique en Roumanie

1090. Conseil National de Lutte contre la Discrimination. En Roumanie, la définition, la lutte, la prévention et la sanction de la discrimination sont des termes réglementés par l'Ordonnance Gouvernementale n° 137/2000. En Roumanie, en tant qu'État démocratique et social fondé sur la primauté du droit, le principe d'égalité entre les citoyens, l'exclusion des privilèges et de la discrimination sont garantis par la loi.[3193] La discrimination fondée sur des motifs génétiques dans la fourniture de soins de santé, dans l'emploi, dans le domaine de l'assurance ou dans tout contexte social est réglementée par la Loi n° 95/2006.[3194] Selon l'art. 369 du Code Pénal, constitue infraction l'incitation à la haine ou à la discrimination.[3195] Les Roumains qui se sentent victimes de discrimination peuvent s'adresser au Conseil National de Lutte contre la Discrimination (CNCD), l'autorité nationale en matière de discrimination[3196].

c). Convention d'Oviedo et autres actes normatifs

[3191] J. Leonhard, *« La place de l'ADN dans le procès pénal »*, Cahiers Droit, Sciences & Technologies, 2019. consulté le 18 septembre 2024.URL: http://journals.openedition.org/cdst/1049 ; DOI : https://doi.org/10.4000/cdst.1049.

[3192] Code de Procédure Pénale L'article 706-55 du Code de Procédure Pénale français régit les obligations d'inscription des données au Fichier National Automatisé des Empreintes Génétiques (FNAEG), la base nationale automatisée des empreintes génétiques en France. Le texte intégral du Code de Procédure Pénale est disponible sur le site officiel de Legifrance : www.legifrance.gouv.fr.

[3193] ORDONNANCE n° 137 du 31 août 2000 relative à la prévention et à la sanction de toutes les formes de discrimination, publiée au BULLETIN OFFICIEL n° 431 du 2 septembre 2000 https://legislatie.just.ro/Public/DetaliiDocumentAfis/24129.

[3194] LOI n° 95 du 14 avril 2006 (**republiée**) portant réforme de la santé Publiée au BULLETIN OFFICIEL n° 652 du 28 août 2015 https://legislatie.just.ro/Public/DetailsDocument/71139.

[3195] « L'incitation du public, par quelque moyen que ce soit, à la violence, à la haine ou à la discrimination à l'égard d'une catégorie de personnes ou à l'égard d'une personne au motif qu'elle appartient à une catégorie spécifique de personnes définie sur la base de la race, de la nationalité, de l'ethnie, de la langue, de la religion, du sexe, de l'orientation sexuelle, de l'opinion ou de l'affiliation politique, de la fortune, de l'origine sociale, de l'âge, du handicap, d'une maladie chronique non contagieuse ou de l'infection par le VIH/SIDA est punie d'une peine d'emprisonnement de 6 mois à 3 ans ou d'une amende. »

[3196] DÉCISION n° 1.194 du 27 novembre 2001 (*mise à jour*) relative à l'organisation et au fonctionnement du Conseil National de Lutte contre les Discriminations (mise à jour jusqu'au 17 novembre 2003*) https://www.cncd.ro/wp-content/uploads/2020/12/HG_1194_2001_actualizat.pdf.

La question législative de la discrimination génétique en Europe. Les chercheurs qui utilisent des données génétiques à des fins scientifiques doivent se conformer à des normes éthiques strictes, garantissant la confidentialité et l'anonymat des données des participants.[3197] En outre, dans la plupart des pays, y compris en Roumanie et en France, les études impliquant des données génétiques doivent être approuvées par des comités d'éthique[3198]. La discrimination génétique est un problème majeur en Europe, et les cas signalés dans différents pays ont conduit à l'introduction de réglementations strictes. Cela a donné lieu à la Convention d'Oviedo, ratifiée par plusieurs pays européens, dont la France et la Roumanie, qui reconnaît que la recherche génétique est considérée comme une information personnelle relevant de la vie privée, qu'elle doit respecter les droits de l'homme et empêcher toute forme d'abus ou de discrimination[3199] [3200].

D'autres textes législatifs abordent la question de la discrimination, comme la Charte des Droits Fondamentaux de l'Union Européenne, Titre III - Égalité, Article 21.1 - Non-discrimination, qui interdit toute forme de discrimination et fait preuve d'une tolérance zéro à l'égard de celle-ci.[3201] La Convention des Nations Unies relative aux Droits des Personnes Handicapées[3202] et le Règlement Général sur la Protection des Données (RGPD)[3203] réglementent également ce sujet.

1091. Aux États-Unis, la loi sur la non-discrimination en matière d'information génétique (Genetic Information Nondiscrimination Act – GINA) interdit aux employeurs et aux compagnies d'assurance maladie d'accéder aux données génétiques d'autrui[3204].

d). Utilisation abusive des données génétiques – Tribu Havasupai

[3197] E.R. Anya, *Prince, Disclosing Privacy and Discrimination Protections in Informed Consent,* 33 Health Matrix, 2023. https://scholarlycommons.law.case.edu/healthmatrix/vol33/iss1/2.

[3198] P. Mehta, O Zimba, A.Y. Gasparyan, B. Seiil, M. Yessirkepov *Ethics Committees: Structure, Roles, and Issues.* J Korean Med Sci. 2023. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10293659/.

[3199] *Convention for the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medecine*, Convention of Human Rights and Biomedicine, Oviedo,1997.

[3200] R. Andorno, *The Oviedo convention: a European legal framework at the intersection of human rights and health law*. J Int Biotechnol Law. 2005. [CrossRef] [Google Scholar].

[3201] EU Charter of Fundamental Rights https://fra.europa.eu/en/eu-charter/article/21-non-discrimination.

[3202]United Nations Convention on the Rights of Persons with Disabilities https://ec.europa.eu/social/main.jsp?catId=1138&langId=en.

[3203] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (Règlement Général sur la Protection des Données - RGPD), Publié au Journal officiel de l'Union Européenne, L 119, le 4 mai 2016, ce règlement est également applicable en France et régit la protection des données génétiques. Disponible sur le site officiel EUR-Lex: www.eur-lex.europa.eu.

[3204]U.S. Department of Labor, *What is the Genetic Information Nondiscrimination Act (GINA*)? https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/our-activities/resource-center/faqs/gina.pdf.

1092. Un cas célèbre d'utilisation abusive de données génétiques est celui de la tribu Havasupai[3205]. En 1990, des membres de cette tribu ont été recrutés pour une étude génétique visant à explorer les causes du diabète de type 2. Cependant, leurs échantillons génétiques ont été utilisés sans consentement explicite pour des recherches ultérieures dans des domaines tels que la schizophrénie et la migration des populations, ce qui a déclenché un scandale majeur. En avril 2010, à la suite du procès « Tribu Havasupai vs. Arizona State University », cette dernière a accepté de verser 700.000 dollars à 41 membres de la tribu indienne[3206]. Cette affaire a souligné l'importance du consentement éclairé et de sa spécificité sur l'utilisation des analyses génétiques à des fins de recherche[3207].

1093. En conclusion, l'utilisation des données génétiques à des fins médicales et scientifiques est profondément influencée par les lois nationales et internationales qui protègent les droits des individus, garantissant la confidentialité, le consentement éclairé et la prévention de la discrimination génétique[3208]. En France et dans d'autres pays européens, le cadre législatif est orienté vers l'équilibre entre l'innovation scientifique et la protection des droits fondamentaux[3209].

d). Discrimination sociale

1094. La peur de la discrimination. Cependant, l'incertitude demeure au sein de la population à ce sujet. Les gens sont sceptiques et anxieux, avec de nombreuses craintes[3210] qui influencent leur mode de vie et leurs décisions en matière de santé, comme le montrent Annet Wauters et Ine Van Hoyweghen dans leur analyse de 2016 de 42 études sur le sujet.[3211] Les craintes de discrimination chez les individus sont principalement dirigées vers le secteur de l'assurance, mais aussi vers l'environnement social, ce dernier étant moins discuté dans médias. La discrimination sociale se réfère à la stigmatisation et au manque de respect et peut

---

[3205] E. Blakemore, *Why the Navajo Nation Banned Genetic Research*. A&E Television Networks. 2017. https://www.history.com/news/why-the-navajo-nation-banned-genetic-research .

[3206] O. Huez. *Éthique et Conséquences Juridiques des Utilisations Abusives des Données Génétiques*, Cahiers de Droit Européen, vol. 57, no. 1, 2018.

[3207] M. Sanders, *Genomic Research in Indian Country: The New Road to Termination?* Okla. City U. L. Rev., 2014. https://ssrn.com/abstract=2318615 ou http://dx.doi.org/10.2139/ssrn.2318615.

[3208] F. FERRAND *Répertoire de procédure civile. Exigence d'un consentement de l'intéressé (879 - 883) (1) - 880. Les articles 16-10 et 16-11 du code civil*, - Dalloz, 2013.(https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ENCY/PCIV/RUB000108/2013- 12/PLAN225.

[3209] S. Bernatchez, *La Protection des Données Personnelles et la Recherche Scientifique en France*, Éditions Dalloz, 2019.

[3210] K.H. Rothenberg, S.F Terry, *Human genetics. Before it's too late--addressing fear of genetic information.* Science. 2002 Jul 12;297(5579):196-7. doi : 10.1126/science.1075221. PMID : 12114610.

[3211] A.Wauters, I Van Hoyweghen, *Global trends on fears and concerns of genetic discrimination: a systematic literature review.* J Hum Genet, 2016, p.275-282. https://www.nature.com/articles/jhg2015151.

considérablement influencer la qualité de vie ainsi que les décisions, c'est pourquoi il important de la réglementer[3212].

Bien que bien réglementée, avec une législation interdisant clairement la discrimination (voir également la déclaration de l'Unesco de 1997)[3213], l'attention des autorités reste focalisée sur cette question, comme en témoigne le séminaire intitulé « Prévention de la discrimination et des choix d'orientation : quels enjeux, quelles alliances ? » en mars 2024 à Paris, organisée par les organisations concernées[3214] en France. Les principaux thèmes abordés étaient l'analyse des cas de discrimination actuels et la promotion des actions de lutte contre les discriminations[3215].

§2. DEMANDE D'EXAMINER LES PROPRES CARACTÉRISTIQUES GÉNÉTIQUES

L'utilité de la médecine de précision dépend de la recherche d'un maximum de profils génétiques et donc de l'acceptation par un maximum d'individus de l'analyse de leur génome personnel, ce qui nécessite confiance et confidentialité[3216]. Nous savons que la science n'a pas toujours été digne de confiance et n'a pas toujours traité tous les participants sur un pied d'égalité[3217], c'est la protection juridique des données et la garantie de systèmes d'information sûrs jouent un rôle crucial. Aujourd'hui, le partage des données repose sur le consentement éclairé du patient, la législation européenne reconnaissant la vie privée comme un droit humain fondamental et fixant des limites strictes à la protection des données personnelles.[3218]

A. Transparence pour l'utilisation des données génétiques

[3212] Lemke, T. *Perspectives on genetic discrimination,* Routledge, 2013. https://www.researchgate.net/publication/261831054_Perspectives_on_Genetic_Discrimination.
[3213] Déclaration internationale de l'UNESCO du 11 novembre 1997 sur le génome humain et les droits de l'homme. https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=T128423.
[3214] Ces organisations sont : *France Urbaine* - https://www.franceurbaine.org/ *Intercommunalités de France* - https://www.intercommunalites.fr/, *le Réseau Ressources Pour l'Egalité des Chances et l'Intégration (RECI*) - https://www.reci-egalite.fr/.
[3215] France : *Prévention des discriminations et choix d'orientation - quels enjeux, quelles alliances Séminaire national RECI,* Paris 2024. https://migrant-integration.ec.europa.eu/index.php/event/france-prevention-des-discriminations-dorientation-quels-enjeux-quelles-alliances.fr.
[3216] Aronson, J. Samuel, L. Heidi, Rehm. "*Building the foundation for genomics in precision medicine*", Nature, 2015. https://www.nature.com/articles/nature15816.
[3217] M. Develaki, *Trustworthiness of Science in Debate: Challenges, Responses, and Implications*, Sci & Educ, 2022. https://doi.org/10.1007/s11191-021-00300-4.
[3218] S. Wachter, *Privacy: Primus Inter Pares - Privacy as a Precondition for Self-Development, Personal Fulfilment and the Free Enjoyment of Fundamental Human Rights*, SSRN, 2017.https://ssrn.com/abstract=2903514 ou http://dx.doi.org/10.2139/ssrn.2903514.

1095. Utilisation des données génétiques, uniquement avec accord préalable. En France, selon les articles 16-10 et L.1130-1 du Code Civil et du Code de la Santé Publique, le consentement éclairé est obligatoire et essentiel pour protéger les droits des patients et assurer la transparence dans l'utilisation des données génétiques.[3219] Dans le Code Pénal, ces droits relèvent de la protection de la vie privée, l'article 226 prévoyant des sanctions graves en cas de violation de la confidentialité.[3220] Dans ce contexte, le Règlement Général sur la Protection des Données (RGPD) a affiné le consentement du patient - il doit être libre, spécifique, éclairé et sans équivoque, et impose également des exigences en ce qui concerne la capacité de la personne à prendre des décisions éclairées.[3221] [3222]

Il n'existe pas de définition claire des tests génétiques, mais d'une manière générale, il s'agit de l'analyse de l'ADN pour détecter des traits génétiques spécifiques, des variations ou des susceptibilités.[3223] Dans le domaine de la santé, les tests génétiques sont de plus en plus accessibles et les gens sont de plus en plus curieux de connaître leurs informations génétiques, tout en leur offrant des options efficaces pour le traitement ou même la prévention des maladies.[3224]

a). Utilisation du corps humain à des fins médicales et scientifiques

1096. Les avantages de la recherche génomique. La recherche en génomique en France est à un niveau avancé[3225], avec de multiples projets de recherche explorant le rôle du génome humain dans la santé et la maladie. Des projets de séquençage génétique à grande échelle, tels que le Projet 100.000 Génomes, ont contribué à une meilleure compréhension de la diversité génétique et de son impact sur la santé humaine[3226]. Un autre projet est l'Alliance Aviesan,

---

[3219] « *La législation Bioéthique en France* », Code Civil et Code de la Santé Publique, articles 16-10 et L.1130-1.
[3220] Code pénal : *Chapitre VI : Des atteintes à la personnalité (articles 226-1 à 226-32)* *https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006149831?init=true&page=1&query=code+penal&searchField=ALL&tab_selection=all&anchor=LEGISCTA000006149831#LEGISCTA000006149831.*
[3221] European Union, "*Regulation (EU) 2016/679 of the European Parliament and of the Councill*", 2016, *Official Journal of the European Union* 1-88.
[3222] Le GDPR définit les données génétiques comme « les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne, résultant de l'analyse d'un échantillon biologique de la personne concernée, en particulier de l'analyse des chromosomes, de l'acide désoxyribonucléique (ADN) ou de l'acide ribonucléique (ARN), ou de l'analyse d'un autre élément fournissant des informations équivalentes ».
[3223] S. Patel, I. Varley, *Exploring the Regulation of Genetic Testing in Sport*. The Entertainment and Sports Law Journal, 2019.
[3224] L.O. Gostin, J.G. Hodge, *Genetic Privacy and the Law : An End to Genetics Exceptionalism*. Jurimetrics Journal, 1999.
[3225] D. Sanlaville, M. Vidaud, C. Thauvin-Robinet, F. Nowak, F. Lethimonnier. *Plan France médecine génomique 2025: la France entre dans l'ère de la médecine génomique,* La Revue du Praticien, 2021. https://www.larevuedupraticien.fr/article/plan-france-medecine-genomique-2025- la-france-entre-dans-lere-de-la-medecine-genomique.
[3226] P. Martin. *Projets de Séquençage à Grande Échelle en France*, Éditions Dalloz, 2022.

lancée en 2015 à la demande du Premier ministre Manuel Valls, qui vise à tracer une perspective à 10 ans sur l'accès de la population aux tests et aux diagnostics génétiques.[3227]

1097. Histoire législative. Le code civil français promulgué en 1804[3228] (plus connu sous le nom de Code Napoléon), l'un des codes juridiques les plus influents au monde, qui a eu un impact colossal sur le développement des systèmes juridiques, tant en France que dans toute l'Europe et en Amérique Latine, ne réglemente pas explicitement le corps humain en tant que sujet de droit distinct. En d'autres termes, la personne du Code Napoléon n'a pas de corps. Toutefois, certains principes pertinents ont été établis : le corps humain ne peut être traité comme une marchandise, il ne peut être vendu ou échangé de quelque manière que ce soit, établissant ainsi le respect et la dignité de l'être humain. Bien que le Code Napoléon n'aborde pas explicitement la notion de droit à l'intégrité corporelle telle que nous l'entendons aujourd'hui, il est à la base de l'idée qu'une personne a des droits sur son propre corps et que celui-ci ne peut être violé ou touché sans consentement. Bien entendu, le Code Civil de 1804 ne réglementait pas des questions telles que les transplantations d'organes, les dons de sang, les tests génétiques, car elles ne faisaient pas partie des préoccupations juridiques de l'époque[3229].

Des réglementations plus détaillées sur l'utilisation du corps humain à des fins médicales et scientifiques ont été élaborées plus tard au cours du 20e siècle. Parmi les premiers documents sur le développement de ce sujet figurent la Loi de l'Anatomie de 1832 en Grande-Bretagne[3230], le Code de Nuremberg (1947)[3231], la Déclaration d'Helsinki (1964)[3232].

1098. Questions actuelles. Aujourd'hui, la question de la nature du corps humain est complexe et débattue dans des domaines tels que la recherche, la médecine, l'éthique, avec d'importantes implications juridiques. Des questions telles que : Qu'est-ce que le corps humain ? Est-il un objet de droit ? Est-il une chose ? Est-il un substrat ? Est-il une identité ? Quel rôle joue l'ADN dans la définition du corps humain ? Qui a des droits sur mon corps ? Qui a un droit sur mon ADN ? Ces questions sont controversées et sensibles et obligent donc le législateur à protéger le corps humain par un ensemble de règles claires et imbattables.[3233]

[3227] *France médecine génomique 2025*. Alliance nationale pour les sciences de la vie et de la santé, 2015 https://www.inserm.fr/wp-content/uploads/2017-11/aviesan-planfrancemedecinegenomique-2025.pdf.

[3228] *The Napoleon Code* :https://courses.lumenlearning.com/suny-hccc-worldhistory2/chapter/the-napoleonic-code/.

[3229] Britannica, The Editors of Encyclopaedia. *"Napoleonic Code*". Encyclopedia Britannica, 2024, https://www.britannica.com/topic/Napoleonic-Code.https://www.britannica.com/topic/Napoleonic-Code. Consulté le 5 septembre 2024.

[3230] R. Haddaway, *Anatomy Act. In: The Palgrave Encyclopedia of Victorian Women's Writing,* Palgrave Macmillan, 2021. https://doi.org/10.1007/978-3-030-02721-6_40-1.

[3231] The Nuremberg Code (1947) *BMJ,* 1996. doi : https://doi.org/10.1136/bmj.313.7070.1448

[3232] *DECLARATION OF HELSINKI Recommendations guiding doctors in clinical research*. Adopted by the 18th World Medical Assembly, Helsinki, Finlande, 1964 https://www.wma.net/wp- content/uploads/2016/11/DoH-Jun1964.pdf.

[3233] V. Cabrillac, *Le corps humain, in Libertés et droit fondamentaux*, Dalloz 2023.- REVET, « Le corps humain est-il une chose appropriée ? », in *RTD*, 2017.

La Loi française de Bioéthique, qui a énormément évolué au cours des 20e et 21e siècles[3234], a intégré des règles plus détaillées sur le corps humain, le don d'organes, l'assistance médicale à la procréation et la recherche scientifique sur le génome humain, clarifiant et complétant ce que le Code Napoléon n'avait pas prévu[3235].

b). Vision sur le corps humain, à partir de la philosophie au droit

1099. Le corps humain : du sens au statut. Aujourd'hui, la définition du corps humain varie selon les domaines – religieux, philosophique[3236], juridique – chacun abordant la signification et la nature du corps d'une manière distincte, mais complémentaire.[3237]

Dans le christianisme, le corps est considéré comme le temple du Saint-Esprit (1 Corinthiens 6:19-20), et il est enseigné aux croyants de le garder propre et respecté. L'intégrité corporelle est liée aux aspects moraux et intellectuels.[3238] Dans l'islam, le corps humain est considéré comme un don d'Allah, confié temporairement à l'homme, et doit être respecté et entretenu selon les lois divines (charia). Il est interdit de le mutiler ou de le vendre[3239].

La philosophie offre une variété de perspectives sur le corps humain, selon tradition philosophique. Dans la philosophie antique, Platon et Aristote ont discuté de la relation entre le corps et l'âme. Platon considérait le corps comme une « prison » de l'âme[3240], tandis qu'Aristote considérait l'âme et le corps comme un tout unitaire[3241]. L'existentialisme[3242] (Jean-Paul Sartre) et la phénoménologie (Maurice Merleau-Ponty) soulignent que notre expérience corporelle est inséparable de notre conscience et de notre existence dans le monde. Le corps n'est pas seulement un objet physique, mais une manifestation du moi en relation avec le monde[3243].

[3234] T., Dominique, *Les lois françaises de bioéthique : Leur construction, leurs évolutions*. Médecine/Sciences, 2019.https://www.researchgate.net/publication/330560340_Les_lois_francaises_de_bioethique_Leur_construction_leu rs_evolutions.

[3235] LOI n° 2021-1017 du 2 août 2021 *relative à la bioéthique sur l'utilisation des données génétiques à des fins scientifiques et médicales* disponible sur : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000043884384.

[3236]U. Plöckinger, U, Ernst-Auga, *Bioethics and the Human Body*. Religions 2024. https://doi.org/10.3390/rel15080909.

[3237] C. Bublitz, *The body of law: boundaries, extensions, and the human right to physical integrity in the biotechnical age,* Journal of Law and the Biosciences, Volume 9, Issue 2, 2022,.https://doi.org/10.1093/jlb/lsac032.

[3238] *Bible* : https://www.bibliaortodoxa.ro.

[3239] A. Shamsy, N.J. Coulson, "*Sharia*". Encyclopedia Britannica, 2024, https://www.britannica.com/topic/sharia. https://www.britannica.com/topic/sharia. consulté le 5 septembre 2024.

[3240] Platon, "*Phaidon*", în *Opere*, vol. IV, traduit en roumain par Petru Creția, Editura Științifică și Enciclopedică, 1983. p.9-340.

[3241] R. D. Hicks, *Aristote De Anima with Translation, Introduction, and Notes,* Cambridge University Press, 1907.

[3242] A. Kevin, "*Existentialism*", The Stanford Encyclopedia of Philosophy, 2023. <https://plato.stanford.edu/archives/sum2023/entries/existentialism/>.

[3243] M.-P. Maurice. *Phenomenology of Perception*, Routledge 2013.

D'un point de vue juridique, le Code Civil Français, à l'instar du code civil roumain, consacre le principe de l'inviolabilité et de l'inaliénabilité du corps humain, protégeant l'intégrité et la dignité de la personne et imposant des restrictions claires à son utilisation.

1100. Le corps humain : protection législative spéciale. Le Code Civil Roumain réglemente les questions relatives au corps humain dans le Livre I, Titre II, consacré aux Personnes. Selon ce code, le corps humain est inviolable et inaliénable, et fait l'objet d'une protection spéciale. L'Article 66 stipule que le droit de toute personne à la vie, à la santé et à l'intégrité physique et mentale est garanti et protégé par la loi. L'Article 67 prévoit que toute intervention sur le corps humain n'est permise qu'à des fins thérapeutiques, avec le consentement éclairé de la personne. L'Article 68 précise que le corps humain ne peut faire l'objet de transactions commerciales et qu'est interdit d'en disposer par des actes entre personnes vivantes[3244].

Dans le Code Civil Français, le corps humain est principalement régi par les articles inclus dans le Titre I de la Charte des Personnes. L'Article 16-1 stipule que toute personne a droit au respect de son corps. Le corps humain est inviolable et inaliénable. Aucune de ses parties ne peut faire l'objet de droits patrimoniaux. L'Article 16-3 précise que toute intervention sur le corps d'une personne doit être justifiée par une nécessité médicale et ne peut se faire qu'avec le consentement libre et éclairé de la personne, et l'Article 16-5 renforce l'idée que le corps humain, ainsi que ses produits et ses éléments, ne peuvent faire l'objet d'un commerce[3245].

L'analyse de ces réglementations soulève des questions qui restent à débattre, telles que: Puis-je demander l'examen de mes propres caractéristiques génétiques ? Quelqu'un d'autre aurait le droit de le faire à ma place ?[3246] Ces questions sont examinées ci-dessous.

B. Tests génétiques sans intervention d'un médecin, directement au consommateur

1101. Tests génétiques commandés par le consommateur. Les tests génétiques sont accessibles à la population générale depuis les années 1960, et ne pouvaient être effectués qu'à des fins médicales, sur recommandation d'un spécialiste et après signature d'un consentement

[3244] Code Civil de Roumanie, Republié au Journal Officiel de Roumanie, Livre I, Chapitre II Respect dû à l'être humain et à ses droits inhérents, Section 2e Droits à la vie, à la santé et à l'intégrité de la personne physique, Art. 61-69 No. 505 du 15 juillet 2011 https://www.codulcivil.ro/.

[3245]Le Code Civil – Chapitre II : Du respect du corps humain (articles 16 à 16-9) https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070721/LEGISCTA000006136059/#LEGISCTA000006136059.

[3246] *Réflexion éthique sur l'évolution des tests génétiques liés au séquençage de l'ADN humain à très haut débit*. Comité Consultatif National d'Ethique pour les sciences de la vie et de la santé, 2016. https://www.ccne-ethique.fr/sites/default/files/2021-02/ccne_avis_124.pdf.

éclairé.[3247] Aujourd'hui, il existe une grande variété de tests génétiques qui peuvent être commandés en ligne par les consommateurs, qu'ils soient médicaux ou non[3248]. Ces types de tests sont connus sous le nom générique de tests ADN DTC ("Direct to Consumer")[3249] et les principaux laboratoires internationaux qui les proposent sont *23andMe, AncestryDNA, FamilyTree DNA et MyHeritage***.** Les tests DTC impliquent la fourniture de services génétiques directement au consommateur, sans l'intervention d'un médecin. La première catégorie comprend les tests diagnostiques pour le diabète, les maladies cardiovasculaires, la mucoviscidose, les tests visant à évaluer le risque de différents types de cancer ou les tests pour les maladies liées au chromosome X ou autosomiques récessives. Les tests non médicaux comprennent les tests sur l'ascendance, les origines ancestrales, les tests de performance sportive, les tests de traits (couleur des yeux, type de cérumen).[3250] Cette pratique est considérée comme controversée et a été intensément critiquée[3251], avec de nombreux débats sur les tensions entre le progrès scientifique et l'éthique et sur la façon dont la génétique peut influencer notre perception de l'identité et du corps humain.[3252] D'une part, les partisans de cette méthode estiment qu'elle renforce la protection de la vie privée, en contournant le système de soins de santé et en rendant les consommateurs responsables de leur propre santé.[3253] D'autre part, elle permet d'identifier les maladies génétiques à des stades précoces, lorsqu'elles sont plus faciles à gérer, voire à prévenir. La médecine personnalisée, facilitée par la compréhension des profils génétiques individuels, permet des traitements plus efficaces et mieux adaptés, réduisant les risques d'effets secondaires et améliorant les résultats thérapeutiques.[3254] En outre,

[3247] P.G. Sanfilippo, L.S. Kearns, P. Wright, D.A Mackey, A.W. Hewitt, *Current landscape of direct-to-consumer genetic testing and its role in ophthalmology: a review*, Clin Exp Ophthalmol, 2015. [PubMed] [CrossRef] [Google Scholar] [Ref list].

[3248] A.M. Phillips, "*Only a clic away – DTC genetics for ancestry, health, love… and more: A view of the business and regulatory landscape"*, Appl. Transl Genom. 2016. https://pubmed.ncbi.nlm.nih.gov/27047755/.

[3249] S.M. Onstwedder, M.E. Jansen, M.C. Cornel, T. Rigter T. *Policy Guidance for Direct-to-Consumer Genetic Testing Services: Framework Development Study.* J Med Internet Res. 2024 https://pubmed.ncbi.nlm.nih.gov/39018558/

[3250] EASAC and FEAM Working Group (2012) *Direct-to-consumer genetic testing for health-related purposes in the European Union*. Consulté le 10 janvier 2014 à l'adresse http://www.easac.eu/home/reports-and-statements/detail-view/article/direct-to-co.html [Ref list].

[3251] J.S. Roberts, J. Ostergren, *Direct-to-Consumer Genetic Testing and Personal Genomics Services : A Review of Recent Empirical Studies*. Curr Genet Med Rep. 2013.

[3252] J.H., Déchaux, *L'individualisme génétique : marché du test génétique, biotechnologies et transhumanisme*. Revue française de sociologie, 2019. URL : https://shs.cairn.info/revue-francaise-de-sociologie-2019-1-page-103?lang=fr.

[3253] C. Marietta, A.L. Mcguire, *Direct-to-consumer genetic testing: is it the practice of medicine ?* J Law Med Ethics, 2009. [PMC article gratuit] [PubMed]
[CrossRef] [Google Scholar].

[3254] Genetic Alliance, The New York-Mid-Atlantic Consortium for Genetic and Newborn Screening Services, *Understanding Genetics: A New York, Mid-Atlantic Guide for Patients and Health Professionals*, Washington (DC), 2009. Available from: https://www.ncbi.nlm.nih.gov/books/NBK115571/.

l'identification des risques génétiques peut guider les décisions relatives au mode de vie et les interventions préventives, jouant ainsi un rôle crucial dans la santé publique et individuelle.[3255]

1102. Préoccupations. D'une autre part, les critiques estiment qu'il y a un risque accru de produire un stress inutile par l'interprétation et la gestion incorrectes des résultats des tests par les consommateurs sans formation médicale.[3256] Outre les implications éthiques et sociales[3257], la sécurité du stockage des données suscite également des inquiétudes. Ces critiques sont également étayées par le scandale de la vente de données génétiques par 23andMe. L'entreprise, qui propose des services de tests génétiques directement aux consommateurs, a conclu un accord avec la société pharmaceutique GlaxoSmithKline pour partager l'accès à sa base de données génétiques. Cela a suscité des inquiétudes quant à la confidentialité des données personnelles et à la manière dont les informations génétiques des clients sont utilisées.[3258] En 2023, l'entreprise s'est retrouvée au cœur d'un nouveau scandale. Un pirate informatique a accédé à la base de données ADN, affectant plus de 6 millions d'utilisateurs[3259].

1103.

a). Réglementation des tests génétiques

1104. La situation juridique des tests DTC dans l'UE. Dans l'Union Européenne, outre le cadre juridique national[3260], les tests DTC sont réglementés par le Règlement (UE) 2017/746 relatif aux dispositifs médicaux de diagnostic in vitro (DMDIV), entré en vigueur en mai 2022. Il impose des normes strictes pour les tests génétiques proposés directement aux consommateurs. Les tests génétiques sont considérés comme des dispositifs médicaux de diagnostic in vitro et doivent répondre à des normes strictes de sécurité, d'efficacité et de fiabilité. Les entreprises doivent fournir des informations claires sur l'objectif du test, ses limites et ses risques.[3261] Les tests doivent être conformes au Règlement Général sur la Protection des

---

[3255] O. Huez, *Les Enjeux de la Législation en Génétique : Vers une Protection Globale,* Cahiers de Droit Européen, vol. 57, no. 1, 2020.

[3256]H.C Howard, P. Borry, *Is there a doctor in the house?: the presence of physicians in the direct-to-consumer genetic testing context*. J Commun Genet. 2012. [PMC free article] [PubMed] [CrossRef] [Google Scholar].

[3257] H. Jautrou. *Les tests génétiques en libre accès - Régulation par le marché, ou régulation médicale* Med Sci, 2020. DOI : https://doi.org/10.1051/medsci/2019264.

[3258] S. Bernatchez. *La Vente des Données Génétiques : Entre Confidentialité et Commerce*, Journal de Droit Médical et Éthique, vol. 4, no. 2, 2021.

[3259] E. Roth. *23andMe admits hackers accessed 6.9 million users DNA Relatives data,* Verge Deals, 2023 https://www.theverge.com/2023/12/4/23988050/23andme-hackers-accessed-user-data-confirmed.

[3260] P. Borry, P., R. van Hellemondt, D. Sprumon*t et al*, Legislation on direct-to-consumer genetic testing in seven European countries. Eur J Hum Genet, 2012. https://doi.org/10.1038/ejhg.2011.278.

[3261] Règlement (UE) 2017/746 du Parlement Européen et du Conseil du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro et abrogeant la Directive 98/79/CE et la Décision 2010/227/UE de la Commission https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32017R0746&from=LV.

Données (RGPD), garantissant la protection de la vie privée et le traitement approprié des données génétiques.[3262]

1105. Aux États-Unis. Aux États-Unis, les tests génétiques DTC sont réglementés par deux institutions principales : la Food and Drug Administration (FDA), qui réglemente les tests génétiques DTC commercialisés en tant que dispositifs médicaux. Ces dernières années, la FDA a approuvé plusieurs tests DTC pour les risques génétiques, à condition qu'ils soient accompagnés d'une documentation appropriée concernant les limitations et les risques des tests.[3263] Et la Federal Trade Commission (FTC), qui suit les plaintes concernant la publicité mensongère ou les pratiques commerciales déloyales des entreprises qui fournissent des tests DTC.[3264]

1106. Dans divers pays européens. La Suisse dispose d'une réglementation spécifique[3265] pour les tests génétiques par le biais de la Loi fédérale sur les tests génétiques humains (GUMG), qui exige que tous les tests génétiques proposés directement aux consommateurs soient approuvés par un médecin et comprennent un conseil génétique pour l'interprétation des résultats[3266].

En 1997, compte tenu de la législation en vigueur à l'époque et du développement rapide de la biologie et de la médecine, la Convention Européenne sur les Droits de l'Homme et la Biomédecine[3267] (Convention d'Oviedo) a été adoptée, ce qui oblige les pays participants à réglementer leur législation nationale conformément à ses principes. La Convention vise à protéger les droits de l'homme, la dignité, l'identité et l'intégrité dans des domaines tels que la génétique et la médecine[3268]. Les pays qui ont ratifié la Convention sont : l'Espagne, la Bulgarie, la Croatie, la Lituanie, la Moldavie, l'Islande, la République Tchèque, le Danemark, la Grèce, Chypre, l'Estonie, la Hongrie, le Portugal, la Roumanie, la Slovaquie, Saint-Marin, la Slovénie,

---

[3262] *Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (Règlement Général sur la Protection des Données - RGPD*), Publié au Journal Officiel de l'Union Européenne, L 119, le 4 mai 2016, ce règlement est également applicable en France et régit la protection des données génétiques. Disponible sur le site officiel d'EUR-Lex : www.eur-lex.europa.eu.

[3263] *Food and Drug Administration (FDA*) https://www.fda.gov/search?s=DTA+DNA+test.

[3264] E. Jillson, *The ADN of privacy and the privacy of DNA,* FTC Division of Privacy & Identity Protection 2024. https://www.ftc.gov/business-guidance/blog/2024/01/dna-privacy-privacy-dna.

[3265] D. Sprumont: *Quelle réglementation des trousses d'analyse génétique*; in C. Joye(ed): *L'analyse génétique humaine: quelles perspectives législatives,* Schulthess, 2004, p. 71-88. Google Scholar.

[3266] La loi fédérale sur l'analyse génétique humaine en Suisse / « Loi sur l'analyse génétique humaine » est entrée en vigueur en 2007 : https://insightplus.bakermckenzie.com/bm/healthcare-life-sciences/switzerland-the-new-human- genetic-testing-act-and-correlating-ordinances.

[3267] La Convention pour la protection des droits de l'homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médicine : Convention sur les droits de l'homme et la biomédicine, Oviedo, 1997.http://ccea.usv.ro/legislatie/6._Conventia_pt_protectia_drepturilor_omului.pdf.

[3268] R. Andorno, *The Oviedo Convention : A European Legal Framework at the Intersection of Human Rights and Health Law. Journal of International Biotechnology Law*, 2005.

la Turquie et la Géorgie.[3269] Parmi les grands absents on compte : le Royaume-Uni, l'Allemagne et la France. Le Royaume-Uni considère les principes de la Convention trop stricts, l'Allemagne trop permissives.[3270] La France, initialement signataire de la Convention, a dû se retirer pour attendre l'adoption de sa loi nationale de bioéthique. Elle a ensuite ratifié la Convention le 13 décembre 2011.[3271] À l'été 2024, Amélie Dionisi-Peyrusse a publié une analyse dans le *Recueil Dalloz* sur les 30 dernières années concernant les principales lacunes de la législation en matière de bioéthique. Celles-ci découlent des avancées rapides dans des domaines tels que la fécondation in vitro (FIV), l'insémination artificielle, la maternité de substitution, la recherche sur l'embryon, la réingénierie du génome humain, qui nécessitent une mise à jour fréquente de la loi. Dans ce contexte, l'auteur considère que la législation ne suit pas le progrès, ce qui donne lieu à des litiges et à des limitations éthiques[3272].

1107. Alignement de la Roumanie sur la législation européenne. La Roumanie, bien qu'elle ait signé et ratifié la Convention d'Oviedo, s'engageant ainsi à respecter les dispositions de l'Article 12, n'a pas explicitement introduit dans sa législation l'obligation d'une recommandation médicale pour les tests génétiques[3273]. Dans la législation roumaine, les tests génétiques sont réglementés par une série d'actes normatifs qui régissent la manière dont les tests génétiques sont effectués, leur confidentialité et les contextes dans lesquels ils peuvent être utilisés. La Loi n° 95/2006 sur la réforme des soins de santé souligne au Chapitre IV le droit du patient à l'information, à la confidentialité et au refus des tests génétiques effectués à des fins médicales. L'Article 618 aborde également les questions de prévention et de détection des maladies par l'utilisation de tests génétiques[3274]. La Loi n° 46/2003 sur les droits des patients prévoit, à l'Article 14, le droit du patient à la vie privée et à la confidentialité en ce qui concerne les informations personnelles et les tests génétiques, ces derniers nécessitant le consentement éclairé du patient. En outre, l'Art.12 stipule que toute intervention médicale, y compris les tests génétiques, doit être effectuée seulement après que le patient a été informé et a donné son consentement.[3275] Le Règlement Général sur la Protection des Données (RGPD) – Règlement

[3269] *État des signatures et ratifications du traité 164*, Conseil de l'Europe, 1999. https://www.coe.int/fr/web/conventions/full- list?module=signatures-by-treaty&treatynum=164.

[3270] R.Andorno, *The Oviedo convention: a European legal framework at the intersection of human rights and health law*, J Int Biotechnol Law, 2005. [CrossRef] [Google Scholar].

[3271] A. Mirkovic, La *Ratification (enfin !) de la convention d'Oviedo sur les droits de l'homme et la biomédecine*. Recueil Dalloz, 2012 https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=RECUEIL/CHRON/2011/0492.

[3272] A. Dionisi-Peyrusse, *30 ans de lois de bioéthique: une grande œuvre inachevée*, Recueil Dalloz, 2024.

[3273] Eurogentest, *Overview of countries who have ratified the European Convention on Human Rights and Biomedicine*, 2002. http://www.eurogentest.org/fileadmin/templates/eugt/pdf/Overview_of_ratifying_countries_-EuroGentest_website.pdf [Ref list].

[3274] *Loi n° 95/2006 sur la réforme des soins de santé,* publiée au Journal Officiel de la Roumanie, Partie I, n° 372 du 28 avril 2006.

[3275] *Loi n° 46/2003 sur les droits des patients*, publiée au Journal Officiel de la Roumanie, partie I, n° 51 du 29 janvier 2003.

(UE) 2016/679, également applicable en Roumanie, qui a conduit à l'abrogation de la loi n° 677/2001 pour la protection des personnes physiques à l'égard du traitement des données à caractère personnel et de la libre circulation de ces données[3276], définit à l'art. 4 paragraphes 13-15 les données génétiques, en soulignant leur caractère personnel.

Leur traitement n'est autorisé que dans certaines conditions strictes, telles que le consentement explicite de la personne ou la nécessité d'un diagnostic ou d'un traitement. L'Article 9 réglemente clairement les conditions dans lesquelles les données génétiques peuvent être traitées, ainsi que la nécessité d'un niveau elevé de protection.[3277] La Loi n° 17/2001 ratifiant la Convention pour la protection des droits de l'homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine (Convention d'Oviedo) prévoit que tout test génétique ne peut être effectué que pour des raisons médicales, s'il y a un bénéfice pour la santé du patient et seulement après la signature d'un consentement éclairé[3278].

b). Respect des données privées du patient

1108. Expertise génétique judiciaire. Dans le nouveau Code de Procédure Pénale mis à jour en 2024, l'article 191 précise que l'expertise médico-légale génétique peut être réalisée dans des conditions strictes, sur ordonnance ou avec l'accord du tribunal. L'expertise génétique judiciaire doit être effectuée dans des institutions médico-légales ou dans une institution certifiée et accréditée pour ce type d'analyses. Le matériel biologique prélevé lors de l'examen corporel ne peut être utilisé que pour identifier le profil génétique médico-légal, les données obtenues étant considérées comme des données personnelles et protégées par la loi.[3279] La loi n° 95 du 14 avril 2006 sur la réforme de la santé réglemente dans sa partie IV la réalisation de prélèvements et de transplantations d'organes, de tissus et de cellules d'origine humaine à des fins thérapeutiques, en stipulant clairement que les informations génétiques ne peuvent être fournies qu'en protégeant l'identité de la personne concernée.[3280] L'arrêté n° 904 du 25 juillet 2006 portant approbation des Normes sur l'application des règles de bonne pratique dans la conduite

---

[3276] *Loi n° 677/2001 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données,* Publiée au Journal Officiel de la Roumanie, partie I, n° 790 du 12 décembre 2001. (Abrogée)

[3277] *Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016*, publié au Journal Officiel de l'Union Européenne, L 119, le 4 mai 2016.

[3278] *Loi n° 17/2001 sur la ratification de la Convention pour la protection des droits de l'homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine (Convention d'Oviedo),* Publiée au Journal Officiel de Roumanie, partie I, n° 103 du 28 février 2001.

[3279] Art. 191 Nouveau Code de Procédure Pénale Expertise génétique judiciaire Expertise et constatation https://legeaz.net/noul-cod-procedura-penala-ncpp/art-191.

[3280] LOI n° 95 du 14 avril 2006 sur la réforme de la santé https://www.cdep.ro/pls/legis/legis_pck.htp_act_text?idt=72105.

des essais cliniques réalisés avec des médicaments à usage humain, détaille les procédures spécifiques liées à la réalisation de tests génétiques dans le contexte médical.[3281]

L'analyse de la législation roumaine telle qu'exposée ci-dessus nous permet de conclure qu'elle met l'accent sur la protection et le respect des données privées du patient, l'information correcte du patient sur la finalité et les implications du test génétique, la limitation des abus et de la discrimination, et en même temps la protection de la dignité et de l'intégrité de la personne. Elle souligne également que les tests génétiques doivent être utilisés de manière responsable, uniquement lorsqu'ils sont médicalement utiles. En Roumanie, les tests génétiques sont autorisés et disponibles dans deux domaines : le domaine médical, pour le diagnostic et la prévention des maladies, et le domaine juridique pour les enquêtes criminelles ou pour établir la paternité.

1109. Demande de ses propres données génétiques : interdite en France. En France, les tests sont strictement réglementés afin de protéger les droits et la vie privée des individus[3282]. Le Code pénal français définit comme un délit « l'examen des données génétiques d'une personne à des fins autres que la recherche médicale ou scientifique ou sans avoir obtenu consentement, lequel doit préciser le motif de l'examen »[3283]. Selon les articles 226-27 et 226-28 du Code Pénal, il est interdit d'identifier clairement, de collecter ou d'utiliser les informations génétiques d'une personne. En outre, l'article 226-28-1 interdit de solliciter ses propres informations génétiques.[3284] Il existe quelques exceptions, des situations dans lesquelles l'analyse génétique est autorisée, qui sont régies par l'article 16-11 du Code Civil.[3285] Actuellement, la loi n° 2003-239[3286] du 18 mars 2003 autorise le prélèvement d'ADN sur les personnes soupçonnées d'avoir commis des infractions (article 55-1 du Code de procédure

[3281] *Ordonnance n° 904/2006 relative à l'approbation des Normes d'application de la Loi n° 95/2006*, Publiée au Journal Officiel de la Roumanie, Partie I, n° 628 du 20 juillet 2006.

[3282] Le Code Pénal - section 6 : Des atteintes à la personne résultant de l'examen de ses caractéristiques génétiques ou de l'identification par ses empreintes génétiques (Articles 226-25 à 226-30). Article 226-28. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042919801.

[3283] F. Ferrand, *Le juge et les techniques biologiques modernes. Section 1re - Introduction de la technique des empreintes génétiques en procédure pénale*. Dalloz, 2013 (actualisation 2024). https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ENCY/PCIV/RUB000108/2013-12/PLAN221.

[3284] Le Code Pénal - Section 6 : Des atteintes à la personne résultant de l'examen de ses caractéristiques génétiques ou de l'identification par ses empreintes génétiques (Articles 226-25 à 226-30). Article 226-28-1. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000024324189.

[3285] Le Code Civil - Chapitre III : De l'examen des caractéristiques génétiques d'une personne et de l'identification d'une personne par ses empreintes génétiques (articles 16-10 à 16-13).

[3286] LOI n° 2003-239 du 18 mars 2003 pour la sécurité intérieure https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000412199/.

pénale)[3287], qui peut être ordonné par le procureur de la République ou par l'officier de police judiciaire (article 76-2 du Code de procédure pénale)[3288].

Les règlements reflètent les préoccupations en matière de bioéthique et de protection des données génétiques sensibles, la Commission Nationale de l'Informatique et des Libertés (CNIL) appelant à la vigilance du public sur le sujet.[3289]

1110. Situations dans lesquelles les tests génétiques sont autorisés. Le cadre juridique français sur les tests génétiques comprend le Code Civil, qui stipule clairement dans quelles conditions les tests génétiques sont autorisés (à des fins médicales et de recherche) et dans quelles conditions ils sont interdits (à des fins commerciales ou récréatives). Il est également possible d'établir la filiation par le biais de tests génétiques, mais uniquement avec l'autorisation d'un tribunal et après signature du consentement des parties concernées.[3290] Dans le Code de la Santé Publique (Chapitre III - Dispositions Pénales - Art. L. 1133-1 - Art. L. 1133-11), les tests génétiques sont strictement réglementés afin de veiller à ce qu'ils soient utilisés uniquement pour le diagnostic, la prévention ou le traitement d'une maladie. Le consentement éclairé est obligatoire et le patient doit être informé de la finalité, de la nature et des conséquences possibles du test[3291]. La Loi de Bioéthique, adoptée en 1994 mais régulièrement révisée et mise à jour, coordonne l'utilisation des tests génétiques, y compris les tests prénataux ou prédictifs de prédispositions génétiques[3292]. La dernière mise à jour date de 2011 et précise notamment que l'examen des données génétiques ne peut être effectué qu'à des fins médicales et judiciaires et ne peut être demandé par un employeur, un assureur ou une banque[3293].

L'analyse de la littérature[3294] permet de conclure qu'en France, les tests génétiques sont autorisés à des fins médicales et de recherche, pour le diagnostic et la prévention des maladies génétiques, avec le consentement éclairé du patient et dans le respect de la protection des participants. Ils peuvent également être utilisés dans le cadre de procédures judiciaires. En

---

[3287] Code de procédure pénale Art. 55,https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CPRP000912.

[3288] Code de procédure pénale - Art. 76-1,https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CPRP001256.

[3289]CNIL, *Tests génétiques sur Internet: la CNIL appelle à la vigilance*, 2024. https://www.cnil.fr/fr/tests-genetiques-sur-internet-la-cnil-appelle-la-vigilance.

[3290] Code Civil (Code Civil Français), art. 16-10, Publié à l'origine en 1804, avec des mises à jour périodiques. Disponible sur le site officiel de Legifrance : www.legifrance.gouv.fr.

[3291] Code de la Santé Publique, Publié à l'origine en 1953, avec des mises à jour régulières. Réglemente les questions de santé publique, y compris les tests génétiques. Disponible sur le site officiel de Legifrance : www.legifrance.gouv.fr.

[3292] Loi n° 2011-814 du 7 juillet 2011 relative à la bioéthique Mise à jour majeure de la législation en matière de bioéthique en France, y compris les réglementations relatives aux tests génétiques. Disponible sur le site officiel de Legifrance : www.legifrance.gouv.fr.

[3293] V. Desgardin-Bourdeau. *Révision des lois de bioéthique : adoption par l'Assemblée nationale du projet de loi*, Dalloz, 2011.https://www-dalloz-fr.docelec.u- bordeaux.fr/documentation/Document?id=ACTU0139705.

[3294] A. Dionisi-Peyrusse, *Actualité de la bioéthique*, AJ fam. 2024. p.180 https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=AJFAM/CHRON/2024/0154.

revanche, leur utilisation à des fins non médicales et commerciales, telles que la détermination du sexe, de l'identité, de l'appartenance, de l'ascendance ou la sélection d'embryons, est strictement interdite[3295].

c). La France et la Suisse, les seuls pays de l'UE à interdire le test ADN de type DTC

1111. La France et la Suisse sont les seuls pays d'Europe où les tests ADN du type DTC (direct-to-customer) ne sont pas autorisés dans leur forme classique, sans contrôle médical.[3296] À partir de 2023, aucun citoyen français ou résident étranger ne pourra commander/recevoir un test ADN de ce type. Ces types de tests sont délivrés dans toute l'Union Européenne, à l'exception de la France[3297].

Comment l'expliquer ? D'une part, la loi française n'a pas changé depuis 1994. D'autre part, le décryptage de la séquence complète de l'ADN du génome humain (projet lancé fin 1988) a été finalisé en 2003.[3298] Six ans plus tard sont apparus les premiers laboratoires de génétique qui proposent ce type test en ligne, directement au consommateur et sur demande. Comme présenté ci-dessus, l'Article 16-10 du Code Civil français[3299] réglemente la réalisation des tests ADN en France. Toutefois, cet article a été rédigé en 1994, bien avant la création du premier test ADN DTC. Par conséquent, l'article ne fait manifestement référence qu'aux tests existant à l'époque : médicaux, médico-légaux et scientifiques. Ainsi, l'avis d'un médecin est nécessaire pour un test génétique. De plus, seul un juge peut approuver un test de paternité[3300].

1112. Tests ADN utilisés en France, bien qu'illégaux. Bien qu'illégaux, plus de 20.000 tests ADN DTC, disponibles sur internet, ont été commandés en France en 2009[3301]. Les Français, de plus en plus intéressés par ce type de tests, confient leurs données génétiques à des laboratoires étrangers. Invité à clarifier la situation, le procureur général de la Cour de Cassation a souligné l'impossibilité de l'éradication, suggérant que ces tests devraient être placés sous la

---

[3295] Le site du Conseil d'État de France, *Informations sur la législation et la jurisprudence françaises en matière de santé publique et de bioéthique.* Disponible à l'adresse : www.conseil-etat.fr.
[3296] Article 226-28-1 du Code Pénal.
[3297] *Tests ADN sur Internet : est-ce légal ? Quels sont les risques ?* Centre Européen des Consommateurs France 2023 https://www.europe-consommateurs.eu/achats-internet/test-adn-sur-internet.html.
[3298] Voir la déclaration officielle du Consortium International du Génome Humain du 14 avril 2003, disponible en ligne à l'adresse suivante : https://www.genome.gov/11006929/2003-release-international-consortium- completes-hgp/.
[3299] Le code Civil. Chapitre III : De l'examen des caractéristiques génétiques d'une personne et de l'identification d'une personne par ses empreintes génétiques (articles 16-10 à 16-13).
[3300] C. Labruse-Riou *Filiation : généralités - Notion de filiation*, 2009 (actualisation 2023) https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ENCY/CIV/RUB000133/2009-09/PLAN026.
[3301] S. Lavric, *Tests ADN illégaux: quelles solutions ?,* Dalloz 2010 https://www.dalloz-actualite.fr/depeche/tests-adn-illegaux-quelles-solutions.

base légale plutôt qu'interdits[3302]. Comme prévu, cette déclaration a été sévèrement critiquée par l'opinion publique, des comparaisons étant faites avec l'usage du cannabis, qui est également interdit mais pratiqué dans tout le pays. En outre, certains ont rappelé le scepticisme de l'essayiste français Charles Peguy à l'égard de la philosophie morale de Kant[3303].

1113. Nécessité d'une révision législative. Dans ce contexte, en 2019, la Commission de Bioéthique propose de réviser et d'actualiser la loi de bioéthique, en appelant à la réglementation des tests ADN généalogiques, récréatifs et de paternité.[3304] Le raisonnement est basé sur la disponibilité et la légalité de ces tests dans toute l'Europe, ainsi que sur l'évolution de la médecine et de la société en général, offrant de nouvelles opportunités à la population. Les partisans des tests ADN craignent également que par ces interdictions la France reste derrière l'évolution technologique.[3305] Dans l'Assemblée Générale de 2020 sur l'analyse et la régulation des lois de bioéthique, le Gouvernement de la République s'oppose avec véhémence à la légalisation des tests génétiques.[3306]

Une première préoccupation concerne la vie privée des personnes qui ont recours à ces tests et les abus qui peuvent être commis[3307]. En ce qui concerne les tests de filiation (paternité, généalogie, ascendance), le ministre de la santé estime que la question est sensible, notamment dans le cas des enfants nés d'un don de gamètes, car ces dons sont souvent effectués sous la protection de l'anonymat, et la vie privée des personnes concernées peut être profondément affectée par le recours excessif à ces tests (article 10 bis).

1114. Prévention de l'eugénisme. Il existe également un risque de dérive eugénique[3308] si l'accès à la pléthore de tests génétiques existants[3309] est réglementé. Une dernière révision de la loi de Bioéthique a eu lieu en 2021, et bien qu'elle n'aborde pas directement la légalisation des tests ADN DTC, on apporte certaines validations dans le domaine de la recherche, dans le but

---

[3302] Séance du 28 janvier 2020, Comptes rendus intégraux de janvier 2020, le Sénat français https://www.senat.fr/seances/s202001/s20200128/s20200128003.html.

[3303] C. Péguy, *Charles Péguy*. édité par A. Cavazzini et J. Soskin, Presses universitaires Liège, 2016, https://doi.org/10.4000/books.pulg.7098.

[3304] Conseil d'État, section du rapport et des études. *Révision de la loi de bioéthique : quelles options pour demain ?*, Étude à la demande du Premier ministre, 2018 https://www.dalloz-actualite.fr/sites/dalloz-actualite.fr/files/resources/2018/07/07/conseil_detat_sre_etude_pm_bioethique.pdf.

[3305] *Comptes rendus analytiques officiels du 28 janvier 2020*, le Sénat français https://www.senat.fr/cra/s20200128/s20200128_5.html#par_147.

[3306] *Pourquoi la France maintient l'interdiction des tests de généalogie génétique,* DNA Pass. https://dna-pass.com/pourquoi-la-france-maintient-linterdiction-des-tests-de-genealogie-genetique/.

[3307] Inquiétude renforcée par l'incident de la base de données 23andMe décrit ci-dessus.

[3308] D. Smadja, *Les tests génétiques peuvent-ils conduire à l'eugénisme ?,* texte extrait de La Lettre de l'Espace éthique HS n°2, *Les tests génétique : grandeur et servitude*, p 45, Asistance Publique - Hopitaux de Paris, 2003.

[3309] P. Levine, A. Bashford. *Introduction: Eugenics and the Modern World*, Oxford University Press, 2010 https://joelvelasco.net/teaching/3330/levine_and_bashford12-history_eugenics.pdf.

de soutenir l'innovation tout en respectant la ligne éthique et le droit à la vie privée de l'individu[3310].

En conclusion, avec un gouvernement extrêmement prudent[3311] et considérant que les tests ADN favorisent la discrimination et peuvent induire panique et confusion chez les consommateurs, la loi française ne les autorise que sur recommandation médicale ou à des fins de recherche scientifique et, d'un point de vue judiciaire, un tel test ne peut être effectué qu'avec l'approbation d'un juge[3312] [3313].

Section 2**. IDENTIFICATION D'UNE PERSONNE SUR LA BASE DES EMPREINTES GÉNÉTIQUES**

1115. Identification par test ADN. Aujourd'hui, la technologie de l'ADN révolutionne le domaine de la médecine légale[3314], représentant la méthode la plus sûre, la plus rapide et la plus précise pour identifier une personne[3315]. La science devient ainsi un arbitre important dans les dilemmes des affaires judiciaires, mais cette interaction entre la science et la justice peut créer des tensions éthiques et juridiques[3316].

La Cour Européenne des Droits de l'Homme (CEDH) a rendu des décisions exigeant des États membres, y compris la France, qu'ils respectent les droits fondamentaux en ce qui concerne la conservation et l'utilisation des échantillons d'ADN[3317].

§1. FICHIER NATIONAL DES EMPREINTES GÉNÉTIQUES

[3310] Conseil constitutionnel. 29 juillet 2021/n°2021-821 https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CONSCONST_LIEUVIDE_2021-07-29_2021821.

[3311] Loi bioéthique : le gouvernement avance avec précaution - Jean-Marc Pastor - 26 juillet 2019 https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ACTU0196914.

[3312] Rapport fait au nom de la commission spéciale (1) sur le projet de loi, adopté par l'Assemblée nationale, relatif à la bioéthique https://www.senat.fr/rap/l19-237/l19-2371.pdf.

[3313]*Comptes rendus analytiques officiels du 28 janvier 2020,* le Sénat français https://www.senat.fr/cra/s20200128/s20200128_5.html#par_147.

[3314] D. Uberoi, N. Palmour, Y. Joly. *The advent of forensic DNA databases: It's time to agree on some international governance principles!* Forensic Science International: Genetics, Volume 72, 2024, https://doi.org/10.1016/j.fsigen.2024.103095.

[3315] Y. Cherifi, S. Amrani, *Analyses ADN en médecine-légale: revue générale et perspectives,* 1er congrès national „Les conduites médico-légales en anatomopathologie et anthropologie", Algérie, 2018 https://www.researchgate.net/publication/324703143_Analyses_ADN_en_medecine-legale_general_review_and_perspectives.

[3316] R. Bertrand. *Ce que l'ADN fait faire à la justice : sociologie des traductions dans l'identification par analyse génétique en justice pénale* (Doctorat en criminologie), UCL, 2008. *http://hdl.handle.net/2078.1/158063 http://hdl.handle.net/2078.1/158063.*

[3317] Jurisprudence de la Cour Européenne des Droits de l'Homme (CEDH) - Décisions pertinentes de la CEDH sur la protection des données personnelles et les droits fondamentaux. Disponible sur le site officiel de la CEDH : www.echr.coe.int.

1116. Conservation des données génétiques par les autorités. La police peut conserver dans le fichier national des empreintes génétiques[3318] l'ADN des condamnés et des personnes faisant l'objet de poursuites pénales[3319], ce droit étant soumis à des règles strictes[3320] tout en respectant les droits de l'homme. Depuis la création de la première base de données de ce type en 1995 au Royaume-Uni, le nombre de pays disposant de bases de données génétiques étatiques n'a cessé de croître de manière exponentielle[3321]. En 2020, les registres du Fichier Automatisé des Empreintes Génétiques (FNAEG) comprenaient environ 5 millions de personnes, soit plus de 7% de la population française. À cela s'ajoutent plus de 700.000 prélèvements effectués sur les scènes de crime et sur les corps d'inconnus auxquels aucune identité n'a été attribuée.[3322] Face à l'utilisation croissante et à l'importance des données ADN dans les enquêtes criminelles[3323], le FNAEG a été créé en France en 1998 et, dans un premier temps, les données génétiques personnes condamnées pour des infractions à caractère sexuel pouvaient être enregistrées dans ce fichier. Par la suite, la loi n° 2001-1062 du 15 novembre 2001[3324], dans son article 706-47, a étendu et défini clairement l'ensemble des infractions couvertes, des extensions successives ayant été ajoutées au fil des années[3325].

Dans le Code de Procédure Pénale, les articles 706-54, 706-55 et 706-56[3326] régissent les modalités selon lesquelles les autorités policières et judiciaires peuvent recueillir et conserver des échantillons d'ADN dans le FNAEG. À l'heure actuelle, le champ des infractions couvertes par le FNAEG est extrêmement large, puisqu'il englobe la quasi-totalité des

---

[3318] C.F. Schuhl, *Praxis Cyberdroit Chapitre 133 – Données biométriques*, 2020-2021. https://www- dalloz-en.docelec.u-bordeaux.fr/documentation/Document?id=DZ/PRAXIS/CYBERDROIT/2019/L01-T13-C133/PLAN/0006.

[3319] Répertoire de droit pénal et de procédure pénale, Chapitre 2, Section 3, Article 1 - 2. *Fichier national des empreintes génétiques* https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ENCY/PEN/RUB000255/2020-10/PLAN/0058

[3320] Répertoire de droit pénal et de procédure pénal, Chapitre 2, Section 3, Article 1 - 2. Fichier national des empreintes génétiques https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ENCY/PEN/RUB000255/2020-10/PLAN/0058.

[3321] A. Ray, Wickenheiser. *Expanding DNA database effectiveness*, Forensic Science International: Synergy, Volume 4, 2022, https://doi.org/10.1016/j.fsisyn.2022.100226.

[3322] J.-M. Manach, *Plus d'un tiers des Français sont fichés au FNAEG*, Next Inpact, 2021.

[3323] J. Vailly, *Sur la trace des suspects. L'incorporation de la preuve et de l'indice à l'ère de la génétique*, Paris, Editions de la Maison des sciences de l'homme, 2021. https://www.researchgate.net/publication/344100063_Vailly_J_Dir_2021_Sur_la_trace_des_suspects_L'incorporation_de_la_preuve_et_de_l__indice_a_l'ere_de_la_genetique_Paris_Editions_de_la_Maison_des_sciences_de_l'homme_248_p.

[3324]LOI n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000000222052.

[3325] *Rapport d'information déposé en application de l'article 146 du Règlement*, par la Commission des Finances, de L'économie général et du plan sur le fichier, Assemblée nationale, 2002. https://www.assemblee-nationale.fr/12/pdf/rap-info/i0504.pdf.

[3326] Code de procédure pénale, Titre XX : *Du fichier national automatisé des empreintes génétiques (Articles 706-54 à 706-56-1-1)* https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000006138132/#LEGISCTA000006138132.

infractions pénales françaises, à l'exception de certaines infractions financières[3327]. En outre, la loi du 18 mars 2003 a considérablement alourdi les sanctions en cas de refus, avec une peine pouvant aller jusqu'à trois ans d'emprisonnement et 45.000 euros d'amende[3328]. Les profils ADN peuvent être conservés pendant des périodes déterminées, qui varient en fonction de la nature de l'infraction et de la décision des autorités judiciaires. En général, pour les infractions graves, les données peuvent être conservées jusqu'à 40 ans. Les personnes dont les profils ADN ont été stockés dans le FNAEG ont le droit de demander leur suppression si elles sont acquittées ou s'il n'y a plus de motifs légaux de conserver les données[3329], des autorités telles que la CNIL aidant à entamer ce processus[3330]. Bien entendu, les échantillons d'ADN sont considérés comme des données à caractère personnel, de sorte que leur conservation et leur utilisation doivent être effectuées conformément au règlement GDPR[3331].

A. Du stockage des données ADN pour les crimes les plus graves jusqu'aux délits mineurs

1117. Abus liés au stockage des données génétiques. La principale préoccupation concernant le FNAEG[3332] (Fichier National Automatisé des Empreintes Génétiques) a été le risque d'abus. À l'origine, le FNAEG stockait les empreintes génétiques des délinquants accusés d'infractions graves telles que le viol ou le meurtre. Au fil du temps, il s'est progressivement étendu aux profils génétiques de personnes accusées d'infractions mineures ou même de personnes acquittées par la suite[3333], mais il n'a pas réglementé la manière dont ces données génétiques peuvent être supprimées[3334]. Il ne différencie pas non plus la durée de conservation

---

[3327] V. Rabeharisoa, F. Paterson, *Matérialité et juridicité. À propos du Fichier national automatisé des empreintes génétiques*. Droit et société*, no 110,* 2022. p.21-36. URL : https://droit.cairn.info/revue-droit-et-societe-2022-1-page-21?lang=fr.

[3328] V. Dyevre, *Génétique et enquêtes policières*, Les Tribunes de la santé, *n° 17,* 2007. URL : https://shs-cairn-info.docelec.u-bordeaux.fr/revue-les-tribunes-de-la-sante1-2007-4-page-79?lang=fr.

[3329] Code de procédure pénale, *titre XX : Du fichier national automatisé des empreintes génétiques et du service central de préservation des prélèvements biologiques (Articles R53-9 à R53-21).*

[3330] CNIL, *Le droit à l'effacement: supprimer vos données en ligne***,** *2018 https://www.cnil.fr/fr/comprendre-mes-droits/le-droit-leffacement-supprimer-vos-donnees-en-ligne.*

[3331] *Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (Règlement Général sur la Protection des Données - RGPD),* Publié au Journal Officiel de l'Union Européenne, L 119, le 4 mai 2016, ce règlement est également applicable en France et régit la protection des données génétiques. Disponible sur le site officiel EUR-lex : www.eur-lex.europa.eu.

[3332] Le FNAEG est le deuxième plus gros fichier européen après le fichier britannique, avec près de 3 millions de profils enregistrés (traces et individus). 73% des profils qui y sont enregistrés sont ceux d'individus « suspects ».

[3333] V. Rabeharisoa, F. Paterson. *«* Maintenir une infrastructure en droit : le rôle du comité technique du Fichier national automatisé des empreintes génétiques *»,* in *Sur la trace des suspects*, Éditions de la Maison des sciences de l'homme, 2021. https://doi.org/10.4000/books.editionsmsh.30058.

[3334] L. Burgorgue-Larsen. *Actualité de la convention européenne des droits de l'homme,* AJDA, 2012. https://www.dalloz.fr/lien?famille=revues&dochype=AJDA%2FCHRON%2F2017%2F2430.

des données en fonction de la nature ou de la gravité de l'infraction[3335]. En outre, les personnes qui refusent les prélèvements d'ADN sont sévèrement sanctionnées conformément aux lois susmentionnées. Il est considéré que le fichier a été utilisé de manière excessive, bien au-delà de l'objectif initial pour lequel il a été créé, à savoir assurer un équilibre entre le respect de la vie privée et la protection de l'ordre public[3336].

G. Béranger souligne dans sa déclaration l'importance de l'équilibre entre la sécurité et les droits de l'homme : « Il doit demeurer un rapport de proportionnalité étroit entre le degré d'atteinte à la vie privée, d'une part, et l'efficacité du fichier au regard de l'objectif poursuivi ainsi que les garanties dont il est assorti, d'autre part ».[3337]

1118. Le stockage des données génétiques, sujet de critique en France. Dans ce contexte, la France a été critiquée par l'Union Européenne[3338] et des organismes internationaux, avec des préoccupations principalement liées à la violation de l'article 8 de la Convention Européenne des Droits de l'Homme[3339].

L'affaire Aycaguer vs. France[3340], rendue le 22 juin 2017, constitue un exemple probant de la nécessité des changements et des réglementations énoncés ci-dessus. La CEDH a condamné la France pour violation du droit au respect de la vie privée garanti par l'Article 8 de la Convention Européenne des Droits de l'Homme. M. Pierre-François Aycaguer, citoyen français, contestait l'obligation de relever et de conserver ses empreintes génétiques dans le fichier FNAEG après avoir été condamné pour une infraction mineure (son infraction était liée à un conflit social). Il a refusé de se soumettre à cette procédure, raison pour laquelle il a été enquêté et condamné.[3341] La CEDH a estimé que la conservation systématique des données génétiques de toutes les personnes condamnées ou suspectées, quelle que soit la gravité de l'infraction, était disproportionnée et a décidé que cette pratique constituait une violation du

---

[3335] A. Baudelin, *Chronique pénale du prélèvement d'ADN et du fichier national automatisé des empreintes génétiques (FNAEG)*. https://baudelinavocat.fr/chronique-penale-du-prelevement-adn-et-du-fichier-national-automatise-des-empreintes-genetiques-fnaeg/.

[3336] É. Assassi et plusieurs de ses collègues, *Fichage - Propositions de loi Texte n° 367 (2013-2014)*, déposé au Sénat le 12 février 2014, https://www.senat.fr/leg/ppl13-367.html.

[3337] E. Supiot, *Empreintes génétiques et droit pénal Quelques aspects éthiques et juridiques*, Revue de science criminelle et de droit pénal comparé, *N°4,* 2015. p.827-835. https://droit.cairn.info/revue-de-science-criminelle-et-de-droit-penal-compare-2015-4-page-827?lang=fr.

[3338] *FNAEG: la chambre criminelle sourcilleuse quant à la portée des arrêts de condamnation de la CEDH.* Dalloz 2019 https://actu.dalloz-etudiant.fr/a-la-une/article/fnaeg-la-chambre-criminelle-sourcilleuse-quant-a-la- portee-des-arrets-de-condamnation-de-la-ced/h/5a4777fa387795250a94cda76b64108e.html.

[3339] M. Léna, *Conservation des empreintes génétiques en cas d'acquittement ou de classement sans suite*, Dalloz, 2008 https://www.dalloz-actualite.fr/essentiel/conservation-des-empreintes-genetiques-en-cas-d- acquittement-ou-de-classement-sans-suite#results_box.

[3340] *Aycaguer vs. France* - 8806/12 Judgment du 22.6.2017 [Section V].

[3341] Code de procédure pénale, art. 706-56. https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CODE_CPRP_ARTI_706-56&scrll=CPRP020980&FromId=AJPEN_JURIS_.

droit au respect de la vie privée du requérant, considérant que le droit français ne prévoyait pas de garanties suffisantes pour protéger ce droit, en particulier dans le cas d'infractions mineures. En outre, la Cour a souligné que certains changements étaient nécessaires dans la législation sur le FNAEG, tels que la possibilité d'effacer les données même dans le cas des personnes condamnées ou la réglementation de la durée de conservation en fonction de la gravité de l'infraction. Par conséquent, la France a été obligée de payer à M. Aycaguer des dommages-intérêts pour préjudice moral d'un montant de 3.000 euros et des frais de justice d'un montant de 7.000 euros (55)[3342] [3343] ;

a). Suppression de données génétiques

1119. Refus de suppression des données génétiques. D'autre part, les partisans de la loi affirment que la collecte d'échantillons génétiques ne porte pas atteinte au respect de la vie privée, car il est possible de demander leur suppression[3344].

La garantie d'obtenir l'effacement a toutefois un effet limité lorsque les autorités refusent, en réponse à une demande de la personne visée, d'effacer les données en question ou de motiver leur décision de les conserver. L'affaire M.K. vs. France en est un exemple. Le citoyen MK, impliqué dans une affaire de vol de livres, a par la suite demandé l'effacement des données du fichier automatisé des empreintes génétiques. Sa demande ayant été refusée, il a accusé les autorités françaises de violer son droit à la vie privée. L'affaire a été portée devant la CEDH, qui a conclu à une violation de l'Article 8 de la Convention des Droits de l'Homme en raison de l'absence de garanties concernant la collecte, la conservation et l'effacement des données génétiques des personnes soupçonnées d'avoir commis des infractions. Cette affaire a un impact, notamment en raison de la nature de l'infraction, et ne peut être comparée à des infractions graves telles que la criminalité organisée ou les agressions sexuelles, pour lesquelles il est nécessaire et extrêmement utile de conserver de telles données.[3345] [3346]

1120. Durée de conservation proportionnelle à la gravité de l'infraction. Bien entendu, ces situations ont aussi leur revers de la médaille, de nombreux criminels utilisant ce précédent. Dans l'affaire DAGREGORIO AND MOSCONI vs. FRANCE[3347], les deux hommes

---

[3342] Le fichier des empreintes génétiques condamné par la Cour européenne des droits de l'homme, 2017 / n° 8806/12 / n°. 8806/12. https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=CEDH_LIEUVIDE_2017-06-22_880612.

[3343] Council de L,Europe. *Case law of the European court of human rights concerning the protection of personal data,* pag 277, 2018. https://rm.coe.int/t-pd-2018-15-case-law-on-data-protection-may2018- fr/16808b2d36.

[3344] M. Recotillet. *FNAEG(refus du prélèvement): respect au droit à la vie privée,* Dalloz, 2019 https://www.dalloz-actualite.fr/flash/fnaeg-refus-du-prelevement-respect-au-droit-vie-privee.

[3345] *Case of M.K. v. France, application n° 19522/09. https://hudoc.echr.coe.int/eng#{"itemid" :["001- 119075"]}.*

[3346] *Conservation des empreintes digitales: atteinte au respect de la vie privée,* Dalloz.fr, *2013.* https://www-dalloz-fr.docelec.u- bordeaux.fr/documentation/Document?id=CEDH_LIEUVIDE_2013-04-18_1952209.

[3347] *Félix Dagregorio et Alain Mosconi contre la France, Requête no 65714/11.*

condamnés pour enlèvement et séquestration de personnes, occupation et blocage d'un navire de la SNMC ont refusé d'introduire leurs données génétiques personnelles dans le fichier national (FNAEG), ce qui leur a valu d'être jugés et condamnés pénalement. En relation avec cette condamnation, ils ont allégué une violation de leur droit à la vie privée et à l'intégrité physique. Mais la Cour Européenne des Droits de l'Homme a déclaré à l'unanimité la requête irrecevable[3348].

Dans les affaires B.B. contre la France, 2009, point 68[3349], Gardel contre la France, 2009, point 69[3350] et M.B. contre la France, 2009, point 60[3351], la Cour a estimé que les règles de l'Article 8 sur le droit au respect de la vie privée ont été respectées et que la durée de conservation des données est proportionnée à l'infraction commise et au but poursuivi (prévention de l'infraction).

1121. Incompatibilités entre le respect de la vie privée et le stockage des données génétiques. Sur la base de l'arrêt de la CEDH dans l'affaire Aycaguer vs. France, d'autres décisions similaires ont été prises dans la République. Par exemple, dans le cas d'un individu poursuivi pour violences graves et refus de se soumettre à un prélèvement d'ADN, la Cour d'Appel a estimé que les poursuites pour l'infraction visée à l'article 706-56, II, du Code de procédure pénale étaient contraires à l'article 8 de la Convention Européenne des Droits de l'Homme, et a acquitté le défendeur[3352].

Des voix s'élèvent également dans la République pour souligner l'incompatibilité entre la collecte et le stockage de données dans le FNAEG[3353] et le droit à la vie privée granti par l'article 8 de la Convention Européenne des Droits de l'Homme, en faisant valoir la nécessité de conséquences normatives, soit en réglementant la suppression de ces données, soit en limitant le champ d'application.[3354]

B. Durée de conservation des données génétiques, selon la nature de l'infraction

https://hudoc.echr.coe.int/eng#{"display":[2],"tabview":["related"],"itemid":["001-175036"]}.

[3348] E. Autier. *CEDH: absence de précédent jurisprudentiel et épuisement des voies de recours internes,* Dalloz, 2017. https://www.dalloz-actualite.fr/flash/cedh-absence-de-precedent-jurisprudentiel-et-epuisement-des-recours interne.

[3349] *Affaire B.B. c. France,* requête n° 5335/06. https://hudoc.echr.coe.int/fre#{"itemid" :["001-96361"]}.

[3350] *Affaire Gardel c. France* – requête no 16428/05. https://hudoc.echr.coe.int/eng#{"itemid" :["002-1198"]}.

[3351] *Affaire M.B. c. France,* requête n° 22115/06. *https://hudoc.echr.coe.int/fre#{"itemid" :["001-96363"]}.*

[3352] M. Recotillet. *FNAEG (refus du prélèvement): respect au droit à la vie privée*, Dalloz 2019. https://www.dalloz-actualite.fr/flash/fnaeg-refus-du-prelevement-respect-au-droit-vie-privee.

[3353] C.Girault, *Identification et identité génétiques*, AJ pénal 2010. p.224 https://www.dalloz.fr/lien?famille=revues&dochype=AJPEN%2FCHRON%2F2010%2F0042.

[3354] J.P. Marguénaud, D. Roets, *Droits de l'Homme. Jurisprudence de la CEDH*. Revue de science criminelle et de droit pénal comparé, n° 1, art 8, 2015. https://droit-cairn-info.docelec.u-bordeaux.fr/revue-de-science-criminelle-et-de- droit-penal-compare-2015-1-page-1-155?lang=fr.

1122. La FNAEG devant la Cour constitutionnelle. Face aux multiples plaintes concernant la violation des droits fondamentaux par la conservation des informations génétiques, le FNAEG a été soumis à l'examen du Conseil Constitutionnel[3355]. Le Conseil Constitutionnel constate que le fichier national des empreintes génétiques est un moyen efficace d'identifier les auteurs de certaines infractions et le déclare conforme à la Constitution, mais sous réserve de deux observations. La première concerne la durée de conservation des informations, qui doit tenir compte de la gravité de l'infraction et de la finalité de la conservation. La seconde concerne le droit de contestation effectif, si les personnes concernées estiment que la collecte de ces données n'est pas justifiée[3356].

1123. Demande de suppression de ses propres données génétiques. À la suite de ces critiques, la France prend des mesures. S'appuyant sur l'arrêt de la CEDH dans l'affaire Aycaguer, a modifié les articles du Code Pénal relatifs au Fichier National Automatisé des Empreintes Génétiques. En 2019, elle a introduit la disposition permettant aux personnes condamnées demander l'effacement anticipé de leurs données du FNAEG. En 2021, elle réglemente les durées de conservation des données en fonction de la gravité de l'infraction et du fait que la personne est majeure ou mineure[3357]. Des durées de conservation longues, pouvant aller jusqu'à 40 ans, s'appliquent en cas d'infractions graves ou d'actes de terrorisme. En réglementant la possibilité d'effacement, les nouveaux amendements ont élargi la catégorie de personnes dont les données génétiques peuvent être conservées : les amendements permettent la conservation des données génétiques des personnes condamnées ainsi que des suspects ou des personnes impliquées dans des enquêtes[3358]. En outre, la France a facilité l'échange de données génétiques entre le FNAEG et d'autres bases de données internationales des États membres de l'UE, assurant ainsi une meilleure coopération dans le but commun de lutter contre le terrorisme et la criminalité transfrontalière. Elle a également détaillé les conditions de conservation des données et les modalités d'accès à celles-ci, dans le respect des règles de protection et des droits fondamentaux[3359].

[3355] Décisions du Conseil constitutionnel du 1er juillet 2010 au 30 septembre 2010. *Les Nouveaux Cahiers du Conseil constitutionnel, n° 30,* 2011.p.97-168. https://shs-cairn- info.docelec.u-bordeaux.fr/revue-nouveaux-cahiers-conseil-constitutionnel-2011-1-page-97?lang=fr.

[3356] M. Léna. *Cons. const. 16 sept. 2010, n° 2010-25 QPC*, D. actu., 2010. https://www-dalloz- fr.docelec.u-bordeaux.fr/documentation/Document?id=CONSCONST_LIEUVIDE_2010-09-16_201025.

[3357] Department for the Execution of Judgment of the European Court of Human Rights. *France reinforces the guarantees around the FNAEG, 2022.* https://www.coe.int/el/web/execution/-/france-reinforces-the-guarantees-around-the-fnaeg-national-automated-genetic-fingerprints-database-.

[3358] Délibération n° 2021-009 du 7 janvier 2021 portant avis sur un projet de décret relatif au traitement de données à caractère personnel dénommé « Fichier national automatisé des empreintes génétiques » et modifiant les dispositions du code de procédure pénale (demande d'avis n° 19017520) https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044272373.

[3359] Délibération n° 2021-009 du 7 janvier 2021 portant avis sur un projet de décret relatif au traitement de données à caractère personnel dénommé « Fichier national automatisé des empreintes génétiques » et modifiant les

1124. FNAEG conforme à la CEDH. Le 8 décembre 2021, la Cour de Cassation (décision n° 20-84.201) décide que le Fichier National Automatisé des Empreintes Génétiques (FNAEG) est conforme à l'Art. 8 de la Convention Européenne des Droits de l'Homme. Bien que portant atteinte à la vie privée, la collecte et la conservation de ces données sont justifiées aux fins de prévention et de recherche d'infractions graves[3360].

Avec ces modifications et ajouts à la législation, la France a largement satisfait les obligations réglementaires découlant de la pratique de la Cour Européenne des Droits de l'Homme[3361].

a). Adaptation législative

1125. Alignement du FNAEG sur les exigences de la CEDH. Aujourd'hui, la conventionnalité et la constitutionnalité du FNAEG sont bien stabilisées et perfectionnées, les fichiers ne constituent plus une atteinte à la vie privée, dans le respect des droits fondamentaux tels que stipulés à l'article 8 de la CEDH[3362], et donc ne font plus l'objet de critiques.[3363]

Considérons ici l'arrêt n° 23-84.520 rendu par la Cour de Cassation le 4 avril 2024[3364], concernant M.E. qui, renvoyé en jugement pour le délit de menace d'incendie d'une rédaction d'un journal, refuse le prélèvement de ses données biométriques lors de son arrestation. En l'espèce, la Cour considère que l'infraction en question est suffisamment grave pour permettre le prélèvement d'échantillons génétiques et rejette le pourvoi[3365].

1126. Base de données génétiques européenne. Par ailleurs, à l'instar de la base FNAEG, la Commission Européenne a proposé en 2008, dans le prolongement du traité de Prüm[3366], la

dispositions du code de procédure pénale (demande avis no. 19017520) https://www.legifrance.gouv.fr/download/pdf?id=Ng9i2KEYFB_uOM29YFJd_a-9m5qJfR8SKEUQrqs-CMQ=.

[3360] Cour de cassation, Pourvoi n° 20-84.201, 2021. https://www.courdecassation.fr/decision/61b058eddc637ddd76c35e61.

[3361] Résolution CM/ResDH(2022)84-Execution of the judgment of the European Court of Human Rights Aycaguer against France. (Adopted by the Committee of Ministers on 6 April 2022 at the 1431st meeting of the Ministers' Deputies) *https://hudoc.exec.coe.int/ENG#{"execidentifier" :["001-2169.*

[3362] D. Pamart, *FAED et FNAEG à l'épreuve du droit de l'Union*, Dalloz, 2024. *https://www.dalloz-actualite.fr/flash/faed-et-fnaeg-l-epreuve-du-droit-de-l-union*,

[3363] *Précisions sur la nécessité des collectes de données biométriques et génétiques* - Cour de cassation, crim. 4 avril 2024 – AJ pénal 2024. 331 https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=AJPEN/JURIS/2024/0105.

[3364] Cour de cassation, criminelle, Chambre criminelle, 4 avril 2024, 23-84.520, Publié au bulletin https://www.legifrance.gouv.fr/juri/id/JURITEXT000049385467.

[3365] *Précisions sur la nécessité des collectes de données biométriques et génétiques* - Cour de cassation, crim. 4 avril 2024 – AJ pénal 2024. 331 https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=AJPEN/JURIS/2024/0105.

[3366] Le traité de Prüm a été signé par 7 États européens le 27 mai 2005 : l'Espagne, la Belgique, les Pays-Bas, le Luxembourg, l'Allemagne, la France et l'Autriche ; d'autres pays ont adhéré ultérieurement à ce traité: Bulgarie, Roumanie, Slovénie, Finlande, Hongrie, Estonie, Slovaquie. https://www-dalloz-fr.docelec.u-

création d'une base de données européenne d'empreintes digitales de condamnés ou même de suspects. L'objectif est de « faciliter l'échange d'informations entre les services répressifs » et la lutte « contre la criminalité organisée et le terrorisme »[3367].

Les débats sur ce sujet se poursuivent, d'autant que la Cour de Justice de l'Union Européenne remet sur le devant de la scène, début 2023, la discussion sur la protection des droits fondamentaux, le respect de la vie privée et la protection des données à caractère personnel dans le cadre de la collecte des données biométriques et génétiques des personnes mises en cause, affaires relevant du champ d'application de la Directive (UE) 2016/680 du 27 avril 2016.[3368] Des mises en garde contre les abus sont également soulevées, la Cour estimant que ces collectes doivent être justifiées, sur la base d'une évaluation individuelle de chaque cas, respectant ainsi l'équilibre entre les libertés fondamentales et la garantie d'une justice équitable[3369].

b). Stockage des données génétiques en Roumanie

1127. Utilisation des données ADN en Roumanie. En Roumanie, les empreintes génétiques sont une technique d'identification des personnes utilisée dans le cadre de la recherche scientifique, de la justice et de la sécurité publique[3370].

L'article 65 du Code Civil stipule que l'examen des caractéristiques génétiques d'une personne ne peut être entrepris qu'à des fins médicales ou de recherche scientifique, dans le respect de la loi, et que l'identification d'une personne sur la base de ses empreintes génétiques ne peut être effectuée que dans le cadre d'une procédure judiciaire civile ou pénale[3371].

Le Code de procédure pénale roumain fait référence aux empreintes génétiques, mais pas directement sous cette rubrique, mais dans le contexte du prélèvement d'échantillons

---

bordeaux.fr/documentation/Document?ctxt=0_YSR0MD10cmFpdMOpIGRlIFByw7xtwqd4JHNmPXNpbXBsZS1zZW, Art2, (95-96).

[3367] C. Féral-Schuhl. *Praxis Cyberdroit - Chapitre 133 - Données biométriques, § 6 - Création d'une base de données européenne d'empreintes digitales des condamnés*, Dalloz.fr, 2020-2021. https://www-dalloz-en.docelec.u-bordeaux.fr/documentation/Document?id=DZ/PRAXIS/CYBERDROIT/2019/L01-T13-C133/PLAN/0011.

[3368] Directive (UE) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and of the free movement of such data, and repealing Council Framework Decision 2008/977/JAI https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680.

[3369] C. Crichton, *Inconventionnalité de la collecte systématique de données biométriques d'un mis en examen : quelles conséquences sur le droit français?,* Dalloz, 2023 https://www.dalloz-actualite.fr/flash/inconventionnalite-de-collecte-systematique-de-donnees-biometriques-d-un-mis-en-examen-quelles.

[3370] R. Potorac. *Genetică judiciară*, Centrul Tehnic-Editorial al Armatei, 2005.

[3371] Code Civil de Roumanie – Art. 65. Examen caractéristiques génétique https://www.codulcivil.ro/category/textul-integral/.

biologiques et des analyses d'ADN, en vertu de l'Article 190, qui réglemente les conditions de collecte, d'utilisation et de conservation de ces échantillons.[3372] En outre, l'article 191 réglemente l'expertise génétique médico-légale[3373].

1128. Modalités de stockage des données ADN : SNDGJ. Ces données génétiques (ADN) sont stockées dans une base de données appelée **Système National de Données Génétiques Judiciaires** (SNDGJ), qui est réglementée par la Loi n° 76/2008, mise à jour en 2024, qui établit les conditions dans lesquelles des échantillons biologiques peuvent être prélevés afin de déterminer le profil génétique, ainsi que les conditions dans lesquelles les données contenues dans le S.N.D.G.J. peuvent être traitées.[3374] En conclusion, le système comprend les profils génétiques des condamnés, des suspects, des corps dont l'identité est inconnue, des traces biologiques prélevées sur les lieux d'une infraction. L'objectif est de prévenir et de combattre les infractions graves qui portent atteinte au droit à la vie et à l'intégrité physique et psychique.[3375] Des améliorations et des précisions ont été apportées à la loi, notamment en ce qui concerne les personnes sur lesquelles ces échantillons biologiques peuvent être prélevés.[3376]

c). Durée de conservation des données génétiques en Roumanie

1129. Comme en France, en Roumanie, la durée de conservation des empreintes digitales dépend du statut juridique de la personne, et elles peuvent être effacées si elles ne sont plus nécessaires ou si la loi l'exige. Cette disposition est régie par la Loi 290/2004 sur les casiers judiciaires, tout comme les règles relatives à la protection des données à caractère personnel et à leur utilisation dans un contexte judiciaire. L'analyse de la loi susmentionnée permet de conclure que les empreintes digitales des personnes condamnées seront conservées jusqu'à la réhabilitation de la personne. Après cette période ou en cas d'amnistie ou de grâce, les empreintes digitales sont effacées du casier judiciaire. En ce qui concerne les personnes faisant l'objet d'une enquête pénale, si la procédure pénale se termine sans condamnation ou si la personne est acquittée, les empreintes digitales doivent être immédiatement effacées. Si des

[3372] Art. 190 Nouveau Code de Procédure Pénale Examen physique Expertise et constatation https://legeaz.net/noul-cod-procedura-penala-ncpp/art-190.
[3373] Art. 191 Nouveau Code de Procédure Pénale Expertise génétique médico-légale Expertise et constatation https://legeaz.net/noul-cod-procedura-penala-ncpp/art-191.
[3374] R. A. Nestor. *Utilizarea datelor stocate în Sistemul Național de Date Genetice Judiciare – restrângere necesară adusă vieții private sau protecție dincolo de limitele convenționale ?*, Jessentials, 2024. https://www.juridice.ro/essentials/8074/utilizarea-datelor-stocate-in-sistemul-national-de-date-genetice-judiciare-restrangere-necesara-adusa-vietii-private-sau-protectie-dincolo-de-limitele-coventionale.
[3375] LOI n° 76 du 8 avril 2008 relative à l'organisation et au fonctionnement du Système National de Données Génétiques Judiciares https://legislatie.just.ro/Public/DetaliiDocumentAfis/215.
[3376] *Décision ICCJ - RIL No 18 du 18.11.2013* https://legeaz.net/monitorul-oficial-7-2014/decizia-iccj-ril-18.

empreintes digitales ont été relevées sur des victimes ou des témoins, elles ne sont conservées que pendant la période nécessaire à la résolution de l'affaire.[3377]

Rappelons que cette loi est soumise et conforme à la législation européenne sur la protection des données (GDPR), qui impose des règles strictes en matière de collecte, de conservation et de suppression de ces données. Ainsi, toute personne a le droit de demander l'effacement de ses données si elles ne sont plus nécessaires ou si leur conservation est contraire à la loi[3378].

§2. LES CONTROVERSES JURIDIQUES AUTOUR DE LA GESTION DES CARACTÉRISTIQUES GÉNÉTIQUES EN EUROPE

1130. Jurisprudence relative à la suppression des données génétiques des personnes condamnées. Les discussions sur l'utilisation des données génétiques dans le domaine de la justice sont toujours d'actualité en Europe[3379]. Les plus grands débats portent sur la manière de les supprimer des bases de données nationales, ce qui fait l'objet de nombreux procès.[3380] En 2022, la Cour de Justice de l'Union Européenne (C.J.U.E.) est saisie et se prononce sur les limites temporelles de la conservation, à des fins de lutte contre les infractions pénales, de données à caractère personnel, y compris les preuves biologiques d'une personne condamnée définitivement pour une infraction pénale (affaire C-118/22). Il s'agit du cas d'un citoyen bulgare reconnu coupable et condamné pour une infraction. En 2022, il a été réhabilité et a demandé la suppression de ses données génétiques des registres de police, ce qui lui a été refusé[3381]. Le 30.01.2024, la C.J.U.E. a jugé dans l'affaire C-118/22 que la législation nationale autorisant la conservation par la police, à des fins de prévention, de détection, d'enquête ou de poursuite d'infractions pénales ou d'exécution de sanctions pénales, de données à caractère

[3377] LOI n° 290 du 24 juin 2004 (**republiée**)(*actualisée*) sur le casier judiciaire**) (actualisée jusqu'au 10 décembre 2016*) https://legislatie.just.ro/Public/DetaliiDocument/184428.

[3378] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (Règlement Général sur la Protection des Données - RGPD), Publié au Journal Officiel de l'Union Européenne, L 119, 4 mai 2016, ce règlement est également applicable en France et régit la protection des données génétiques. Disponible sur le site officiel EUR-Lex : www.eur-lex.europa.eu.

[3379] CEPD-EDPS, *Joint Opinion 5/2021 on the proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act),* 2021, https://www.edpb.europa.eu/system/files/2021-06/edpb-edps_joint_opinion_ai_regulation_en.pdf.

[3380] Cour de Justice de l'Union Européenne, Arrêts sur l'effacement des données génétiques https://curia.europa.eu/jcms/jcms/nbo1_147688/ro/?text=dATE+GENETICE&mode=all&rech_dans_tout=*&searchedFields=&searchedAllFields=true&searchInFiles=true&replaceFileDoc=true&dateSince=&dateSince_user=&dateSince_unit=86400000&cids=&catMode=ou&jsp=plugins%2FCuriaPlugin%2Fjsp%2Fquery.jsp.

[3381] Affaire C-118/22 Résumé de la demande de décision préjudicielle au titre de l'article 98, paragraphe 1, du Règlement de procédure de la Cour de Justice https://curia.europa.eu/juris/showPdf.jsf?text=&docid=257623&pageIndex=0&doclang=ro&mode=req&dir=&occ=first&part=1&cid=2680510.

personnel, y compris de données biométiques et génétiques, concernant des personnes qui ont été condamnées pour une infraction pénale par un jugement définitif, n'est pas conforme au droit de l'Union Européenne[3382].

A. Décision de la CJUE (le 30 janvier 2024) : conservation des données biométriques et génétiques, de « nécessité absolue »

1131. Question préjudicielle bulgare sur l'article 5 de la Directive (UE) 2016/680. Dans un arrêt récent, rendu le 30.01.2024, la CJUE[3383] souligne que la collecte et la conservation de données biométriques et génétiques de personnes impliquées dans des enquêtes pénales (en cours ou achevées) doivent être effectuées dans des cas « d'absolue nécessité ». La juridiction bulgare a saisi la CJUE d'une question préjudicielle sur l'interprétation de l'article 5 de la Directive (UE) 2016/680 du Parlement Européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données par rapport au droit national[3384].

Le litige au fond concernait la demande de NG, un ressortissant bulgare qui avait été reconnu coupable de parjure et condamné à une condamnation définitive pour parjure, de voir ses données génétiques et biométriques supprimées du registre national de la Police. Après avoir purgé sa peine et achevé sa période de réhabilitation, NG a introduit une demande auprès de la structure spécialisée du Ministère Bulgare de l'Intérieur et a demandé l'effacement de son casier judiciaire. Le 2 septembre 2020, la demande a été rejetée au motif que la réhabilitation ne faisait pas partie des motifs de radiation de l'enregistrement. Ces motifs ont également été confirmés par le Tribunal de la ville de Sofia lors de l'examen du recours du requérant.

La Cour d'Appel a renvoyé l'affaire devant la CEDH pour savoir si une législation nationale qui empêche la suppression des données biométriques et génétiques d'une personne après la période de réadaptation est contraire au droit européen.

[3382] *Affaire C-118/22 - NG contre Direktor na Glavna direktsia "Natsionalna politsia" pri Ministerstvo na vatreshnite raboti-* Sofia, Arrêt de la Cour (Grande Chambre) du 30 janvier 2024 https://curia.europa.eu/juris/document/document.jsf?docid=282268&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=RO&cid=2680510.

[3383] https://curia.europa.eu/juris/document/document.jsf?text=&docid=282264&pageIndex=0&doclang=RO&mode=req&dir=&occ=first&part=1&cid=1808675

[3384] Directive (UE) 2016/680 du Parlement Européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la Décision-cadre 2008/977/JAI du Conseil https://eur- .lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016L0680.

La réponse de la Cour a été assez catégorique, à savoir que le droit national doit être interprété comme ne restreignant pas le droit à l'effacement si la conservation n'est plus nécessaire, et que les autorités judiciaires ont l'obligation de vérifier périodiquement si les raisons de la conservation subsistent ou pas[3385].

1132. Stockage des données génétiques, aussi longtemps que nécessaire. En d'autres termes, « le droit à l'effacement des données à caractère personnel établi par le droit de l'Union interdit la conservation générale et indifférenciée, jusqu'à leur mort, des données biométriques et génétiques des personnes condamnées pour des infractions »[3386]. Le commentaire de la doctrine française sur cette décision accorde une attention particulière au considérant 26[3387] de la Directive 2016/680, qui prévoit que ces données ne doivent pas être conservées plus longtemps que nécessaire, et après que la finalité de la conservation a déjà été atteinte.

En pratique, le délai de conservation de la fiche dactyloscopique, de la photographie et de l'échantillon prélevé à des fins de profilage ADN ne pourrait pas aller jusqu'au décès du plaignant bulgare, sur la base de critères généraux et non individualisés. Par ailleurs, d'autres auteurs français[3388] rappellent que : « toutes les personnes ne présentent pas le même degré de risque d'implication dans d'autres infractions pénales. Ainsi, des éléments tels que la nature et la gravité de l'infraction commise ou l'absence de récidive peuvent indiquer que le risque présenté par la personne condamnée ne justifie pas nécessairement la conservation des données

---

[3385] Dispositif de la décision de la CJUE dans l'affaire C-118/22 : « L'article 41, lettres c) et e), de la Directive (UE) 2016/680 du Parlement Européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention, de détection, d'enquête ou de poursuite concernant des infractions pénales ou l'exécution de sanctions pénales, ainsi que de la libre circulation de ces données, et abrogeant la Décision-cadre 2008/977/JAI du Conseil, lue en combinaison avec ses articles 5 et 10, avec l'article 13, paragraphe 2, lettre b), tout comme l'article 16, paragraphes 2 et 3, et à la lumière des articles 7 et 8 de la Charte des droits fondamentaux de l'Union Européenne, doit être interprétée en ce sens que s'oppose à une législation nationale qui prévoit la conservation par les services répressifs, à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions, de données à caractère personnel, y compris de données biométriques et génétiques, relatives à des personnes ayant fait l'objet d'une condamnation définitive pour une infraction pénale commise intentionnellement et pour laquelle des poursuites pénales sont engagées d'office, jusqu'au décès de la personne concernée, y compris en cas de réhabilitation de celle-ci, sans imposer au responsable du traitement l'obligation vérifier à intervalles réguliers si cette conservation est encore nécessaire et sans reconnaître à la personne concernée le droit à l'effacement de ces données si leur conservation n'est plus nécessaire au regard des finalités pour lesquelles elles ont été traitées ou, le cas échéant, le droit à la limitation du traitement**. »**

[3386]D. Berlin, , *« En dépit de son intérêt pour de futures enquêtes pénales, la conservation des données des individus condamnées pénalement doit être limitée*", La Semaine Juridique, Edition Générale n° 07-08, art. 23, 2024.

[3387] « En particulier, il convient de veiller à ce que les données à caractère personnel collectées ne soient pas excessives et à ce qu'elles ne soient pas conservées pendant une durée excédant celle nécessaire à la réalisation de la finalité pour laquelle elles sont traitées. Les données à caractère personnel ne doivent être traitées que si la finalité du traitement ne peut raisonnablement être atteinte par d'autres moyens. Afin de garantir que les données ne sont pas conservées plus longtemps que nécessaire, des délais d'effacement ou de réexamen périodique devraient être fixés par le responsable du traitement. Les États membres devraient prévoir des garanties appropriées pour les données à caractère personnel qui sont conservées pendant une période plus longue à des fins d'archivage dans l'intérêt public ou à des fins scientifiques, statistiques ou historiques ».

[3388] G. Marti, L. Cluzel-Métayer, S. Merabet, *Intelligence artificielle - Droit et Intelligence artificielle*, La Semaine Juridique Edition Générale n° 25, doctr.820, 2024

la concernant jusqu'à son décès. Par conséquent, cette durée de conservation n'est pas appropriée lorsqu'elle est appliquée de manière générale et indifférenciée ».

Analyse doctrinale de la CJUE. Sur la base de cette affaire, la Cour de Justice de l'Union Européenne a rappelé que l'article 4, paragraphe 1, lettres c) et e), de la directive (UE) 2016/680 du Parlement Européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention, de détection, détection, d'enquête ou de poursuite en matière pénale ou d'exécution de sanctions pénales, ainsi que de libre circulation de ces données, et abrogeant la Décision-cadre 2008/977/JAI du Conseil, lue en combinaison avec ses articles 5 et 10, son article 13, paragraphe 2b), et son article 16, paragraphes 2 et 3[3389], et à la lumière des articles 7 et 8 de la Charte des droits fondamentaux de l'Union Européenne[3390] doit être interprétée en ce sens qu'elle s'oppose à une réglementation nationale qui prévoit la conservation, par les autorités de police, de données à caractère personnel à des fins de prévention, de détection, d'enquête ou de poursuite en matière pénale ou d'exécution de sanctions pénales. à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions, des données à caractère personnel, y compris des données biométriques et génétiques, relatives à des personnes ayant fait l'objet d'une condamnation définitive pour une infraction pénale commise intentionnellement et pour laquelle des poursuites pénales sont engagées d'office, et ce jusqu'au décès de la personne concernée, y compris dans le cas de sa réhabilitation, sans imposer au responsable du traitement l'obligation de vérifier intervalles réguliers si cette conservation est encore nécessaire et sans reconnaître à la personne concernée le droit à l'effacement de ces données si leur conservation n'est plus nécessaire au regard des finalités pour lesquelles elles ont été traitées ou, le cas échéant, le droit à la limitation du traitement.[3391]

En conclusion, la collecte et la conservation des données génétiques et biométriques des personnes condamnées sont effectuées de manière limitée dans le temps, en cas d'absolue nécessité, sans que l'État puisse porter atteinte aux droits à la protection des données privées

[3389] Règlement (UE) 2016/679 du Parlement Européen et du conseil du 27 avril 2016 https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32016R0679.
[3390] Charte des Droits Fondamentaux de l'Union Européenne, 2012/C 326/02, articles 7 et 8. pag 7 https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:12012P/TXT.
[3391] *Décision no. C-118/22/2024 du 30 janvier 2024,* Cour de Justice de l'Union Européenne https://sintact.ro/jurisprudenta/hotarari-judecatoresti/hotarare-nr-c-118-22-2024-din-30-ian-2024-curtea-de-justitie-a-13145574.

dans le but de prévenir ou de détecter des infractions de manière injustifiée et sans respecter le principe de proportionnalité[3392].

B. Intervention de la CJUE en cas de refus d'utilisation des données biométriques

1133. Renforcement de la sécurité vs limitation du droit à la vie privée. L'Allemagne étant l'un des premiers pays à générer des documents d'identité à partir d'empreintes digitales génétiques, les premières actions en justice sur le sujet ont également vu le jour. À Wiesbaden, un homme refuse de consentir à l'utilisation d'empreintes digitales biométriques sur sa carte d'identité, estimant que ses droits fondamentaux à la vie privée et à la protection des données sont violés. En réponse, les autorités de la ville de Wiesbaden refusent de lui délivrer une nouvelle carte d'identité sans y inclure ses empreintes digitales, conformément aux dispositions de l'article 3, paragraphe 5, du Règlement 2019/1157.[3393] Ce refus a été contesté devant le tribunal administratif de Wiesbaden. Ce dernier a demandé à la Cour de Justice de l'Union Européenne (CJUE) de résoudre cette affaire.[3394] La CJUE a examiné la conformité avec le Règlement (UE) 2019/1157 du Parlement Européen et du Conseil, qui légifère pour renforcer la sécurité des cartes d'identité par l'ajout d'empreintes digitales personnelles, clarifiant ainsi si l'utilisation obligatoire des empreintes digitales dans les documents d'identité respecte la vie privée et garantit la protection des données à caractère personnel. La CJUE de Luxembourg s'est prononcée sur cette affaire le 21 mars 2024. En ce qui concerne la validité du règlement, la CJUE l'a déclaré invalide car il a été adopté sur une base juridique incorrecte. Toutefois, il reste en vigueur jusqu'au 31 décembre 2026, date à laquelle l'Union Européenne devra adopter un nouveau règlement. En termes de droits fondamentaux, la Cour considère que, bien que la mesure limite le droit à la vie privée, elle est justifiée pour lutter contre la falsification et l'usurpation d'identité et pour faciliter la coopération entre les États membres de l'UE[3395].

[3392] P. Bonneville, C. Gänser, A. Iljic, *Chronique de jurisprudence de la CJUE, Poursuites pénales - Enregistrement des données biométriques et génétiques* AJDA 2023. https://www-dalloz- fr.docelec.u-bordeaux.fr/documentation/Document?id=AJDA/CHRON/2023/0510.

[3393] Règlement (UE) 2019/1157 du Parlement Européen et du Conseil du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation (Texte présentant de l'intérêt pour l'EEE.) https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32019R1157.

[3394] UE: *CJUE publishes judgment on the mandatory insertion in identity cards of two fingerprints* https://www.dataguidance.com/news/eu-cjeu-publishes-judgment-mandatory-insertion-identity.

[3395] Judgment of the Court in Case C-61/22 https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-03/cp24240050en.pdf.

De nombreux experts en la matière se sont exprimés sur le sujet. Mélanie Clément-Fontaine[3396], souligne que le stockage des empreintes digitales sur les documents d'identité est utile dans la lutte contre la fraude et l'usurpation d'identité, qui sont des objectifs d'intérêt majeur. Cependant, elle constitue une limitation du droit à la vie privée de l'individu, notamment en ce qui concerne le traitement des données à caractère personnel, qui est justifié par la finalité de la mesure (exposée ci-dessus). Elle souligne également que les données ne sont accessibles qu'au titulaire de la carte d'identité. En outre, en référence à l'affaire C-61/22 présentée ci-dessus, elle soutient qu'il n'était pas nécessaire d'analyser la conformité de la Cour de Justice de l'Union Européenne avec le règlement 2019/1157.

La Directive 2004/38/CE relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres est un autre texte législatif pertinent. La loi établit des règles claires sur la liberté de circulation, le droit d'établissement, le droit de travailler, les conditions de séjour, la protection contre l'expulsion[3397].

a). Empreintes digitales et faciales dans les documents d'identité

1134. Réglementation relative aux données biométriques sur les cartes d'identité. L'introduction de données biométriques[3398] (empreintes digitales et faciales) dans les bulletins électroniques est de plus en plus évoquée. En fait, le sujet est activement débattu en Europe, avec de nombreuses initiatives législatives en cours et des points de vue contradictoires quant à son impact sur les droits individuels.[3399]

Le Règlement (UE) 2019/1157 du Parlement Européen et du Conseil du 20 juin 2019 prévoit que les empreintes digitales et faciales du porteur doivent être incluses dans les documents d'identité (article 3). Cela a pour principal objectif d'identifier correctement l'individu, d'accroître la sécurité et la confiance dans l'utilisation des documents d'identité, de

[3396] M. Clément-Fontaine, *« Technologies de l'information » de la semaine du 26 juin 2023* Panorama rapide de l'actualité, 2023. https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=ACTU0218886.
[3397] Directive 2004/38/CE du Parlement Européen et du Conseil relative à la liberté de circulation et de séjour sur le territoire des États membres des citoyens de l'Union et des membres de leur famille, modifiant le Règlement (CEE) n° 1612/68 et abrogeant les Directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE du 29 avril 2004 https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32004L0038.
[3398] *Biometrics: definition, use cases and latest news,* Thales*,* 2023. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics.
[3399] M.Clément-Fontaine. *Panorama rapide de l'actualité «Technologies de l'information» de la semaine du 29 mai 2023*, Dalloz Actualité, 2023. https://www.dalloz-actualite.fr/flash/panorama-rapide-de-l-actualite-technologies-de-l-information-de-semaine-du-29-mai-2023.

réduire les cas de falsification.[3400] Selon le texte législatif susmentionné, tous les États membres de l'UE devaient commencer à délivrer ces cartes d'identité au plus tard le 2 août 2021, avec une période de transition pour le remplacement des anciennes cartes d'identité, facilitant ainsi les déplacements et l'identification dans l'espace de l'Union Européenne.

Bien entendu, l'utilisation de ces données génétiques personnelles doit se faire dans le respect du Règlement Général sur la Protection des Données (RGPD).[3401]

1135. L'Allemagne, pionnière de l'identité biométrique. L'Allemagne produit des cartes d'identité à empreintes digitales depuis 2021, ce qui en fait l'un des premiers pays à mettre en œuvre cette procédure. Selon le Ministère Allemand de l'Intérieur, les empreintes digitales sont enregistrées exclusivement sur le document d'identité, sans être stockées dans une base de données centralisée[3402]. Des pays comme la Suède et la France incluent également les empreintes digitales sur les documents nouvellement délivrés[3403]. En Roumanie, cette procédure est mise en œuvre à partir de 2023[3404].

1136. Préoccupations relatives aux atteintes à la vie privée. Le sujet suscite de nombreuses préoccupations et critiques. Certains se demandent s'il ne s'agit pas d'atteinte à la vie privée et d'une violation de la confidentialité, des droits et de la liberté personnelle[3405] si on n'arrive pas aux abus de la part des autorités, à une surveillance excessive, à des fins discriminatoires, d'exclusion sociale ou de stigmatisation.[3406] Elle soulève également des questions quant à la

[3400] Règlement (UE) 2019/1157 du Parlement Européen et du Conseil du 20 juin 2019 visant à renforcer la sécurité des cartes d'identité des citoyens de l'Union et des documents de séjour délivrés aux citoyens de l'Union et aux membres de leur famille exerçant leur droit à la libre circulation (Texte présentant de l'intérêt pour l'EEE.) https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32019R1157.

[3401] Règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 (Règlement Général sur la Protection des Données - RGPD), Publié au Journal Officiel de l'Union Européenne, L 119, 4 mai 2016, ce règlement est également applicable en France et régit la protection des données génétiques. Disponible sur le site officiel EUR-lex : www.eur-lex.europa.eu.

[3402] Loi relative à l'introduction d'une carte pour les citoyens de l'Union Européenne et les citoyens de l'Espace Économique Européen avec fonction d'identification électronique. https://www.gesetze-im-internet.de/eidkg/index.html#BJNR084610019BJNE000702116.

[3403] Code de la protection des données personnelles. Art. 4-3 (Décr. nº 2016-1460 du 28 oct. 2016, art. 15 ; Décr. nº 2017-910 du 9 mai 2017, art. 1(er)). https://www-dalloz-fr.docelec.u-bordeaux.fr/documentation/Document?id=DATA058348.

[3404] M.A.I. - D.E.P.A.B.D. - CEI. *Lignes directrices pour l'introduction des cartes d'identité électroniques* https://depabd.mai.gov.ro/directii_cei.pdf.

[3405] K. H. Orbán, F. Ní Aoláin. *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?*, Human Rights Centre - University of Minnesota, 2020. https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/Use-Biometric-Data-Summary.pdf.

[3406] A. M'charek, R. Hagendijk, W. Vries,(2013). *Equal before the Law: On the Machinery of Sameness in Forensic DNA Practice*. Science, Technology & Human Values, *2013. p.*542-565. https://doi.org/10.1177/0162243912453623.

sécurité du stockage de ces informations[3407] et à la protection adéquate des bases de données contre les menaces potentielles[3408].

Face à ces suspicions, le Contrôleur Européen de la Protection des Données cherche à clarifier les idées fausses sur la technologie biométrique en donnant des assurances solides sur la sécurité, la confidentialité et la protection de ces données.[3409] Selon l'article 10 de la Directive (UE) 2016/680, l'utilisation de ces données est soumise à une autorisation stricte[3410] et l'équilibre entre la finalité (dépendant principalement du type d'infraction) et l'impact sur les droits de l'individu est analysé au cas par cas[3411].

b). La Grande-Bretagne, un cas particulier

1137. Conservation illimitée des données ADN au Royaume-Uni. En ce qui concerne la situation en Europe, la plupart des États membres du Conseil de l'Europe autorisent le prélèvement obligatoire d'empreintes digitales et d'échantillons cellulaires dans le cadre de procédures pénales[3412], la plupart d'entre eux se limitant à des circonstances particulières ou à des infractions graves. Le Royaume-Uni est le seul État membre qui autorise expressément la conservation systématique et indéfinie des profils ADN[3413] et des échantillons cellulaires, y compris dans le cas de personnes qui ont été acquittées ou déchargées des poursuites pénales[3414]. Dans l'affaire Gaughran contre le Royaume-Uni,[3415] 2020, points 97-98, dans laquelle les autorités ont décidé de conserver pour une durée illimitée le profil ADN, les empreintes digitales et la photographie d'une personne condamnée pour conduite en état

---

[3407] L. voor Mensenrechten, *Nos empreintes digitales sur les cartes d'identité? Une mesure inutile et dangereuse,* Ligue des Droits Humains *2019.* https://www.liguedh.be/nos-empreintes-digitales-sur-les-cartes-didentite-une-mesure-inutile-et-dangereuse/.

[3408] Défenseur des Droits, Report *Biometrics: the urge to safeguard fundamental rights*, 2021 https://www.defenseurdesdroits.fr/sites/default/files/2023-07/ddd_rapport_technologies-biometriques_2021_EN.pdf.

[3409] European Data Protection Supervisor, *14 misunderstandings with regard to identification and authentication, June* 2020 https://www.edps.europa.eu/sites/default/files/publication/joint_paper_14_misunderstandings_with_regard_to_identification_and_auuthentication_en.pdf.

[3410] Council of State Decision no. 439360, paragraph 13 https://www.conseil- etat.fr/fr/arianeweb/CE/decision/2021-04-13/439360.

[3411] Council of Europe, Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention 108, Guidelines on Facial Recognition, 2021. p.3. https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.

[3412] *Manuel de législation européenne concernant la protection des données Edition 2018* https://fra.europa.eu/sites/default/files/fra_uploads/fra-coe-edps-2018-handbook-data-protection_ro.pdf.

[3413] A. Amankwaa, C. McCartney. *The UK National DNA Database: Implementation of Protection Freedoms Act 2012*, Forensic Science International, Volume 284, 2018, p.117-128 https://doi.org/10.1016/j.forsciint.2017.12.041. (https://www.sciencedirect.com/science/article/pii/S0379073817305571).

[3414] *Case of S. and Marper v. The United Kingdom, applications nos. 30562/04 et 30566/04*, Strasbourg 2008.

[3415] *Case of Gaughran v. The United Kingdom, applications no. 45245/15*, Strasbourg 2020.

d'ivresse, la Cour a conclu à la violation de l'article 8 de la CEDH, estimant que la conservation des données à caractère personnel du requérant, mesure prise sans tenir compte de la gravité de l'infraction commise et sans lui donner une véritable possibilité de recours, ne reflétait pas un juste équilibre entre les intérêts publics et privés concurrents[3416].

c). Eurodac, la base de données d'empreintes digitales de l'UE

1138. L'utilité d'une base de données biométrique internationale. L'Union Européenne (UE) dispose actuellement d'une base de données d'empreintes digitales appelée **Eurodac**.[3417] Celle-ci contient les empreintes digitales des migrants illégaux et des demandeurs d'asile politique des États membres de l'UE. Eurodac aide à respecter le **Règlement Dublin,** qui détermine l'État responsable de l'analyse des demandes d'asile, en vérifiant si et dans quels pays l'individu concerné a déjà demandé l'asile politique et s'il a déjà été détenu. Il permet également l'échange d'informations entre les pays de l'UE et la Norvège, l'Islande, la Suisse, le Liechtenstein, permettant ainsi de contrôler la situation des migrants.[3418] Ces dernières années, l'utilisation de cette base de données biométriques s'est développée dans des domaines tels que la lutte contre le terrorisme[3419] et la criminalité.[3420] Eurodac fonctionne dans le cadre du Règlement (UE) 603/2013, qui prévoit des mesures strictes en matière de protection et de confidentialité des données à caractère personnel.

[3416] A. Amankwaa, C. McCartney. *Gaughran vs the UK and public acceptability of forensic biometrics retention,* Science & Justice, Volume 60, Issue 3, 2020, p.204-205. https://doi.org/10.1016/j.scijus.2020.04.001. (https://www.sciencedirect.com/science/article/pii/S1355030620300629).

[3417] Mise à jour de la base de données d'empreintes digitales de l'UE https://www.consilium.europa.eu/ro/policies/eu- migration-policy/eu-migration-asylum-reform-pact/fingerprinting-database/#eurodac.

[3418] Règlement (UE) n° 603/2013 du Parlement Européen et du Conseil du 26 juin 2013 concernant la création du système « Eurodac » pour la comparaison des empreintes digitales en vue de l'application effective du Règlement (UE) n 604/2013 de détermination des critères et des mécanismes de détermination de l'Etat membre responsable pour l'analyse d'une demande de protection internationale présentée dans l'un des Etats membres par un ressortissant d'un pays tiers ou par un apatride et concernant les demandes des autorités d'application de la loi dans les Etats membres et d'Europol de comparaison des donéees Eurodac pour assurer le respect de l'application de la loi et de modification du Règlement (UE) no. 1077/2011 portant création d'une Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle dans le domaine de la liberté, de la sécurité et de la justice (refonte) https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32013R0603.

[3419] Report OL FRA 4/2020 Mandates of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; and the Special Rapporteur on the right of peaceful assembly and freedom of association, 12 November 2020 https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=25705.

[3420] K. Huszti-Orban, F. Ni Aolain, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?*,Human Rights Center, 2020. https://www.ohchr.org/sites/default/files/Documents/Issues/Terrorism/Use-Biometric-Data-Summary.pdf.

d). Identification basée sur les empreintes génétiques, interdite par l'Ordre des médecins

1139. Identification basée sur les empreintes génétiques, strictement réglementée. Le Code de Déontologie du Collège Roumain des Médecins stipule que la participation à des activités d'identification d'une personne sur la base de ses empreintes génétiques doit se faire conformément à la législation en vigueur et dans le respect des droits individuels. Il est interdit dans l'exercice de la profession médicale dans le domaine de la recherche médicale, de participer ou d'être impliqué dans une activité d'identification d'une personne sur la base de ses empreintes génétiques autrement que dans le cadre d'une procédure judiciaire pénale ou civile ou à des fins de recherche strictement médicale ou scientifique, toutes deux menées dans le strict respect de la loi.[3421]

Conclusions du Chapitre 3

Le chapitre 3 montre que les données génétiques se trouvent au cœur d'une zone de densité juridique maximale, dans laquelle la protection de la vie privée, la bioéthique et les intérêts légitimes de la médecine et de la justice doivent être harmonisés par des règles claires et différenciées. Les réglementations relatives aux caractéristiques génétiques – en particulier la législation française en matière de bioéthique, le droit à l'oubli génétique, le cadre de la médecine personnalisée et l'interdiction de la discrimination génétique – soulignent l'obligation de traiter les informations génétiques comme un élément essentiel de l'identité de la personne, soumis à un régime autonome de confidentialité et de limitation des utilisations. Les exemples d'utilisation abusive et le risque de discrimination sociale confirment la nécessité de garanties effectives en matière de consentement, de transparence et de finalité exclusive du traitement.

L'analyse des tests génétiques effectués directement pour les consommateurs met en évidence la vulnérabilité d'un secteur dans lequel les intérêts commerciaux peuvent contourner les filtres professionnels et déontologiques. La distinction entre l'utilisation des données à des fins médicales et scientifiques, sous contrôle éthique, et les offres directes au public, sans surveillance médicale adéquate, justifie des solutions restrictives telles que celles adoptées en France et en Suisse. Il en ressort la nécessité d'un cadre réglementaire garantissant le contrôle de la personne sur ses propres informations génétiques et empêchant la constitution de bases de données privées opaques.

[3421] *Code de déontologie médicale du Collège Roumain des Médecins du 04.11.2016 (En vigueur depuis le 06 janvier 2017*), Journal Officiel, Partie I n° 981, 2016.

En ce qui concerne l'identification par empreintes génétiques, le chapitre souligne l'extension progressive des registres ADN des crimes graves aux délits mineurs, la différenciation des durées de conservation et les particularités de la réglementation roumaine. Les récentes interventions de la CJUE, qui subordonnent la conservation des données biométriques et génétiques à une « nécessité absolue », confirment que la gestion de ces données ne peut être laissée à une logique d'accumulation illimitée. Les discussions sur les documents d'identité, Eurodac et les limites imposées à l'utilisation médico-légale indiquent une ligne jurisprudentielle qui ne conteste pas les instruments d'identification, mais les soumet à des critères stricts de proportionnalité et de finalité. Le chapitre pose ainsi les bases d'une protection de la vie privée génétique dans laquelle les intérêts pénaux et médicaux ne sont admis que dans la mesure où ils ne vident pas de son sens le droit de la personne à contrôler ses propres données biologiques.

Conclusions pour le Titre 2

Le titre 2 souligne un point commun aux trois chapitres : l'ingérence de l'État dans la vie privée ne peut plus être analysée uniquement à travers le prisme des techniques classiques d'enquête pénale, mais doit être replacée dans le contexte de l'ensemble des moyens techniques utilisés, depuis les perquisitions et les écoutes téléphoniques jusqu'à la surveillance électronique et l'exploitation des données génétiques. Il en ressort que le droit pénal est appelé à fonctionner à la fois comme un instrument de légitimation des mesures nécessaires à la protection de l'intérêt public et comme un système de garanties limitant l'extension incontrôlée du pouvoir public. La synchronisation du droit pénal avec l'évolution technologique ne signifie pas la multiplication illimitée des compétences de l'État, mais la clarification des conditions dans lesquelles la technologie peut être utilisée sans annuler le contenu du droit à la vie privée. Les éléments convergents des trois chapitres sont les suivants : la nécessité d'une base juridique précise pour toute forme d'intrusion ; la soumission des moyens techniques à un contrôle juridictionnel réel ; la distinction entre les mesures d'enquête, les sanctions et les instruments de gestion des données sensibles ; et le maintien d'un noyau intangible de l'autonomie de la personne. Ainsi, la technologie n'est pas acceptée comme argument pour relativiser les garanties, mais comme test de la capacité de l'ordre juridique à préserver les normes de l'État de droit dans des conditions d'intervention sans précédent.

CONCLUSIONS GÉNÉRALES ET PROPOSITIONS DE LEGE FERENDA

La protection pénale de la vie privée à l'ère technologique ne peut plus être envisagée comme un appendice du droit commun des libertés, mais comme un domaine autonome, traversé par la tension constante entre trois pôles : l'expansion technologique, l'extension de la capacité d'intervention de l'État et l'exigence de préserver un noyau effectif d'intimité, de dignité et d'autonomie personnelle. L'analyse comparative France-Roumanie montre qu'au-delà des différences de technique législative et de rythme de réaction, les solutions valables sont celles qui refusent à la fois le réflexe prohibitionniste général et l'abandon face à une technologie présentée comme inévitable. La recherche confirme que cette protection de la vie privée dans un monde entièrement nouveau et numérisé n'est pas une question de détail, mais un critère permettant de vérifier la maturité de l'État de droit. Dans un contexte dominé par les algorithmes, les données biométriques, la surveillance à distance, les identités numériques et les infrastructures de cryptage la question centrale n'est plus de savoir si le droit pénal intervient, mais comment il le fait, à quel coût et avec quelles garanties.

Le résultat principal consiste à clarifier un cadre de référence cohérent, dans un domaine où les normes sont dispersées, se chevauchent et sont parfois contradictoires. L'analyse des incriminations, de la jurisprudence et des pratiques institutionnelles met en évidence les domaines dans lesquels la protection est effective et ceux dans lesquels elle reste purement déclarative. Les exemples évoqués – atteinte à la vie privée, recours à la surveillance technique en dehors de garanties réelles, extension des bases de données génétiques, utilisation de *deepfakes* à des fins de discrédit ou de chantage, les interceptions effectuées par des structures non transparentes, l'utilisation du cryptage comme prétexte pour des mesures intrusives généralisées – montrent que le risque majeur n'est pas l'absence de moyens juridiques, mais la tentation de les utiliser sans délimitation stricte. La contribution de cet ouvrage consiste à établir des repères normatifs clairs pour ce domaine d'intersection : toute intervention dans la vie privée – physique ou numérique – doit avoir une base juridique claire, un objectif déterminé, une durée limitée, un contrôle externe réel et la possibilité d'une vérification ultérieure. Les algorithmes, l'intelligence artificielle, le métaverse, le cryptage ou les registres ADN ne justifient pas la suppression de ces exigences, au contraire, ils les rendent plus nécessaires.

Dans la lignée traditionnelle, la protection du domicile, de la correspondance et des conversations privées a été recalibrée pour intégrer la capture audio-vidéo, la géolocalisation, la surveillance électronique, les interceptions massives et l'utilisation de moyens techniques cachés. Le droit français offre un cadre fragmenté mais dense, dans lequel les incriminations et la jurisprudence délimitent les situations protégées, formalisent les conditions d'autorisation et

laissent place à des contrôles externes (CNCTR, contrôle juridictionnel). En droit roumain, la création d'une infraction autonome d'atteinte à la vie privée, la réglementation des moyens spéciaux de surveillance et l'adaptation aux normes européennes en matière de protection des données et des communications dessinent un cadre normatif moderne, aligné sur les exigences contemporaines. Ce cadre reste toutefois en cours de consolidation : son efficacité dépend de la cohérence législative, de l'uniformité de la pratique judiciaire et de la capacité des institutions à appliquer les mesures intrusives exclusivement dans des conditions de légalité, de nécessité et de proportionnalité, afin que l'intervention pénale ne soit pas perçue comme une extension du contrôle étatique, mais comme une garantie de la protection des droits fondamentaux. En comparaison, le droit français se distingue par une construction plus ancienne et plus élaborée : incriminations détaillées, contrôles institutionnalisés, intervention constante des autorités indépendantes. Le droit roumain se distingue par l'adoption rapide de normes européennes et par des incriminations modernes (par exemple, la divulgation d'images intimes), mais il reste vulnérable aux ambiguïtés institutionnelles, aux pratiques parallèles et à une jurisprudence fluctuante, souvent indulgente.

Les technologies algorithmiques et les médias numériques génèrent un autre type de pression : la vie privée est affectée non seulement par la divulgation, mais aussi par la construction et la manipulation. Le profilage de masse, les recommandations opaques, les *deepfakes*, les campagnes coordonnées de désinformation, l'utilisation du métaverse ou des identités numériques reconfigurent la criminalité sans la dissocier du support humain.

La dimension comparative France-Roumanie permet de vérifier ces conclusions dans deux systèmes soumis aux mêmes normes européennes, mais avec des traditions institutionnelles différentes. Deux tendances se dessinent : d'une part, la préférence pour des solutions techniques de plus en plus sophistiquées (surveillance électronique, profilage, accès à des données sensibles) présentées comme une réponse inévitable à la criminalité contemporaine ; d'autre part, la difficulté réelle de maintenir un contrôle judiciaire authentique, la traçabilité des décisions et la responsabilité personnelle dans l'utilisation de ces outils. L'étude montre que lorsque la base juridique est précise, que le contrôle est efficace et que les institutions indépendantes fonctionnent, les ingérences peuvent être compatibles avec la protection de la vie privée ; lorsque ces conditions font défaut, la technologie devient rapidement un vecteur d'abus structurels.

Dans cet recherche, je n’avais pas l’intention d’analyser uniquement la transformation de la vie privée d’un simple concert spécifique à la philosophie ou à la sociologie en un droit fondamental, mais la manière dont le droit, notamment le droit pénal, offre une protection réelle à ce droit. Le développement de la technologie et le monopole des algorithmes représentent à

la fois un territoire de bénéfices pour l'individu ou la société mais aussi un défi pour le droit pénal.

Étant une étude comparative, j'ai pu trouver et présenter des arguments concrets sur le fait que l'appétit pour la régulation du législateur français est beaucoup plus développé que celui du législateur roumain. Les outils utilisés par le droit pénal pour garantir la protection que tout le monde a été acclamé sont conscients de certaines limites générées par la nature du changement social et numérique. Par exemple, alors qu'à première vue, cela peut sembler une idée dilatante, la vie privée et privée peuvent bénéficier d'une protection accrue dans un espace public surpeuplé plutôt que dans votre propre maison. En effet, les appareils intelligents à la maison ne servent plus seulement le rôle classique que nous connaissons, mais servent également de superviseur des utilisateurs : le fer à repasser peut enregistrer audio-vidéo une querelle conjugale tout en repassant un t-shirt, le réfrigérateur envoie des préférences culinaires à des serveurs tiers, la montre transmet la santé du propriétaire aux réseaux sociaux.

Je comprends que le principal problème auquel est confronté le droit pénal aujourd'hui, dans le contexte de la protection de la vie privée, est de traiter des algorithmes, de la surveillance massive et de la collecte injustifiée de données privées.

1140. Compléments pour la protection de la vie privée. Je pense que la loi peut subir quelques changements et à cet égard, je formule les propositions suivantes *de la loi à être élaborée* :

- 1) en ce qui concerne la manière dont les actes visés au paragraphe 1 de l'article 226 du Code pénal sont détenus, je considère que la disposition juridique devrait être modifiée en ce sens que la notion de « logement, chambre ou dépendance » s'étendrait à « tout espace de nature privée » et non à la notion d'espace contenue dans la « notion de domicile » pénale, de sorte que la condition de caractère objectif de la violation de la vie privée ne limite pas strictement et restrictivement l'espace où le délit est commis.

Bien que, par la décision HP no 18/2024[3422], la haute Cour de cassation et de justice ait établi que « les notions de logement, de chambre ou de dépendance à l'égard du contenu du délit d'atteinte à la vie privée, prévues au paragraphe 1 de l'article 226 du Code pénal, ont le même sens que les notions de logement, La place ou la dépendance par rapport au contenu de l'infraction de violation du domicile, prévue à l'article 224, paragraphe 1, du Code pénal, étant subsumée à la notion de domicile au sens du droit pénal », Toutefois, dans les considérants de la décision, elle rappelle que dans les lois des autres états, ce supplément pour la protection de la vie privée étendue à tous les locaux a été introduit, soulignant que toute modification du cadre

[3422] ICCJ, *décision nº 18, le 22 avril 2024*, https://www.iccj.ro/2024/05/15/decizia-nr-18-din-22-aprilie-2024-2/

juridique « représente l'option exclusive du législateur », ce dernier étant tenu de modifier la forme actuelle de l'article 226, paragraphe 1, du Code pénal.

1141. Personnalisation des espaces : logement, toilettes, cabine d'essayage. Afin de renforcer cette proposition, nous soulignons que dans d'autres législations, cette distinction claire entre la notion d'espace de vie et la notion de toilettes ou de salle d'essai est traitée, une spécification qui n'a pas été reprise dans la législation roumaine.

Dans le contexte de la question de droit, nous considérons que la « personnalisation de ces espaces » par le législateur pour ne subsumer qu'à la notion classique de résidence, selon le droit pénal, est limitative, au détriment des victimes et des dispositions relatives aux droits de l'homme, puisque la loi sur la protection de la vie privée n'a pas été adaptée à la réalité sociale actuelle.

Le législateur doit considérer et accepter le raisonnement logique selon lequel la « vie privée » ne se déroule pas seulement dans le foyer exclusif. Nous considérons qu'il est essentiel de noter que « les notions de logement, de chambre, de dépendance » visées à l'article 226, paragraphe 1, du Code pénal sont *des notions autonomes* qui n'acquièrent pas le même sens et ne doivent pas être rattachées au sens de la notion figurant à l'article 224 du Code pénal. La preuve de distinction dans l'interprétation de ces notions clés réside précisément dans le fait qu'à l'article 226, paragraphe 1, du Code pénal, le législateur a indiqué que « la personne est dans une pièce (…) » Et n'utilise pas l'espace comme une maison, comme le prévoit l'article 224 du Code pénal « logement, chambre, dépendance sans le consentement de la personne qui les utilise »

L'essence réside dans leur interprétation précisément en analysant le nom marginal du délit de *violation de la vie privée de* manière à inclure le sens de l'« espace » pour inclure les lieux où nous menons des aspects de notre vie privée de quelque manière que ce soit, y compris le groupe sanitaire, la salle d'essai et le vestiaire, le bureau personnel, le lieu de travail, etc.

- (2) en ce qui concerne l'intégration des algorithmes dans la vie quotidienne, je considère que l'article 77 du Code pénal peut être modifié en ce sens que l'utilisation de l'intelligence artificielle pour commettre des délits constitue une circonstance aggravante. Je considère que le raisonnement pour lequel le législateur a estimé qu'une circonstance aggravante devrait être retenue si l'acte est commis par trois personnes ou plus ou si un majeur utilise un mineur pour commettre un crime, il en va de même pour l'utilisation de l'intelligence artificielle à des fins criminelles.
- (3) en ce qui concerne la volonté du législateur roumain de ne pas punir la tentative de violation de la vie privée, je considère qu'elle est erronée et devrait être sanctionnée. Cela permettrait de mieux protéger le droit défendu et de décourager les comportements antisociaux

qui se multiplient, selon les statistiques fournies par le Ministère de la justice. Le Code pénal français punit la tentative.

(4) je considère également que l'article 226 du Code pénal peut être complété par une disposition visant à prévenir l'utilisation abusive de la géolocalisation, afin de surveiller le lieu où se trouve une personne. À ce stade-ci, il existe une réglementation juridique très générale, qui est utilisée dans le but de punir les personnes qui surveillent l'emplacement d'une autre personne, mais je trouve cela inapproprié. Par exemple, l'installation d'un dispositif de repérage dans le sac ou la voiture d'un partenaire commercial est punie par l'article 26 de la loi 51 du 29 juillet 1991[34233424] sur la sécurité nationale de la Roumanie. Je comprends que l'approche du législateur roumain n'est pas conforme aux réalités dans lesquelles nous vivons aujourd'hui et que l'instrumentation de certains faits qui, de mon point de vue, sont étroitement liés à la protection du droit à la vie privée, sur la base d'une loi sur la sécurité nationale, semble inappropriée. Ainsi, je reprendrais le règlement dans la forme prévue par l'article 226, paragraphe 1, du Code pénal français, qui sanctionne l'acte de violation délibérée de la vie privée d'autrui : « en capturant, enregistrant ou transmettant, par tout moyen, le lieu en temps réel ou avec un délai d'une personne, sans leur consentement. » Les éléments constitutifs de ce délit sont liés à la protection de la vie privée des individus et non à la sécurité nationale.

[3423] *Loi n° 51 du 29 juillet 1991 relative à la sécurité nationale de la Roumanie, publiée au Journal officiel n° 190 du 18 mars 2014*, https://legislatie.just.ro/Public/DetaliiDocument/1517.

[3424] *Article 26*:

(1) l'exercice, sans autorisation, d'activités spécifiques de collecte d'informations soumises à l'autorisation prévue par la présente loi ou excédant l'autorisation accordée est passible d'une peine d'emprisonnement de deux à sept ans si l'acte ne constitue pas une infraction plus grave.

(2) la même peine sanctionne l'acte du fonctionnaire qui révèle, refuse ou empêche, de quelque manière que ce soit, l'exécution du mandat délivré en vertu de la présente loi.

(3) la tentative est punie.

Bibliographie

I. Dictionnaires généraux

ALLAND, D., RIALS, S.(dir.), *Dictionnaire de la culture juridique,* Quadrige/Lamy, PUF, 2003.

ANTONIU G., BULAI C., *Dicționar de drept penal și procedură penală*, Hamangiu, 2011.

CADIET L.(dir.), *Dictionnaire de la justice*, PUF, 2004.

CHAGNOLLAUD, D., DRAGO, G., *Dictionnaire des droits fundamentaux*, 1e éd., Dalloz, 2006.

CORNU, G., *Vocabulaire juridique*, Association Henri Capitant, 12e éd., PUF, 2018.

DE SABOURET, D*., Dictionnaire élémentaire du droit*, 2e éd., Dalloz, 2016.

GUINCHARD, S., DEBARD, T., *Lexique des termes juridiques 2025-2026,* 33e éd., Paris, Dalloz, 2025.

LALANDE, A., *Vocabulaire technique et critique de la philosophie,* PUF, 2010.

LITTRÉ, É., *Dictionnaire de la langue française*, Paris, 1863-1873.

ROLAND, H., BOYER, L., *Adages du droit français*, Litec, 3e éd., 1992.

SĂULEANU, L. B., RĂDULEȚU, S., *Dicționar de termeni și expresii juridice latine*, ed. a II-a, C.H. Beck, 2011.

II. Thèses

AÏDAN, G., *Le Fait psychique: objet des normes juridiques*, 357 p., Thèse de doctorat: droit public, Paris I, Panthéon-Sorbonne, 2012.

ANCIAUX, N., *Essai sur l'être en droit privé*, 607 p., Thèse de doctorat: droit privé, Paris II, Panthéon-Assas, 2018.

AUBRY DE MAROMONT, C*., Essai critique sur la théorie des obligations en droit privé*, 279 p., Thèse de doctorat: droit privé et sciences criminelles, Nantes, 2015.

BARNIN, E., *La protection directe de l'intérêt général par l'administration: la mise en œuvre de la police administrative préventive*, 140 p.,Thèse de Master 2: droit public, Lyon 3, n° 23, 2013.

BÉNÉJAT, M, *La responsabilité pénale professionnelle*, 522 p., Thèse de doctorat: droit, Bordeaux IV, 2010.

BIOY, X., *Le concept de personne humaine en droit public. Recherche sur le sujet des droits fondamentaux,* Thèse de doctorat: droit public, Toulouse 1, 2001.

BORDÈRE, C., *La justice algorithmique. Analyse comparée (France/Québec) d'un phénomène doctrinal*, 881 p.,Thèse: droit public, Bordeaux, 2023.
BOSSAN, J., *L'intérêt général dans le procès pénal*, 752 p., Thèse de doctorat: droit privé et sciences criminelles, Poitiers, 2007.
DALLOZ, M., *Les circonstances aggravantes légales en droit criminel français,* Thèse de doctorat: droit privé et sciences criminelles, Nice, 2001.
DÉCIMA, O., *L'identité des faits en matière pénale*, 496 p, Thèse de doctorat:droit pénale, Bordeaux IV, 2006.
DELEGOVE, N., *Le droit commun et le droit spécial*, Thèse de doctorat: droit, Paris 2, 2011.
EL HILALI, K., *De la surveillance à la vigilance de l'État*, 612 p, Thèse de doctorat: droit, Paris II, Panthéon-Assas, 2022.
EYNARD, J*., Les données personnelles: quelle définition pour un régime de protection efficace?*, 435 p., Thèse de doctorat: droit, Toulouse, 2013.
FOREST, G., *Essai sur la notion d'obligation en droit privé*, 570 p, Thèse de doctorat: droit privé, Tours, 2010.
HARIVEL, J*., Libertés publiques, libertés individuelles. Risques et enjeux de la société numérique*, 633 p., Thèse de doctorat: droit public, Paris I, Panthéon-Sorbonne, 2018.
HUTTNER, L*., La décision de l'algorithme*, *Étude de droit privé sur les relations entre l'humain et la machine*, 694 p*.,* Thèse de doctorat: droit privé, Paris I, Panthéon-Sorbonne, 2022.
JACOBET DE NOMBEL, C., *Théorie générale des circonstances aggravantes*, 538 p., Thèse de doctorat: droit, Bordeaux IV, 2004.
JAMMET, A., *La Prise en Compte de la Vie Privée dans l'Innovation Technologique*, thèse de doctorat en droit, Université de Lille, 2018.
KOUMPLI C., *Les données personnelles sensibles: contribution à l'évolution du droit fondamental à la protection des données personnelles. Étude comparée: Union européenne, Allemagne, France, Grèce, Royaume-Uni,* Thèse de doctorat: droit public, Paris I, Panthéon-Sorbonne, 2019.
LACAZE, M., *Réflexions sur le concept de bien juridique protégé par le droit pénal*, 553 p, Thèse de doctorat: droit pénal, Montpellier 1, 2009.
LANGLOIS, B., *Culture de l'information, culture de l'image et culture par l'image dans l'enseignement secondaire*, 416 P., thèse de doctorat, Université de Montpellier 3, 2019.
MALABAT, V., *Appréciation in abstracto et appréciation in concreto en droit pénal,* Thèse de doctorat: droit, 471 p., Bordeaux IV, 1999.

NAGOUAS-GUÉRIN, M.C., *Le doute en matière pénale,* 444 p., Thèse de doctorat: droit pénale, Bordeaux IV, 2000.
PERCEROU, R., *La personne morale de droit privé : patrimoine d'affectation*, 196 p.,thèse de doctorat: droit privé, Paris 1 – Panthéon-Sorbonne 1951.
PORTNOFF R. S., *The Dark Net: De-anonymization, Classification, and Analysis*, 129 p., Thèse de doctorat: philosophy in Computer Sciences, UC Berkeley, 2018.
POUYANNE, J., *L'auteur moral de l'infraction,* 685 p., Thèse de doctorat: droit, Bordeaux IV, 2001.
PUIGELIER, C., *Géraldine Aïdan,Le fait psychique, objet des normes juridiques,* 562 p., Thèse de doctorat: droit public, Paris I, Panthéon-Sorbonne, 2017.
RENARD, B., *Ce que l'ADN fait faire à la justice : Sociologie des traductions dans l'identification par analyse génétique en justice pénale*, 511 p., Thèse de doctorat:criminologie, Louvain, 2008.
SAINT-PAU, J.-C., *L'anonymat et le droit*, Thèse de doctorat: droit privé, Bordeaux IV, 1998.
SHANNON, C. E., *A Symbolic Analysis of Relay and Switching Circuits,* 72 p., Thèse de master: Computer Science, Michigan, United States, 1936.
VANVLASSELAER, M., *Un avenir commun au sein de la société numérique*, Mémoire de Master 2, 2025.
VERGNOLLE, S*., L'effectivité de la protection des personnes par le droit des données à caractère personnel,* 560 p.,Thèse de doctorat: droit privé, Paris II, Panthéon-Assas, 2020.
VÉRON, N., *Protection des données personnelles et renseignement. Contribution à l'indentification d'un régime juridique autonome,* 646 p., Thèse de doctorat: droit public, Pau*,* 2021.
VIAL, A., *Systèmes d'intelligence artificielle et responsabilité civile: droit positif et proposition de réforme*, 421 p, Thèse de doctorat: droit privé et sciences criminelles, Besançon, 2022.
VIGNON-BARRAULT, A., *JurisClasseur – Responsabilité civile et assurances, Fasc. 133-10 : Droit à réparation. Responsabilité fondée sur la faute. Atteintes aux droits de la personnalité. Droit à la vie privée. Droits susceptibles d'atteinte*, Lexis 360 Intelligence, 2022.
VISCIANO, T., *L'obligation adjointe,* 395 p, Thèse de doctorat: droit, Paris Cité, 2023.
YOUHNOVSKI SAGON, A.L*., Le droit à la vie humaine*, *Contribution à l'étude des relations entre la vie humaine et le droit,* 845 p., Thèse de doctorat: droit public, no 492, Lyon III, 2021.

III. Ouvrages généraux

Droit pénal et droit de la peine

Langue française

ANDRÉ, C., *Droit pénal spécial*, 7e éd., Paris, Dalloz, 2024.

BAUER, A., *La criminologie pour les nuls*, First, 2022.

BEAUVAIS P., CHILSTEIN D., DREYER E.(dir.), *Le droit pénal de l'avenir*, coll. *Thèmes & commentaires*, Dalloz, 2024.

BEAUVAIS P., *La nouvelle surveillance pénale*, 1er éd., coll. Droit & Justice , PUF, 2022.

BENTHAM, J., *Traités de législation civile et pénale*, trad. Étienne Dumont, Paris, Dalloz, coll. « Traités », n° 1, 2010.

BERGÉ, J.-Syl., COURBE, P., *Introduction générale au droit*, 19e éd., Paris, Dalloz, coll. Mémentos, 2025.

BERGEAUD-WETTERWALD, A., SAINT-PAU, J.C.(dir*.), La preuve pénale: Problèmes contemporains en droit comparé*, L'Harmattan, 2013.

BERGEL, J.-L., *Théorie général du droit*, coll. Méthodes du droit, Dalloz, 4e éd., 2003.

BONFILS, P., GRÉGOIRE, L**.**, *Droit pénal spécial*, Paris, Lextenso, 2022.

BOULOC, B., *Droit pénal général*, coll. Précis, Dalloz, 28e éd., 2024.

BOULOC, B., *Droit pénal général*, coll. Précis, Dalloz, 29e éd., 2024.

BOULOC, B*., Procédure pénale*, 29e éd., collection Précis, Dalloz, Paris, 2023.

CONTE P., *Droit pénal spécial – Infractions du Code pénal,* 7e éd., Dalloz, 2014.

CONTE, P., DETRAZ, S., LARGUIER, J., *Procédure pénale*, 26e éd., coll. Mémentos, Paris, Dalloz, 2023.

CONTE, P., *Droit pénal spécial*, 6e éd., LexisNexis, 2019.

DÉCIMA, O., DETRAZ, S., VERNY, É., *Droit pénal général*, 6e éd., Paris, LGDJ, 2024.

DECOCG, A., *Droit pénal général*, 1re éd., Paris, Dalloz, coll. Bibliothèque Dalloz, 2025.

DONNEDIEU DE VABRES, H., *Traité élémentaire de droit criminel et de législation pénale comparée*, Paris, Librairie du Recueil Sirey, 1924.

DREYER, E., *Droit pénal spécial*, 3e éd., Paris, Ellipses, n° 449, 2016.

DREYER, V.-E., *Droit pénal général*, 6e éd., Paris, LexisNexis, n° 1283, 2021.

FOUCAULT, M., *Théories et institutions pénales. Cours au Collège de France, 1971-1972*, Paris, Éd. EHESS/Gallimard/Seuil, coll. « Hautes études », 2015.

HERZOG-EVANS, M*., Droit de l'exécution des peines*, Paris, Dalloz, 2023/2024.
JEANDIDIER, W, BELOT, J., *Les grandes décisions de la jurisprudence:procédure pénale,* coll. Thémis, Presses universitaires de France (PUF), 1986.
JEANDIDIER, W., *Droit pénal général*, Paris, Montchrestien, coll. Domat droit public, 1991.
JOSÈPHE, P., *La société immédiate*, Paris, Calmann-Lévy, 2008.
LARGUIER, J., FOURNIER S., CONTE, P*., Droit pénal spécial*, Paris, Dalloz, 2024.
LAUGHLAND, J., *Le Tribunal pénal international: gardien de l'ordre mondial*, Paris, François-Xavier de Guibert, 2003.
LEPAGE, H., MATSOPOULOU, H., *Droit pénal spécial,* 1re éd., coll. Thémis Droit , PUF, 2015.
LOLIES, I., *La protection pénale de la vie privée,* Presses Universitaires d'Aix-Marseille (PUAM), 1999.
MALABAT, V., . *Droit pénal spécial*, 10e éd., Dalloz, collection HyperCours, 2022.
MALABAT, V., *Droit pénal spécial,* 7e éd., Dalloz, 2015
MERLE, R., VITU, A., *Droit pénal spécial*, Cujas, 1982.
MERLE, R., VITU, A., *Traité de droit criminel*, vol.I, 7e éd., n° 550, Paris, Cujas, 1997.
PIN, X., *Droit pénal général*, 17e éd., Paris, Dalloz, coll. Cours – Série Droit privé, 2025.
PIN, X., *Le consentement en matière pénale*, Paris, LGDJ, 2002.
PRADEL, J, *Droit pénal comparé*, 4e éd., Dalloz, Paris, 2016.
PRADEL, J., DANTI-JUAN, M., *Droit pénal spécial*, 7e éd., Cujas, 2017.
PRADEL, J., *Droit pénal général*, coll. Référence, 19e éd., Cujas, 2012.
PRADEL, J., *Procédure pénale*, 18e éd., Cujas, 2015.
RASSAT, M.-L., *Droit pénal spécial – Infractions du Code pénal*, 9e éd., Dalloz, 2024.
RASSAT, M.-L., *Droit pénal spécial,* 5e éd., Dalloz, 2006.
RASSAT, M.-L., *Le droit pénal*, 2e éd., coll. Connaissance du droit, Dalloz, Paris, 2025.
SAINT-PAU, J.C., *Droit pénal et autres branches du droit*, coll. Actes Et Etudes, Cujas, 2012.
VÉRON, M., *Droit pénal spécial,* 14e éd., coll. Sirey Université, Paris. Sirey, 2012.
VÉRON, M., *Droit pénal spécial,* 16e éd., Dalloz, 2017.
VÉRON, M., *Droit pénal spécial*, 17e éd., coll. Sirey Université, Paris, Sirey, 2019.

Langue roumaine

ANTONIU, G, *Codul Penal pe înțelesul tuturor*, Politică, 1970.
BOGDAN, S., ȘERBAN, D. A., *Drept penal. Partea specială*, Universul Juridic, 2022.
BOGDAN, S., ȘERBAN, D. A., ZLATI, G., *Noul Cod Penal. Partea specială*, Universul Juridic, 2014.

BOROI, A., NEGRUȚ, G., *Drept procesual penal*, 3e éd., Ed. Hamangiu, Bucarest, 2022.

BOROI, Al., *Drept penal. Partea specială*, C.H. Beck, 2022.

CIOCLEI, V., *Drept penal. Partea specială I. Infracțiuni contra persoanei și infracțiuni contra patrimoniului*, 2e éd., C.H. Beck, 2017.

CRIȘU, A., *Drept procesual penal. Partea generală*, 6e éd., Ed. Hamangiu, Bucarest, 2022.

DOBRINOIU, V., et al., *Noul Cod Penal comentat. Partea specială*, Universul Juridic, 2016.

GHEORGHE, T.V., *Aflarea adevărului, principiu fundamental al procesului penal*, Ed. Hamangiu, Bucarest, 2021.

GHEORGHE, T.V., et all., *Codul de procedură penală. Comentariu pe articole. Vol I. Partea generală*, 4e éd., Ed. Hamangiu, Bucarest, 2024.

LOGHIN, O., TOADER, T., *Drept penal român. Partea specială*, Șansa, 2001.

MICU, B., SLĂVOIU, R., ZARAFIU, A., *Procedură penală*, 2e éd., Ed. Hamangiu, Bucarest 2024.

NEAGU, I., DAMASCHIN, M., *Tratat de procedură penală. Partea generală*, IVe édition révisée et augmentée, Universul Juridic, Bucarest, 2022.

NEAGU, N., *Noul Cod penal comentat*, Universul Juridic, 2014.

PARASCHIV, C.S., *Drept Procesual Penal. Curs pentru Master*, Éditions Hamangiu, Bucarest, 2024.

PINTEA, A., PINTEA D.C., BĂLĂNESCU, A.C., *Urmărirea penală. Aspecte teoretice şi practice, Modele de acte procesuale şi procedurale*, 2e édition révisée et augmentée, Ed. Universul Juridic, Bucarest, 2020.

STRETEANU, F., NIȚU, D., *Drept penal. Partea generală*, vol. I, Universul Juridic, 2014.

TEODORU, G.G., CHIȘ, I.-P., *Tratat de Drept procesual penal*, 4e éd., Ed. Hamangiu, Bucarest, 2020.

TOADER, T., ANTONIU, G.(coord.), *Explicațiile Noului Cod Penal*, vol. IV, Universul Juridic, 2016.

TOADER, T., ANTONIU, G.(coord.), *Explicațiile Noului Cod Penal*, vol. III, Universul Juridic, 2015.

TOADER, T., *Drept penal român. Partea specială*, vol. I, Universul Juridic, 2019.

TOADER, T., *Noul Cod Penal. Comentarii pe articole*, Hamangiu, 2014.

UDORIU, M., et all., *Codul de procedură penală. Comentariu pe articole*, 2e éd., Ed. C.H. Beck, Bucarest, 2017.

UDORIU, M., et all., *Codul de procedură penală. Comentariu pe articole*, 3e éd., Ed. C.H. Beck, Bucarest, 2020.

UDROIU, M. *Sinteze de drept penal. Partea specială*, vol. I, C.H. Beck, 2022.

UDROIU, M., *Drept penal. Partea specială*, , C.H. Beck, 2016.
UDROIU, M., *Fişe de procedură penală. Partea generală. Teorie şi cazuri practice*, 3e éd., ed. C.H. Beck, Bucarest, 2022.
UDROIU, M., *Procedură penală. Partea generală*, 4e éd., Ed. C.H. Beck, Bucarest, 2017.

Autre langue

FIANDACA, G., MUSCO, E., *Diritto penale. Parte generale*, 3e éd., Bologne, Zanichelli, 2001.
SEMERARO P., *Il sistema penale di Gabriel Tarde*, Padoue, CEDAM, coll. Collana di Studi Penalistici, vol. XXXVI, 1984.

Droit civil et droit de la personne

Langue française

ANCIAUX, N., *Essai sur l'être en droit privé*, Paris, LexisNexis, Hors collection, 1re éd., 2019.
CARBONNIER, J., *Traité de droit civil*, 21e éd., coll. Thémis, PUF, 2000.
CLAUX, P.-J., DAVID, S., et all*., Droit et pratique du divorce,* 6e éd., Dalloz Référence, 2024-2025.
DUGUIT, L., *Les transformations générales du droit privé depuis le Code Napoléon*, Félix Alcan, 1912.
FENOUILLET, D., TERRÉ, F., *Droit civil. Les personnes*, 8e éd., Dalloz, 2012.
GÉNY, F., *Science et technique en droit privé positif: nouvelle contribution à la critique de la méthode juridique*, Paris, LGDJ, 1922.
GLEIZE, B., BRUGUIÈRE, J. M., *Droits des personnes*, 1e éd., Lefebvre Dalloz, 2023.
HENNETTE VAUCHEZ, S., ROMAN, D., *Droits de l'homme et libertés fondamentales,* Dalloz, 5e éd., 2022.
KAYSER, P., *La protection de la vie privée par le droit: Protection du secret de la vie privée*, Economica, 1995.
LUCAS, F.-X., *Manuel de droit de la faillite*, 5e éd., Paris, PUF, n° 7, 2024.
MUZNY, P., *La liberté de la personne sur son corps*, Dalloz, 2010.
SAVATIER, R., *Les métamorphoses économiques et sociales du droit privé d'aujourd'hui*, vol. I, 2e série, Dalloz, 1959.
TERRE, F., SIMLER, P., LEQUETTE, Y., *Droit civil, Les obligations,* coll. Précis Droit privé, 11e éd, Dalloz, 2013.
ZENATI-CASTAING, F., REVET, Th., *Manuel de droit des personnes*, PUF, 2006.

Autre langue

ACKERMAN, B.*, Before the Next Attack: Preserving Civil Liberties in an Age of Terrorism,* Yale Univerisity Press, 2006.

BARAK, A., *Proportionality. Constitutional Rights and their limitations*, Cambridge, CUP, 2012.

BERSIER, N., BEZEMEK, C., SCHAUER, F., *Common Law – Civil Law,* Springer 2022.

HARRIS, D., O'BOYLE, M., WARBICK, C., *Law of the European Convention on Human Rights*, Oxford University Press, 2023.

Droit de la personnalité / Presse / Protection des données

Langue française

BÉNÉDICTE, R., *La Vie privée à l'ère du numérique*, Cachan, Lavoisier, 2012.

BERNATCHEZ S., *La protection des données personnelles et la recherche scientifique en France*, Dalloz, 2019.

BROGLI, M. et al., *Droit des données personnelles*, Paris, Dalloz, coll. Décryptage, 1re éd., 2019.

DESGENS-PASANAU, G., *La protection des données personnelle,* 5e éd., LexisNexis, 2022.

DREYER, E., *Droit de la presse et droits de la personnalité*, Dalloz, 2012.

FAUCHOUX, V., BRUGUIÈRE, J.-M., DEPREZ, P., *Le droit de l'Internet, lois, contrats et usages*, 2e éd., LexisNexis, 2013.

FÉRAL-SCHUHL, C., *Cyberdroit. Le droit à l'épreuve de l'internet*, Dalloz, 2020.

FÉRAL-SCHUHL, C., *La protection des données personnelles*, Dalloz, 1e éd., 2019.

FÉRAL-SCHUHL, C., *Protection des données personnelles*, Paris, Dalloz, 2021.

GRYNBAUM, L., LE GOFFIC, C., PAILLER, L., *Droit des activités numériques*, 2e éd., Paris, Lefebvre Dalloz, 2023.

HASLER,T., *Droits de la personnalité: rediffusion et droit à l'oubli*, Dalloz, 2007.

LE TOURNEAU, Ph., *Contrats du numérique: informatiques et électroniques*, 11e éd., Dalloz, 2020.

LUCAS, A., DEVEZE, J., FRAYSSINNER, J., *Droit de l'informatique et de l'Internet*, coll. Thémis, PUF, 2001.

MAISON-ROUGE, O. *Les cyberisques. La gestion juridique des risques à l'ère immatérielle*, LexisNexis, 2018.

MALLET-POUJOL, N., *Droit des communications électroniques*, Légipresse, 2016.
MATTATIA, F., *RGPD et droit des données personnelles,* 5e éd., Eyrolles, 2021.
SAINT-PAU, J.-Ch.(dir.), *Droits de la personnalité*, LexisNexis, 2013.
TAILLAT, S., CATTARUZZA, A., DANET, D.(dir.), *La cyberdéfense – Politique de l'espace numérique*, Armand Colin, 2018.
TAMBOU, O., *Manuel de droit européen de la protection des données à caractère personnel,* coll. Paradigme, Bruylant, 2021.

Langue roumaine

ALEXE, I., PLOEȘTEANU, N.D., ȘANDRU, D.M., *Protecția datelor cu caracter personal*, ed. Universitară, 2017.
MIHĂILĂ, C., *Drepturile personalității. Studiu comparativ*, Universul Juridic, 2024.
OPRE, A., SĂVOIU, A., *Protecția datelor cu caracter personal în România*, Universul Juridic, 2022.
ȘANDRU, S., *Protecția datelor personale și viața privată,* Hamangiu, București, 2016.

Théorie générale / Philosophie du droit/ Éthique/ Sources interdisciplinaire/Sociologie

Langue française

ANDRÉ W., *Aristote, L'Éthique à Nicomaque,* Bulletin de l'Association Guillaume Budé, n°1, 1972.
ARISTOTE *Les politiques*, éd. P. Pellegrin, Paris, Flammarion, 2015.
BEIGNIER B., THOMAT-RAYNAUD A.-L., *Introduction au droit*, 9e éd., Paris, LGDJ-Lextenso, 2024.
BENTHAM , J., BOWRING, J. (éd.), *The Works of Jeremy Bentham*, vol. IV, Edinbourg, William Tait, 1843. (11vols.)
CABRILLAC, R., *Introduction générale au droit*, 16e éd., Paris, Dalloz, 2025.
CARBONNIER J., *Essais sur les lois*, Paris, LGDJ, coll. Anthologie du droit, 2013.
CARBONNIER, J., *Sociologie juridique,* coll. Quadrige, PUF, 1972, rééd. 2016.
CARLEVARIS, M.-T., *Le Kaléidoscope de la vie*, Société des Écrivains, 2016.
CHAMPEIL-DESPLATS, V., *Méthodologies du droit et des sciences du droit*, 3e éd., Paris, Dalloz, 2022.
DE BECHILLON D, *Qu'est ce qu'une règle de droit ?* éditions Odile Jacob, Paris, 1997.
DEBORD G., *La société du spectacle*, Paris, Buchet-Chastel, 1967.
DELMAS-MARTY, M**.**, *Le pluralisme ordonné. Les forces imaginantes du droit, II. L'un et le multiple: les divers pluralismes. Introduction*, Paris, Seuil, 2009.

DU CHÈNE P.-H., *La bioéthique et le droit en France*, Presses Universitaires de France, 2020.
FONTAINE, L., *La pensée kaléidoscopique de Jacques Zylberberg*, coll. Thélème, Academia, 2021.
FOUCAULT, M., *Pierre Boulez, l'écran traversé*, in *Dits et écrits II. 1976-1988*, 2e éd., 1994, Paris, Gallimard, « Quarto », 2001, vol. 2/2.
GIROT, J.-L. (dir.), *Le harcèlement numérique*, Paris, Dalloz, 2005.
GODELIER, M., *L'idéel et le matériel. Pensée, économies, sociétés*, Paris, LGF, 1992.
GUILHEM, J. (dir.), *Sciences et sens de l'intelligence artificielle*, Paris, Dalloz, coll. « Thèmes & commentaires », 2020.
HABERMAS, J., *L'Espace public*, *archéologie de la publicité comme dimension constitutive de la société bourgeoise*, Payot, 1978.
HART, H.L.A., *Le concept du droit*, Bruxelles, Facultés universitaires Saint-Louis, 1976.
HENNING, J., *Introduction historique au droit*, 1re éd., Paris, Dalloz, 2025.
HERVÉ, M., *Décloisonner les identités : Essai sur les enjeux anthropologiques de l'altérité*, Paris, Le Cavalier Bleu, 2024.
HIRSCHMAN, A. O., *Bonheur privé, action publique*, L'espace du politique, Fayard, 1983.
HOBSBAWM, E., *L'Âge des extrêmes. Histoire du court XXe siècle*, Bruxelles, Éditions Complexe / Le Monde diplomatique, 1999.
JESTAZ, Ph., *Les sources du droit*, 3e éd., Paris, Dalloz, coll. Connaissance du droit, 2022.
JOUANJAN, O., ZOLLER, E., *Le « moment 1900 ». Critique sociale et critique sociologique du droit en Europe et aux États-Unis*, Paris, Éditions Panthéon-Assas, 2015.
KELSEN, H., *Théorie pure du droit*, Paris, Dalloz, 1962.
LAREF, L., LAREF, M., MICHAËL (dir.), *Surveillance*, coll. Thèmes & Commentaires, Paris, Dalloz, 2024.
LECLERC, G., *Le regard et le pouvoir*, Presses Universitaires de France, 2006.
LECOUTRE, F., *La controverse entre Hans Kelsen et Eric Voegelin en théorie du droit et en théorie politique*, Institut francophone pour la justice et la démocratie, coll. « Collection des thèses », vol.195, 2020.
MADELÉNAT, D., *L'intimisme*, Paris, PUF, coll. Littératures modernes, 1989.
MARTIN, P., *Projets de séquençage à grande échelle en France*, Paris, Dalloz, 2022.
OST, F., VAN DE KERCHOVE, M., *Jalons pour une théorie critique du droit*, Bruxelles, Facultés universitaires Saint-Louis, 1987.
PERROT, M., *Les ombres de l'histoire: Crime et châtiment au XIXe siècle*, Paris, Flammarion, 2001.
RABAULT, H., *La logique juridique*, Dalloz, coll. Connaissance du droit, 1re éd., 2024.

SUPIOT, A., *La gouvernance par les nombres*, Paris, Fayard, 2015.
TERRÉ, F., MOLFESSIS, N., *Introduction générale au droit*, 17e éd., Paris, Dalloz, 2025.

Langue roumaine

ARISTOTEL, *Etica Nicomahică*, București, Editura Științifică și Enciclopedică, 1988.
BANU, *Sistemul filozofic al lui Aristotel*, Universitatea din București, 1977.
BOBOȘ, Gh., *Teoria generală a dreptului*, Editura Argonaut, 1999.

Autre langue

BALL, K., HAGGERTY, K., LYON, D.(dir.), *Routledge Handbook of Surveillance Studies*, London/New York, Routledge, 2012.
BODEN, M. A., *Mind as Machine: A History of Cognitive Science,* 2 vol., Oxford, Oxford University Press, 2006.
FULLER, L., *The Morality of Law*, Yale University Press, 1969.
GELLNER, E**.**, *Nations and Nationalism*, Ithaca (NY), Cornell University Press, 1983.
GILLESPIE, T., *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media,* Yale University Press, 2018.
HABERMAS, J., *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society,* Cambridge, Polity Press, 1989.
HABERMAS, J., *A New Structural Transformation of the Public Sphere and Deliberative Politics*, Wiley, 2023
HAN, B.-Ch., *The Transparency Society*, Redwood City (Calif.), Stanford University Press, coll. Stanford Briefs, 2015.
HART, H. L. A., *Punishment and Responsibility: Essays in the Philosophy of Law*, Oxford University Press, 1968.
KANT, I., *Critique of Pure Reason*, Cambridge University Press, 1998.
KAPLAN, E., HEGARTY, C.(dir.), *Understanding GPS: Principles and Applications*, 2e éd., Artech House Inc., 2006.
KURKI, V. A., *A Theory of Legal Personhood*, Oxford University Press, 2019.
SMET, S., *Resolving Conflicts between Human Rights. The judge's dilemma,* London and New York, Routledge, 2017.
TYLOR, E. B., *Primitive Culture : Researches into the Development of Mythology, Philosophy, Religion, Art, and Custom*, Vol. 1, Londres, J. Murray, 1871.

IV. Ouvrages spéciaux, monographies, volumes thématiques

Langue française

ARIÈS, Ph., *Histoire de la vie privée*, Éditions du Seuil, 1985-1987.

BIGOT C., *Protection pénale des droits de la personnalité*, Paris, Dalloz, 2023–2024.

BIGOT, C., *Pratique du droit de la presse 2023-2024*, 4e éd., coll. « Hors collection – Pratique du droit de la presse », Paris, Dalloz, 2023.

BIZET, T., *Vers la fin de la vie privée ? Les données personnelles à l'ère des Big Data*, Privacy Law, Academia.edu.

BONIS, P., et all., *Enjeux numériques*, *Compliance et nouvelles régulations*, Annales des Mines, n° 30, 2025.

BOSSAN, J., *La protection de la représentation à l'ère du numérique et du deepfake: le délit de montage version 2.0*, Légipresse, 2024.

BRAYER, F., *La Loi Annotée du 11 Mai 1868 sur la Presse*, Librairie A. Durand, 1868.

BRISSON, L., *Le dialogue socratique comme moyen d'accorder l'usage privé du discours à son usage public,* Études platoniciennes, vol.6, 2009.

BRUNETEAUX, P., *Maintenir l'ordre : les transformations de la violence d'État en régime démocratique*, Paris, Presses de Sciences Po, 1996.

BURROUGHS, W., *Révolution numérique*, Paris, Allia Éditions, 2017.

BYK C., *L'utilisation des tests génétiques dans le domaine de l'assurance en droit français et européen : une affaire d'assurance et de politique publique* , in book: *Genetic Testing and the Governance of Risk in the Contemporary Economy,* p.193-220 Springer, 2020.

CABRILLAC, V., *Le corps humain*, in: *Libertés et droits fondamentaux*, Dalloz, 2023.

CALLEWAERT, J., *L'adhésion de l'Union européenne à la Convention européenne des droits de l'homme*, Éd. du Conseil de l'Europe, 2013.

CARON, C., *Le caractère anodin de l'information chasse la vie privée*, Dalloz, 2004

CASTETS-RENARD, C., EYNARD, J. (dir.), *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général, perspectives comparées*, Bruxelles, Bruylant, 2023.

CATHELINE, N., *L'évolution des politiques françaises de lutte contre le harcèlement scolaire et le cyber-harcèlement*, in CHAGNON, J., WEISMANN-ARCACHE, C., *Le harcèlement scolaire : approche clinique et psychopathologique*, In Press, 2023.

CESPEDES ARTEAGA, P., PARAVANO, L., SAURON, J.-L., *S'y retrouver au sein du droit de la protection des données : boussole pour DPO et autres usagers de la donnée*, Luxembourg/Paris, Éd. Legitech, 4e éd., 2022.

CESTAC, J., MEYER, T., *Des attitudes à la prédiction du comportement : le modèle du comportement planifié*, in MORCHAIN, P., SOMAT, A., *La psychologie sociale : applicabilité et applications*, Presses universitaires de Rennes, 2010.

CHEVALIER, É*., Leçon 5 – Propriété, données personnelles et publiques* , in M. BOUDOT, D. VEILLON (dir.), *Les propriétés*, Presses universitaires juridiques de Poitiers, 2016.

CHOPIN, F., *Répertoire de droit pénal et de procédure pénale: Cybercriminalité – Responsabilité pénale des fournisseurs de contenu*, Dalloz, 2020.

CLARÉKE, R., *Introduction to Dataveiélance and Information Privacy, and Definitions of Terms*, version révisée, Xamax Consultancy Pty Ltd, 2006.

CLÉMENT FONTAINE, M., *L'homo numericus*, in Claire Bouglé-Le Roux (dir.), *Le corps et le droit : des cheveux du roi mérovingien à l'homo numericus*, Paris, LexisNexis, 2019.

CLERMONT-FERRAND, *The home : the public use of a private space, from Antiquity to the present day*, journée d'étude, Maison des Sciences de l'Homme, 2012.

COMPIÈGNE, I., *Chapitre VI. Société de liberté ou de surveillance ? La société numérique en question(s)*, Éditions Sciences Humaines, 2010.

COMPIÈGNE, I., *La société numérique en question(s)*, Éditions Sciences Humaines, 2010.

CORBIN, A., COURTINE J.-J., VIGARELLO G. (dir.), *Histoire du corps – Tome 1: De la Renaissance aux Lumières*, Éditions du Seuil, 2011.

CORNUÉJOLS, A., MICLET, L**.**, *Apprentissage artificiel: concepts et algorithmes*, Paris, Éditions Eyrolles, 2011.

COSTA, J.-P., *Les droits de l'homme et la bioéthique*, Éditions La Découverte, 2019.

CROUZATIER-DURAND, F., *Fiche 7. Le droit à la vie privée (1) : la protection de la vie privée*, in *Fiches de Libertés publiques et droits fondamentaux : Rappels de cours et exercices corrigés*, p. 63-74, Ellipses, 2017.

DEPADT-SEBAG, V., CHAMBAUD, L., *La Nouvelle Loi de bioéthique en question(s) – Sur quels principes s'établit le droit relatif à la bioéthique ?*, Presses de l'EHESP, 2021.

DOMINGO-FERRER, J., SORIA-COMAS, J., *Anonymization in the time of big data*, in DOMINGO-FERRER, J., PEJIÉ-BACH, M. (éd.), Privacy in Statistical Databases, PSD, coll. Lecture Notes in Computer Science, vol. 9867, 2016.

DOUBLIER, P., *Le consentement de la victime*, in G. Stéfani (dir.), *Quelques aspects de l'autonomie du droit pénal*, ouvrage collectif, Paris, Dalloz, 1956.

DUPRÉ, M., *Numérique – majorité numérique et lutte contre la haine en ligne*, Lexis 360 Intelligence, 2023.

EL YAHYAOUI, Y., « Chapitre troisième. Les plateformes numériques “globales”: puissance et abus de position », in *Économie des plateformes numériques : Captation de la valeur, pouvoir de marché et communs collaboratifs*, L’Harmattan, 2021.

FABRE-MAGNAN, M*, L’institution de la liberté*, Paris, PUF, 2018.

FAHMY-ABDOU, V.-A., *Le consentement de la victime*, Paris, LGDJ, coll. « Bibliothèque de sciences criminelles », t. XI, 1971.

FAUVARQUE-COSSON, B. (dir.), *La sphère privée : IXe Journées Juridiques Franco-Japonaises*, Société de législation comparée, 2016.

FELDMAN, J., *L’idée de science au XIXe siècle*, L’Harmattan, 2006.

FERRAND, F., *Répertoire de procédure civile: exigence d’un consentement de l’intéressé (879–883)*, Dalloz, déc. 2013, actualisation juil. 2024.

FEYERABEND, P., *Contre la méthode. Esquisse d’une théorie anarchiste de la connaissance*, Seuil, 1979.

FUENTES-CAMACHO, T., *Les Dimensions internationales du droit du cyberespace*, Éditions Unesco, 2000.

FUKUYAMA F., *La fin de l’homme. Les conséquences de la révolution biotechnique*, trad. fr., Paris, La Table Ronde, 2002.

G’SELL, F. (dir.), *Le Big Data et le Droit*, Paris, Dalloz, coll. « Thèmes & commentaires – Actes », 2020.

GALLIC, C., MARRONE, R., *Le grand livre du marketing digital*, Dunod, 2023.

GANASCIA, J.-G., *Le “Big Data” menace la démocratie*, in *Intelligence artificielle : vers une domination programmée ?*, Le Cavalier Bleu, 2017.

GANASCIA, J.-G., *Le mythe de la singularité : faut-il craindre l’intelligence artificielle ?*, Paris, Seuil, 2017.

GANTEZ A., *L’Entretien des musiciens*, Paris, 1643.

GAUTIER, M., *L’ordre public*, in AUBY, J.B.(dir.), *L’influence du droit européen sur les catégories du droit public*, Paris, Dalloz, 2010.

GHERNAOUTI, S., *Cybersécurité : analyser les risques, mettre en œuvre les solutions*, 7e éd., Dunod, 2022.

GÎRBEA, C., *Le bouclier dans l’imaginaire médiéval : Les fonctions symboliques du bouclier*, Paris, Classiques Garnier, 2024.

GONOD, P., MELLERAY, F., YOLKA P. (dir.), *Traité de droit administratif*, vol.2, Paris, Dalloz, 2010.

GRAWITZ M., *Méthodes des sciences sociales*, 11e éd., Paris, Dalloz, 2000.

GRUSON, C., HAN, B.C., *Infocratie. Numérique et crise de la démocratie*, Paris, PUF, 2023.

GRUZD A., HERNÁNDEZ-GARCÍA Á., *Privacy Concerns and Self-Disclosure in Private and Public Uses of Social Media*, Cyberpsychology, Behavior, and Social Networking, vol. 21, n° 7, 2018.

GUÉRIN-PACE, F., et al., *En quête d'appartenances*, Ined Éditions, 2009.

GUILHEM, J. (dir.), *Sciences et sens de l'intelligence artificielle*, Paris, Dalloz, coll. Thèmes & Commentaires, 2020.

HALBWACHS M., *La mémoire collective*, Paris, Presses Universitaires de France, 1950.

HALBWACHS, M., *Les cadres sociaux de la mémoire*, Paris, Félix Alcan, 1925.

HARBULOT, C., *Fabricants d'intox. La guerre mondialisée des propagandes*, Lemieux Éditeurs, 2016.

HARCOURT B. E., *La société d'exposition. Désir et désobéissance à l'ère numérique*, Paris, 2020.

HARTCOURT B. E., *Le Big Brother de George Orwell*, Cairn, 2024.

HERON J., *L'ordre public dans le procès. Rapport français*, dans *L'ordre public*, Travaux de l'Association Henri Capitant, Journées libanaises, t. XLIX, Beyrouth, 1998, Paris, LGDJ, 2001.

HOOG, E., *Mémoire année zéro*, Paris, Le Seuil, coll. Essais, 2009.

IFRAH, G., *Histoire universelle des chiffres*, Paris, Robert Laffont, 1981.

JANICOT, L., *L'anonymisation du juge*, in BOURDON, P. (dir.), *La communication des décisions du juge administratif*, Paris, LexisNexis, 2020.

KAPLAN, D., *Informatique, libertés, identités*, Paris, FYP Éditions, 2010.

KAUFMANN, J.-C., *L'invention de soi. Une théorie de l'identité*, Paris, Armand Colin, 2004.

KAYSER, P., *La protection de la vie privée*, 2e éd., Revue internationale de droit comparé, vol. 43, n° 1, 1991.

KHOURY L., BLACKETT A., VANHONNAEKER L.(dir.), *Genetic Testing and the Governance of Risk in the Contemporary Economy*, vol. 34, Cham, Springer, 2020.

KURZWEIL, R., *Humanité 2.0: La Bible du changement*, Paris, M21, 2007.

LAREF, L., LAREF, M.(dir.), *Surveillance*, Paris, Dalloz, coll. « Thèmes & commentaires – Actes », 1re éd., 2024.

LATIL, A., À quand le *Quantum Act* ?, Dalloz, 2023, n° 43.

LATIL, A., *Droit de l'intelligence artificielle (droit international et droit européen)*, JurisClasseur Communication, fasc. 988, LexisNexis, 2024.

LATIL, A., *Le droit du numérique : une approche par les risques*, Paris, Dalloz, coll. Droit numérique, 2023.

LAZERGES C., HENRION-STOFFEL H., *Chronique de politique criminelle*, Archives de politique criminelle, Paris, Éditions Pedone, 2015.

LE COLLECTIF ONZE, *Au tribunal des couples : Enquête sur des affaires familiales*, Odile Jacob, 2013.

LE TOURNEAU, P., *Contrats du numérique : informatiques et électroniques 2025-2026*, 13e éd., Paris, Dalloz, 2025.

LEMIEUX, F., *Intelligence and state surveillance in modern societies : an international perspective*, Leeds, Emerald Publishing, 2024.

LEMKE, T., *Perspectives on Genetic Discrimination*, Routledge, 2013.

LEONETTI, X., *Smartsécurité et cyberjustice*, Paris, Presses Universitaires de France, 2021.

LEVÊQUE, A., *Données et intelligence artificielle : quels enjeux pour la cybersécurité des États ?*, Cahiers français, 419(1), 2021.

LINDON R., *La presse et la vie privée*, *JCP*, 1965.

LOIVISI, C., *Introduction historique au droit*, 6e éd., Paris, Dalloz, coll. « Cours », 2022.

MALHERBE P.-J., *La vie privée et le droit moderne*, Librairie du Journal des notaires et des avocats, 1968.

MALLET-BRICOUT B., FAVARIO Th., *L'identité, un singulier au pluriel*, Dalloz, 2015.

MARCOS, S. (éd.), *Entre espace public et espace privé : les élites en représentation*, Presses Universitaires de Perpignan, 2018.

MARZANO, M., *Visages de la peur*, PUF, coll. La condition humaine, 2009.

MATOSAS-LOPEZ, L., *The Impact of Digitalization on Current Marketing Strategies*, Emerald Publishing Limited, 2024.

MORIN, E., *Penser global. L'humain et son univers*, Paris, Robert Laffont, 2015.

NEGROPONTE, N., *L'Homme numérique*, Paris, Éditions Pocket, 1997.

NOCETII, J., *Tous influencés par les réseaux sociaux?,* La Documentation française, 2025.

PÉGUY, C., *Charles Péguy*, éd. Cavazzini et Soskin, Presses universitaires de Liège, 2016.

PELTIER V., *Le placement sous surveillance électronique et l'environnement du condamné*, în *Actes du Colloque Environnement et peine privative de liberté*, s.s. dir. E. Bonis, A. Zabalza, Travaux de l'Institut de sciences criminelles et de la justice de Bordeaux, Cujas, n° 2, 2013.

PETTIT P., *Républicanisme: une théorie de la liberté et du gouvernement*, Paris, Gallimard, 2004.

PIANETA, D., *Histoire de l'informatique : Tome 1 – Les histoires*, Édition 2020.

PIGEON, G., *Sécurisez votre ordinateur et vos données : déjouer les pièges et user des bonnes pratiques*, Éditions ENI, 2021, p. 45.

PIN, X, *La théorie du consentement de la victime en droit pénal allemand : éléments pour une comparaison,* Revue de science criminelle et de droit pénal comparé (RSC), n° 2, 2003.

PIOLINO P., DESGRANGES B., EUSTACHE F., *La mémoire autobiographique : théorie et pratique*, Paris, Solal, 2000.

PLATON, *Œuvres complètes*, Paris, Flammarion, nouv. éd. revue et corrigée, 2023.

POSNER, R. A., SOLOVE, D., *Nothing to Hide: The False Tradeoff between Privacy and Security*, New Haven, Yale University Press, 2011.

QUÉMÉNER, M., *Crimes et délits – le cyberharcèlement et les raids numériques : quelles réponses juridiques ?*, La Semaine Juridique – Édition Générale, n° 3, 2025.

RABAGNY-LAGOA, A., *Fiches de droit du traitement et de la protection des données personnelles : rappels de cours et exercices corrigés*, Ellipses, 2022.

RABEHARISOA, V., PATERSON F., *Maintenir une infrastructure en droit : le rôle du comité technique du Fichier national automatisé des empreintes génétiques*, in VAILLY J.(dir.), *Sur la trace des suspects*, Éditions de la Maison des sciences de l'homme, 2021.

RABUT-BONALDI, G., *Le préjudice en droit pénal*, Paris, Dalloz, coll. « Nouvelle Bibliothèque de Thèses », n° 159, 1re éd., 2016.

RAZAC, O., *Avec Foucault, après Foucault : Disséquer la société de contrôle*, L'Harmattan, 2008.

REY, B., *La vie privée à l'ère du numérique*, Paris, Hermès-Lavoisier, coll. « Traitement de l'information », 2012.

REY, B*., La vie privée à l'ère du numérique*, Lavoisier, coll. Traitement de l'information, 2012.

RHEINGOLD, H., *Les communautés virtuelles. Autoroutes de l'information : pour le meilleur ou pour le pire ?*, Paris, Addison Wesley France, 1995.

RICOEUR*,* P., *Le volontaire et l'involontaire,* coll. « Philosophie de l'esprit », Aubier, Paris, 1948.

ROUSSEAU F., *La personnalité juridique*, in Traité des droits de la personnalité, LexisNexis, 2013.

SAINT-PAU, J.-Ch., *Droit au Respect de la Vie Privée et Droit Pénal*, Dr. Pénal, 2011.

SAURON, J.-L., PARAVANO, L., CÉSPEDES, P., *S'y retrouver au sein du droit de la protection des données: boussole pour DPO et autres usagers de la donnée*, Legitech, 2022.

SAURON, J.-L., VITARD, A., *Vos données personnelles : que savoir et comment faire pour qu'elles le restent !*, Paris, Legitech, 1re éd., 2021.

SLINGENEYER, T., *La surveillance électronique selon le Conseil de l'Europe : entre un contrôle de la réinsertion et une réinsertion par le contrôle*, in R. LÉVY, L. DUMOULIN, A. KENSEY, C. LICOPPE (dir.), *Le bracelet électronique : action publique, pénalité et connectivité*, Médecine & Hygiène, 2019.

SPRUMONT D., *Quelle réglementation des trousses d'analyse génétique*, in JOYE C.(dir.), *L'analyse génétique humaine : Quelles perspectives législatives*, Schulthess, 2004.

STOCK P.-V. (éd), L'affaire Dreyfus. Le procès Zola devant la cour d'assises de la Seine et la cour de cassation (7 février-23 février-31 mars-2 avril 1898): compte rendu sténographique "in extenso" et documents annexes, aux bureaux du „Siècle", 1989.

STUPIOT, A., *La gouvernance par les nombres*, Paris, Fayard, 2015.

TAILLAT, S., CATTARUZZA A., DANET D.(dir.), *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2018.

TOURNAND, J.-C., *Introduction à la vie littéraire du XVII*e *siècle*, Paris, Bordas, 2005.

UNTERSINGER, M., BAYART, B., *Anonymat sur Internet: protéger sa vie privée*, 2e éd., Paris, Eyrolles, 2014.

VAILLY J., *Sur la trace des suspects: l'incorporation de la preuve et de l'indice à l'ère de la génétique*, Éditions de la Maison des sciences de l'homme, 2021.

VAN DROOGHENBROECK, S., VAN DE KERCHOVE, M., *Subsidiarité et droit pénal : aspects nouveaux d'une question ancienne* , in DELPÉRÉE, F.(dir.), *Le principe de subsidiarité. Actes des journées juridiques J. Dabin*, Bruxelles, Bruylant, 2002.

VELASCO, V., *La difficile formalisation d'un droit à la vie privée*, in BAUDRY, P., et al *La vie privée à l'heure des médias*, Presses Universitaires de Bordeaux, 2002.

VITALIS, A., *Informatique, pouvoirs et libertés*, Paris, Économica, 1981.

VIVANT, M., BRUGUIÈRE, J.-M**.**, *Droit d'auteur et droits voisins*, 5e éd., Paris, Lefebvre-Dalloz, 2024.

WALCH, A. (dir.), *La Médiatisation de la vie privée, XVe-XXe siècle*, Arras, Artois Presses Université, coll. Histoire, 2012.

WINTREBERT, B., *Innovation confidentielle : l'avantage secret*, Paris, Éditions EMS, coll. Questions de société, 2024.

YVES, P., *La vie privée à l'heure de la société du numérique. État des lieux*, Bruxelles, Larcier, 2019.

ZOLYNSKI, C., *Privacy by Design et Big Data*, Academia.edu, 2016.

Langue roumaine

BAIAS, F.-A., CHELARU, E., CONSTANTINOVICI, R., MACOVEI, I., *Noul Cod Civil. Comentariu pe articole*, București, C.H. Beck, 2012.

BÎRSAN, C., *Convenția europeană a drepturilor omului. Comentariu pe articole*, Vol. I *Drepturi și libertăți*, Editura All Beck, București, 2005.

BOROI, A., *Drept penal. Partea specială*, Editura C.H. Beck, București, 2011.

FOUCAULT, M., *A supraveghea și a pedepsi*, București, Humanitas, 1997.
OPREA, M., *Banalitatea răului. O istorie a Securității în documente (1949–1989)*, Iași/București, Polirom, 2002.
PAVEL D., TURIANU C., *Calomnia prin presă*, București, Casa de Editură și Presă Șansa, 1996.
POTORAC, R., *Genetică judiciară*, București, Centrul Tehnic-Editorial al Armatei, 2005.
SLĂVOIU, R., *Protecția penală a vieții private*, București, Universul Juridic, 2016.
SUIAN, M., *Metode speciale de supraveghere sau cercetare*, Solomon, 2021.
TANISLAV, E., *Ocrotirea penală a dreptului la intimitate*, RDP nr.3, București, ed. Monitorul Oficial, 1998.
UDROIU, M., *Drept penal. Partea specială. Sinteze și grile*, București, C.H. Beck, 2014.
UDROIU, M., *Fișe de drept penal. Partea specială*, București, Universul Juridic, 2014.
VASILU, A., TOADER, T. (coord.), *Explicațiile Noului Cod Penal*, București, Universul Juridic, 2015.

Autre langue

ABAIMOV, S., MARTELLINI, M., *Artificial Intelligence in Autonomous Weapon Systems*, in MARTELLINI, M., TRAPP R.,(dir.), *21st Century Prometheus*, Cham, Springer, 2020.
ABBOTT R., *Punishing Artificial Intelligence*, in: *The Reasonable Robot: Artificial Intelligence and the Law*, Cambridge University Press, 2020.
ABBOTT, R., *The Reasonable Computer: Disrupting the Paradigm of Tort Liability*, The George Washington Law Review, 2018.
ABD EL-LATIF A., A., et al., *Digital Forensics and Cyber Crime Investigation*, Boca Raton (FL), CRC Press, 2024.
AGUILERA-BARCHET, B., *From Kings to Monarchs: The Resurgence of Public Power in Late Medieval Europe*, Springer, 2015.
AL-KHWARIMI, M., *Algoritmi de numero Indorum,* éd. latine médiévale, s XII.
ALLEN A., *Genetic Privacy: Emerging Concepts and Values* Book Chapters, 83. Peen Law legal, 1997.
AMBOS, K., Article 25: *Individual Criminal Responsibility*, in TRIFFTERER, O., AMBOS, K. (dir.*), Rome Statute of the International Criminal Court: A Commentary*, 2e éd., Munich/Oxford/Baden-Baden, C.H. Beck/Hart/Nomos, 2011.
AMELUNG, K., *Grundsätzliches zur Freiwilligkeit der Einwilligung des Verletzten*, Neue Zeitschrift für Strafrecht (NStZ), 2006.
ASIMOV, I., *Runaround*, in *I, Robot*, Gnome Press, 1950.

ASIMOV, I., *The Complete Robot*, Doubleday, 1982.
BALKIN, J. M., *The Three Laws of Robotics in the Age of Big Data*, *Ohio State Law Journal*, vol. 78, 2017.
BARFIELD, W. (dir.), *The Cambridge Handbook of the Law of Algorithms*, Cambridge, Cambridge University Press, 2021.
BENE T., *L'intercettazione di comunicazioni*, Bari, Cacucci Editore, 2018.
BENNETT, C. J., RAAB, C. D., *The Governance of Privacy: Policy Instruments in Global Perspective*, Cambridge (MA), MIT Press, 2006.
BENNETT, C. J., *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca (NY), Cornell University Press, 1992.
BHATIA, R., (dir.), *Intelligent Systems and Applications. IntelliSys 2020*, Advances in Intelligent Systems and Computing, vol. 1250, Cham, Springer, 2021.
BIEGELMAN, M. T., *Identity Theft Handbook: Detection, Prevention, and Security,* Hoboken (NJ), John Wiley & Sons, 2009.
BOOLE, G., *An Investigation of the Laws of Thought on which are founded the Mathematical Theories of Logic and Probabilities*, London, Walton and Maberly, 1854.
BOSTROM, N., E. YUDKOWSKY, *The Ethics of Artificial Intelligence*, în R. V. YAMPOLSKIY, V.,R.,(dir.), *Artificial Intelligence Safety and Security*, New York, Chapman & Hall/CRC, 2018.
BOSTROM, N., *Superintelligence: Paths, Dangers, Strategies*, Oxford University Press, 2014.
BOYER, C. B., Merzbach, U.C., *A History of Mathematics*, 2e éd., New York, Wiley, 1991.
BRYSON, J., THEODOROU, A., *How Society Can Maintain Human-Centric Artificial Intelligence*, in M. TOIVONEN, E. SAARI (dir.), *Human-Centered Digitalization and Services*, *Translational System Sciences*, Cham, Springer, 2019.
CHESTERMAN, S., *From Ethics to Law: Why, When, and How to Regulate AI*, in D. J. GUNKEL(dir.), *The Handbook of the Ethics of AI*, Cheltenham, Edward Elgar Publishing, (à paraître) 2023.
CLAPP, J., *Windows into the Soul: Surveillance and Society in an Age of High Technology, by Gary T. Marx*, Law & Literature, vol. 30, 2018.
COCCOMINI, D. A., N. MESSINA, C. GENNARO, F. FALCHI, *Combining EfficientNet and Vision Transformers for Video Deepfake Detection*, in S. SCLAROFF et al. (dir.), Image Analysis and Processing – ICIAP 2022, Cham, Springer International Publishing, 2022.
COHEN, J., *Networks, Standards, and Network-and-Standard-Based Governance*, in K. Werbach (dir.), After the Digital Tornado: Networks, Algorithms, Humanity, Cambridge University Press, 2020.

COLE, S. A., *Suspect Identities: A History of Fingerprinting and Criminal Identification*, Harvard University Press, 2001.

COLEMAN, J. P. H., *AI and Our Understanding of Intelligence*, en ARAI K., KAPOOR S. (dir.), *Advances in Information and Communication*, vol. 2, FICC 2020, Advances in Intelligent Systems and Computing, vol. 1131, Cham, Springer, 2020.

COPPIN, B., *Artificial Intelligence Illuminated*, Jones and Bartlett Publishers, Sudbury, 2004.

DE LONDRAS F., DOODY J. (dir.), *The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism*, 1re éd., Abingdon, Routledge, 2015.

DELETANT, D., *Ceaușescu and the Securitate: Coercion and Dissent in Romania, 1965-1989*, Armonk (N.Y.), M. E. Sharpe, 1995.

DELSALLE, P., *Histoires de familles. Les registres paroissiaux et d'état civil, du Moyen Âge à nos jours*(1–), Presses universitaires de Franche-Comté, 2009.

DESABIE, J. Desabie, HAYOUN, M., *Le répertoire d'identification des personnes physiques*, in *Pour une histoire de la statistique*, Tome II : *Matériaux*, Paris, INSEE / Éditions Joëlle Affichard, 1987.

DRESSLER, J., *Cases and Materials on Criminal Law*, 6e éd., West Academic Publishing, 2007.

DREYFUS, H., *What Computers Can't Do. The Limits of Artificial Intelligence*, Cambridge (Mass.), MIT Press, 1972 (2e éd. 1992).

DUFF, R.A., *Legal Moralism and Public Wrongs*, en FERZAN, K.K., MORSE, S.J.(dir.), *Legal, Moral, and Metaphysical Truths: The Philosophy of Michael S. Moore*, Oxford, Oxford University Press, 2015.

DÜNKEL, F., *Electronic Monitoring – Some Critical Issues*, in C. Bijleveld et P. van der Laan (dir.), *Liber Amicorum Gerben Bruinsma*, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR), 2017.

ERIKSSON, A., J. PRATT, *In Defence of Scandinavian Exceptionalism*, in T. UGELVIK, J. DULLUM (dir.), *Penal Exceptionalism?: Nordic Prison Policy and Practice*, Abingdon (Oxon, Royaume-Uni), Routledge, 2012.

FINN, R., D. WRIGHT, M. FRIEDWALD, *Seven Types of Privacy,* in S. Gutwirth, R. Leenes, P. de Hert et Y. Poullet (dir.), *European Data Protection: Coming of Age,* Dordrecht, Springer, 2013.

FRENCH, R. M., *Subcognition and the Limits of the Turing Test* », Mind, vol. 99, n° 393, Oxford University Press, 1990.

GENDREAU, V. P. (dir.), Choosing Correctional Options That Work, Newbury Park (CA), Sage Publications, 1996.

GENDREAU, V. P. (dir.), *Choosing Correctional Options That Work*, Newbury Park (CA), Sage Publications, 1996.

HALLEVY, G., *When Robots Kill: Artificial Intelligence under Criminal Law*, Northeastern University Press, 2013.

HARRIS, M., K. HUGHES, *Privacy and Free Expression: Competing or Complementary Rights?*, in J. Lewis, P. Crick (ed.), *Media Law and Ethics in the 21st Century: Protecting Free Expression and Curbing Abuses*, Hart Publishing, 2014.

HARSHBARGER, D., *A Quiet Hero. A Novel of Resistance in WWII France*, Herndon (VA), Mascot Books, 2019.

HARVARD LAW REVIEW, *Cooperation or Resistance? The Role of Tech Companies in Government*, Harvard Law Review, vol. 131, n° 6, Harvard Law Review Association, 2018.

HOFFMANN-RIEM W., *Artificial Intelligence as a Challenge for Law and Regulation*, in WISCHMEYER T., RADEMACHER T. (dir.), *Regulating Artificial Intelligence*, Cham, Springer, 2020.

HOLDSWORTH, W. S., *A History of English Law,* London, Methuen, 1922.

HOLLAND, B. J., *Transnational Cybercrime: The Dark Web*, in : KHOSROW-POUR M. (dir.), *Encyclopedia of Criminal Activities and the Deep Web*, Hershey (PA), IGI Global, 2020.

KAUR, S., RANDHAWA, S., *Dark Web: A Web of Crimes,* Cham, Springer, 2020.

KNEPPER, P., YSTEHEDE, P. J.(dir.), *The Cesare Lombroso Handbook*, Routledge, Londres, 2013.

KURKI V. A., *A Theory of Legal Personhood*, Oxford University Press, 2019.

LEMLEY, M. A., CASEY B., Remedies for Robots, University of Chicago Law Review, vol. 86, 2019..

LÉVY, R., *Pardons and Amnesties as Policy Instruments in Contemporary France*, in M. TONRY (éd.), *Crime, Punishment, and Politics in Comparative Perspective*, Chicago University Press, 2007.

LIN P., ABNEY K., BEKEY G. A., *A body to kick, but still no soul to damn: legal perspectives on robotics*, in *Robot Ethics: The Ethical and Social Implications of Robotics*, MIT Press, 2012.

LUBIN, A., *We Only Spy on Foreigners: The Myth of a Universal Right to Privacy and the Practice of Foreign Mass Surveillance,* Chicago Journal of International Law, vol. 18, 2018.

LUHMANN, N., *Das Recht der Gesellschaft*, Francfort-sur-le-Main, Suhrkamp, 1993.

LYON D., *Surveillance After Snowden,* Polity, 2015.

MANTELERO, A., *Beyond Data. Human Rights, Ethical and Social Impact Assessment in AI*, The Hague, Springer–T.M.C. Asser Press, 2022.

MARELLI, L., TESTA G., VAN HOYWEGHEN I., *Big Tech Platforms in Health Research: Re-Purposing Big Data Governance in Light of the GDPR's Research Exemption,* Big Data & Society, vol. 8, n° 1, 2021.

MARX et al., *Marx and Engels Anthology*. vol.5, People's Publishing House, 2004.

MINSKY, M., *The Emotion Machine. Commonsense Thinking, Artificial Intelligence, and the Future of the Human Mind*, New York, Simon & Schuster, 2007.

MURRAY T. H., *Genetic Exceptionalism and 'Future Diaries': Is Genetic Information Different from Other Medical Information?*, in ROTHSTEIN M. A. (dir.), *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, Yale University Press, New Haven, 1997.

MÄKI, U.(éd.), et all., *Philosophy of Economics*, coll. « Handbook of the Philosophy of Science », Elsevier, 2012.

NATIONAL ARCHIVES (UK), *Domesday Book*, Londres, 2020.

NEISSER, U., *Cognitive Psychology*, Englewood Cliffs (NJ), Prentice Hall, 1967.

NELLIS M., *Standards and ethics in electronic monitoring: handbook for professionals responsible for the establishment and the use of electronic monitoring*, Council of Europe, 2015.

NELLIS M., *Surveillance, stigma and spatial constraint: the ethical challenges of electronic monitoring*, in *Electronically Monitored Punishment: International and Critical Perspectives*, éd. M. Nellis, K. Beyens, D. Kaminski, Routledge, 2013.

NEWELL A., SIMON, H.A., *Human Problem Solving*, Englewood Cliffs (NJ), Prentice-Hall, 1972.

NIKOLINAKOS N. T., *The Proposed Artificial Intelligence Act and Subsequent 'Compromise' Proposals: Commission, Council, Parliament ,* in : *EU Policy and Legal Framework for Artificial Intelligence, Robotics and Related Technologies* – The AI Act, vol. 53, Cham, Springer, 2023.

NISSENBAUM H., *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2010.

ÖMAN, S., *Implementing Data Protection in Law*, Scandinavian Studies in Law, vol. 47, 2004.

PARLAR, T., *Data Privacy and Security in the Metaverse*, in F. S. ESEN, H. TINMAZ, M. SINGH (dir.), *Metaverse*, Springer, 2023.

QUINN, G., DE PAOR A., BLANCK P.(dir.), *Genetic Discrimination: Transatlantic Perspectives on the Case for a European Level Legal Response*, London/New York, Routledge, 2014.

REGAN P. M., *Legislating Privacy: Technology, Social Values, and Public Policy*, Chapel Hill, University of North Carolina Press, 1995.

RICHARDS, N., *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, Oxford, Oxford University Press, 2015.

RIGGSBY, A., *Roman Law and the Legal World of the Romans*, Cambridge University Press, 2010.

RIVERA, R., *Release, Detain or Surveil: The Effects of Electronic Monitoring on Defendant Outcomes,* manuscrit inédit, Columbia University, 2023.

ROSENBLATT, F., *Principles of neurodynamics : perceptrons and the theory of brain mechanisms*, Spartan Books, 1962.

ROTHSTEIN M. A., *Protecting Privacy and Confidentiality in the Genetic Era*, Yale University Press, 1997.

ROTHSTEINR M. A. (dir.), *Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era*, Yale University Press, 1997.

ROTMAN, B., *Signifying Nothing: The Semiotics of Zero*, London, Macmillan, 1987.

ROYAKKERS, L., OLSTHOORN, P., *Military Robots and the Question of Responsibility*, International Journal of Technoethics, vol. 5, n° 1, 2014.

SCHABAS W., *Mens rea, actus reus, and the role of the State*, in *Unimaginable Atrocities: Justice, Politics, and Rights at the War Crimes Tribunals*, Oxford University Press, 2012.

SCHNEIER, B., *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York/London, W.W. Norton & Company, 2015.

SCHREINER, D., *Building iRIS: A Robotic Immune System*, in R. HÄHNLE, J. KNOOP, T. MARGARIA, D. SCHREINER, et B. STEFFEN (dir.), *Leveraging Applications of Formal Methods, Verification, and Validation. ISoLA 2011*, *Communications in Computer and Information Science*, vol. 336, Springer, 2012.

SOLOVE, D. J., *The Digital Person: Technology and Privacy in the Information Age*, New York University Press, 2004.

SOLOVE, D. J., *Understanding Privacy,* Cambridge (MA), Harvard University Press, 2008.

STALLINGS, W., *Cryptography and Network Security*, 7e éd., New York, Pearson, 2017.

STOBBS, G., *The Digital Millennium Copyright Act*, in *Multimedia Security Technologies for Digital Rights Management*, San Diego, Academic Press, 2006.

TULBING, E., *Episodic and Semantic Memory*, in TULVING, E, DONALDSON W.(dir.), *Organization of Memory*, New York, Academic Press, 1972.

TULVING, E., *Elements of Episodic Memory*, Oxford, Oxford University Press, 1983.

TURNER, J., *Robot Rules: Regulating Artificial Intelligence*, Cham, Springer, 2018.

VAN DEN HOVEN VAN GENDEREN, R., *Do We Need New Legal Personhood in the Age of Robots and AI?,* in M. CORRALES, M. FENWICK et N. FORGÓ (dir.), *Robotics, AI and the Future of Law. Perspectives in Law, Business and Innovation*, Singapore, Springer, 2018.
VAN DIJCK J., *Mediated Memories in the Digital Age*, Stanford, Stanford University Press, 2007.
VAN DIJCK, J., *The Culture of Connectivity: A Critical History of Social Media*, New York, Oxford Academic, 2013.
VAN RIJMENAM, M., *Privacy in the Age of AI: Risks, Challenges and Solutions,* The Digital Speaker, 2023.
VAN-ALSENOY, B., *National Data Protection Laws before 1980*, chapitre en,*Data Protection Law in the EU: Roles, Responsibilities and Liability*, KU Leuven Centre for IT & IP Law Series. Intersentia, 2019.
VENTRE D., GULLOT P., *Electronic Communication Interception Technologies and Issues of Power*, Wiley-ISTE, 2023.
WENNBERG, B., ÖRTENHED, K.(dir.), *Press Freedom 250 Years: Freedom of the Press and Public Access to Official Documents in Sweden and Finland – a living heritage from 1766*, Stockholm, The Riksdag of Sweden, 2018.
WESTIN, A. F., *Privacy and Freedom*, Washington and Lee Law Review, 1968.
ZUBOFF, S., *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, New York, PublicAffairs, 2019.

V. Referances extra-juridiques

Langue française

BOURGEOIS, M., TOUZANNE, B., *Les aéronefs civils télépilotés avec capteur: « drones de droit »*, CCE, n°12, 2015.
CADEC, K., PROULX, S., *Les représentations de l'amitié sur Facebook*, Communication [En ligne], vol. 33, n° 2, 2015.
CAZE-GAILLARDS., *Secret et citoyen – Les risques technologiques de l'information*, Entretiens de Nanterre, 1996.
CHATELLIER R., *Métavers: ce jeu dont qui sera le héros ?*, CNIL – LINC, 2022.
CHERIFI, Y., S. AMRANI, *Analyses ADN en Médecine-Légale: Revue Générale et Perspectives*, 1er Congrès National « Les conduites médico-légales en Anatomopathologie et Anthropologie », Académie Algérienne de Développement des Sciences Médico-Légales (AADSML), 2018.

CHNEIWEISS H., *Modification du génome : quels enjeux éthiques ?*, Sciences Sorbonne Université, 2021.
CLAEYS, A., VIALATTE, J.-S., *Les progrès de la génétique: vers une médecine de précision?*, Office parlementaire d'évaluation des choix scientifiques et technologiques, Paris, 2014.
DIGNST, A., *René Carmille (1886-1945) – La Résistance au bureau des statistiques* , Herodote.net, 2021.
Droit de propriété vs droit au respect du domicile, Dalloz Actu Étudiant, 2018.
GIRARDOT, C., *Comment enquêter sur les algorithmes?*, La Revue des médias, INA, 2017.
KLARSFELD, S, KLARSFELD, B., *Cercle de généalogie juive*, Bulletin, n° 23, 1990.
LAURENT, A., *La mort des médecins*, Les Tribunes de la Santé, n° 54, 2017.
LE GOFF, A., *Introduction au parcours de Philip Pettit*, Raisons politiques, vol. 43, n° 3, 2011.
MALZAC, P., *Les techniques de séquençage de nouvelle génération: enjeux éthiques en pratique clinique*, Laennec, vol. 64, n° 3, 2016.
MULIER, T., *Constitutionnaliser le droit d'accès à Internet : (nouvel) Eldorado du Navigateur 2.0?*, Dalloz Actualité, 2023.

Langue roumaine

BIBLIA, *Biblia sau Sfânta Scriptură,* versiunea Sinodală, Editura Institutului Biblic și de Misiune Ortodoxă, 1988.
BIRD, L., *Internet – Ghid complet de utilizare,* Corint, 2004.
BONCU, Ș., *Psihologie socială, cursul 16 – Deindividualizarea*, Polirom, 2004.
BUDĂI, R., *Unele aspecte practice privind metodele speciale de supraveghere sau cercetare*, articol, Juridice, 2020.
CIOBOTARU, I., *Anonim și autentificat: identitate digitală pe internetul deschis*, Medium, 2020.
MILL, J. S., *Despre libertate*, 3e éd., Humanitas, 2014.
PATRICIU, V. V., *Criptografia și securitatea rețelelor de calculatoare*, ed. Tehnică, 1994.
PLATON, *Phaidon*, în *Opere*, vol. IV, trad. în limba română de P. Creția, București, Ed. Științifică și Enciclopedică, 1983.
PUBLILIUS S., *Maxime*, trad. C. Mureșan, Ed. Cartimplex, 2002.
SFETCU, N., *Biopolitica în pandemia COVID-19*, SetThings, 2020.
TEC, L.M., « *Homo Numericus* : *reflecții și interogații* », Palatul de Justiție, 2025.
VOINEA, V. C., *Tenebrele rețelei : Deep Web și Dark Web*, Revista Intelligence, 2022.

Autre langue

ABELSON, H., et al., *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, Cambridge (MA), MIT Press, 1997.

ANDREJEVIC, M., *Infoglut: How Too Much Information Is Changing the Way We Think and Know*, New York/London, Routledge, 2013.

ARORA, N., ZINOLABEDINI, D., *The ethical implications of the 2018 Facebook-Cambridge Analytica data scandal*, The University of Texas at Austin (working paper), 2019.

AYME, S., *La médecine prédictive vingt ans après*, Actualité et Dossier en Santé Publique, n° 100, 2017.

BADA, M., NURSE, J. R. C., *Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)*, Information & Computer Security, vol. 27, n° 3, 2019, p. 393-410.

BAILY, C., et al., *Apple, Inc.: Data Privacy and a Request from the FBI*, SAGE Business Cases, 2017.

BAROCAS, S., ISSENBAUM H., *Big Data's End Run around Anonymity and Consent*, Book of Anonymity, 2014.

BENTHAM, J., *The Panopticon Writings*, éd. M. Bozovic, London/New York, Verso, 1995.

BLACK, E., *IBM et l'Holocauste. L'alliance stratégique entre l'Allemagne nazie et la plus puissante multinationale américaine*, Paris, Robert Laffont, 2001.

BLOMBERG, J., *Twitter and Facebook Analysis: It's Not Just for Marketing Anymore*, *SAS Global Forum*, vol. 309, Denver (CO), 2012.

BONTA, J., ANDREWS D.,A., *The Psychology of Criminal Conduct*, 6e éd., London/New York, Routledge, 2017.

CALHOUN, C., *Habermas and the Public Sphere*, Cambridge (MA)/London, The MIT Press, 1992.

CHARTIER, R., *The Cultural Origins of the French Revolution*, Princeton University Press, 1991.

CHOPRA, S., WHITE, L., *Artificial Agents: Personhood in Law and Philosophy*, working paper, 2004.

COPELAND, R., S. E. NEEDLEMAN, *Google's Project Nightingale Triggers Federal Inquiry*, The Wall Street Journal, 2019.

COURSERA STAFF, *4 Types of AI: Getting to Know Artificial Intelligence*, Coursera, 2024.

COURSERA STAFF, *What Is Artificial Intelligence? Definition, Uses, and Types*, Coursera, 2024.

COVER, R., *Digital Surveillance, Archives, and Google Earth Identities in/of the Digital World*, in R. Cover (dir.), *Digital Identities*, San Diego, Academic Press, 2016, p. 243-265.

CREWE, G., *How Algorithms Shape Our Online World*, Oxford Open Learning, 2023.
CULP, J., *Democratic Citizenship Education in Digitized Societies: A Habermasian Approach*, *Educational Theory*, vol. 73, n° 2, Wiley-Blackwell, 2023, p. 178-203.
D'AMORE-MCKIM SCHOOL OF BUSINESS, *How Multinational Companies Break the Rules and Why It Matters*, Northeastern University, 2023.
DAVIS, A., *A History of Hacking*, The Institut, 2015.
DELEV Z., *The complex relationship between GDPR and blockchain: ensuring compliance in the decentralized landscape*, GDPR Local Blog, 2024.
DEVELAKI, M., *Trustworthiness of Science in Debate: Challenges, Responses, and Implications*, Science & Education, vol. 31, 2022, p. 1181-1208.
DIAB, D. L., PUI S.Y., YANKELEVICH M., HIGHHOUSE S., *Lay Perceptions of Selection Decision Aids in US and Non-US Samples*, International Journal of Selection and Assessment, vol. 19, n° 3, 2011, p. 209-216.
DODDS, E. R., *The Greeks and the Irrational*, Berkeley, University of California Press, 2004.
DUBOV A., *Ethics of Digital Contact Tracing to Contain the COVID-19 Pandemic*, Institute for Health Policy Leadership, 2021.
EKELUND, R., TOLLISON R., *Politicized Economies: Monarchy, Monopoly, and Mercantilism*, Texas A&M Universiry Press, 1997.
ENCYCLOPAEDIA BRITANNICA (dir.), *Deep Blue*, *Encyclopaedia Britannica*, 2024.
ENCYCLOPAEDIA BRITANNICA (dir.), *Napoleonic Code*, *Encyclopaedia Britannica*, 2024.
ENCYCLOPAEDIA BRITANNICA (dir.), *Publilius Syrus*, *Encyclopaedia Britannica*, 2024.
ENCYCLOPAEDIA BRITANNICA, *PRISM | United States Surveillance Program*, Encyclopaedia Britannica, 21 octobre 2024.
ENCYCLOPAEDIA BRITANNICA*, Al-Khwārizmī*, Encyclopædia Britannica
ENCYCLOPAEDIA BRITANNICA (s.d.), *Pascaline*, Encyclopædia Britannica Online.
FETZER, J. H., *What is Artificial Intelligence?*, in *Artificial Intelligence: Its Scope and Limits*, *Studies in Cognitive Systems*, vol. 4, Dordrecht, Springer, 1990.
GAMBÍN, Á. F., A. YAZIDI, A. VASILAKOS, *Deepfakes: Current and Future Trends*, Artificial Intelligence Review, vol. 57, 2024.
GANDOMI, A., M. HAIDER, *Beyond the Hype: Big Data Concepts, Methods, and Analytics*, International Journal of Information Management, vol. 35, n° 2, 2015, p. 137-144.
GANNON, C., et al., *Child Sexual Abuse Material on the Darknet*, Forensische Psychiatrie Psychologie Kriminologie, vol. 17, Springer, 2023, p. 353-365.

GARDINER, M., *Wild Publics and Grotesque Symposiums: Habermas and Bakhtin on Dialogue, Everyday Life and the Public Sphere*, The Sociological Review, vol.52, Sage Publications, 2004.

GELLER, L., J. ALPER, P. BILLINGS, C. BARASH, J. BECKWITH et M. NATOWICZ, *Individual, Family, and Societal Dimensions of Genetic Discrimination: A Case Study Analysis*, Science and Engineering Ethics, vol. 2, Springer, 1996, p. 71-88.

GENETIC ALLIANCE et NEW YORK–MID-ATLANTIC CONSORTIUM, *Understanding Genetics: A New York, Mid-Atlantic Guide for Patients and Health Professionals*, Bethesda (MD), 2009.

GENT, E., *Lessons From a Second Life: Before Meta, Philip Rosedale Created an Online Universe*, IEEE Spectrum, vol. 59, n° 1, 2022.

GERGURI, D., *Cheapfakes*, in A. Nai, M. Grömping et D. Wirz (dir.), *Elgar Encyclopaedia of Political Communication*, Cheltenham, Edward Elgar Publishing, 2025.

GREENWALD, G., *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, New York, Metropolitan Books, 2014.

HAN, J., et al., *Data Mining: Concepts and Techniques*, Amsterdam, Elsevier, 2011.

HARARI, Y.N., *21 Lessons for the 21st Century*, London, Penguin Books, 2018.

HARARI, Y.N., *Nexus - Scurta istorie a retelelor informationale din epoca de piatra pana la IA*, Editura Polirom, Iași, 2024.

HICKS, R. D., *Aristotle De Anima with Translation, Introduction, and Notes*, Cambridge University Press, 1907.

ICHBIAH, D., *Robots: From Science Fiction to Technological Revolution*, Choice, vol. 43, 2005.

JAIMAN, A., *Deepfakes & Synthetic Media: Humanity at the Edge of an Uncanny Valley*, CRC Press/Routledge, 2022.

JUST, S. N., *The Digital Transformation of the Public Sphere*, in *Controversial Encounters in the Age of Algorithms: How Digital Technologies Are Stifling Public Debate and What to Do About It*, 1re éd., Bristol University Press, 2025.

KALPOKAS, I., *Call for Papers – Synthetic Media and Synthetic Reality: From Deepfakes to Virtual Worlds*, ResearchGate, 2020.

KAPILA, M., *The Long Shadow of COVID-19*, in Pachauri S., Pachauri A.(dir.), *Global Perspectives of COVID-19 Pandemic on Health, Education, and Role of Media*, Cham, Springer Nature, 2023, p. 177-192.

KASPAROV, G., *Deep Thinking: Where Machine Intelligence Ends and Human Creativity Begins*, New York PublicAffairs, 2017.

KOSELLECK, R., *Critique and Crisis: Enlightenment and the Pathogenesis of Modern Society*, Cambridge (MA), MIT Press, 1988.

KREMLING, J., SHARP PARKER A. M., *Cyberspace, Cybersecurity, and Cybercrime*, Thousand Oaks (CA), SAGE Publications, 2017.

KROENER, I., NEYLAND D., *New Technologies, Security and Surveillance*, London/New York, Routledge, 2012.

KURAKU, C., GOLLANGI, H.,K., SUNKARA. J.R., *Biometric Authentication In Digital Payments*, *Utilizing AI and big data for real-time security and efficiency*, Educational Administration Theory and Practice journal, 2020.

KURZWEIL, R., *The Singularity Is Nearer: When We Merge with AI*, London/New York, Penguin Books, 2024.

KWITONDA, J. C., CAMPBELL S., *"The Medium is the Massage/Message": Functions of Synthetic Media in Sense-Making Conditions*, in K. Langmia(dir.), *Black Communication in the Age of Disinformation*, Cham, Palgrave Macmillan, 2023.

LANDAU, S., *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, Cambridge (MA), MIT Press, 2011.

LEVINE, P., A. BASHFORD, *Introduction: Eugenics and the Modern World*, Oxford University Press, 2010.

LEVY, S., *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*, London/New York, Penguin, 2001.

LIN, P., ABNEY K., BEKEY G., *Robots in War: Issues of Risk and Ethics*, Heidelberg, AKA Verlag, 2009.

LUDLOW, P., WALLACE M., *The Second Life Herald: The Virtual Tabloid That Witnessed the Dawn of the Metaverse*, MIT Press, 2007.

LYON, D., *Surveillance Studies: An Overview*, Polity Press, 2007.

LYON, D., *The Culture of Surveillance: Watching as a Way of Life*, Polity Press, 2018.

MADDEN, M., *Privacy, Security, and Digital Inequality*, rapport, Data & Society Research Institute New York, 2017.

MANZOTTI, R., *Why Is There Something Rather Than Nothing?,* Philosophy Now, n° 125, 2018.

MARSHALL, T., *The Age of Walls: How Barriers Between Nations Are Changing Our World*, Scribner Book Company, 2019.

MARX, G. T., *What's New About the New Surveillance?*, Surveillance & Society, vol. 1, n° 1, 2002.

MARX, G. T., *Windows into the Soul: Surveillance and Society in an Age of High Technology*, University of Chicago Press, 2016.
MAYER, M., R. HAVERKAMP et R. LEVY (dir.), *Will Electronic Monitoring Have a Future in Europe*, Freiburg, Max Planck Institute, 2003.
MAYER-SCHÖNBERGER, V., K. CUKIER, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Boston/New York, Houghton Mifflin Harcourt, 2013.
MCAFEE, A., et al., *Big Data: The Management Revolution*, Harvard Business Review, vol. 90, n° 10, 2012.
MCKENNA, N. S., *Secret Life of Oscar Wilde*, London, Arrow, 2024.
MERLEAU-PONTY, M., *Phenomenology of Perception*, London/New York, Routledge, 2013.
MISRA, S., et al., *Security Challenges and Approaches in Internet of Things*, *Springer Briefs in Electrical and Computer Engineering*, Cham, Springer, 2016.
NAKAMOTO, S., *Nakamoto's Blockchain Proposal*, ResearchGate, 2024.
NORRIS, C., *The Success of Failure: Accounting for the Global Growth of CCTV*, in K. Ball, K. D. Haggerty et D. Lyon (dir.), Routledge Handbook of Surveillance Studies, London/New York, Routledge, 2012.
O'NEIL, C., *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, New York, Crown, 2016.
OHLHAVER, P., WEYL E. G., BUTERIN V., *Decentralized Society: Finding Web3's Soul*, white paper, 2022.
OPPY, G., DOWE D., *The Turing Test*, in E. N. Zalta (dir.), *The Stanford Encyclopedia of Philosophy*, Stanford University, 2021.
PADHY, N. P., *Artificial Intelligence and Intelligent Systems*, Oxford University Press, 2005.
PARIENTY, A., *Apple contre le FBI : les dessous d'un bras de fer*, Alternatives économiques, n° 356, 2016.
PERSILY, N., J. A. TUCKER (dir.), *Social Media and Democracy: The State of the Field, Prospects for Reform*, Cambridge University Press, 2020.
PHILLIPS, W., R. M. MILNER, *The Ambivalent Internet: Mischief, Oddity, and Antagonism Online*, Cambridge, Polity, 2017.
POTZ, M., *Theocracies as Political Systems*, Political Science of Religion, 2019.
RAYHAN, S., *AI Superintelligence and Human Existence: A Comprehensive Analysis of Ethical, Societal, and Security Implications*, preprint, 2023.
RONE, J., *Beyond Brexit? Public Participation in Decision-Making on Campaign Data During and After Referendum Campaigns*, Media and Communication, 2023.

RUSSELL, S. J., NORVIG, P., *Artificial Intelligence: A Modern Approach*, 4e éd., New York, Pearson, 2022.

SCARIA, B., *The Importance of a National Digital Identity System*, ISACA Journal, 2022.

SCHOEMAN, F. D., *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, 1984.

SHAMPO, M. A., KYLE, R.A., *Bernard Kouchner — Founder of Doctors Without Borders*, Mayo Clinic Proceedings, vol. 86f, n°1, e6, 2011.

SMITH, A., *The Theory of Moral Sentiments*, ed. K. Haakonssen, Cambridge University Press, 2002.

SMITH, R. E., *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth Rock to the Internet*, Harvard Law Review, vol. 94, 1981.

STROLL A., MARTINICH A. P., *Epistemology ,* Encyclopedia Britannica, 2024.

SUGG, D., L. MOORE, P. HOWARD, *Electronic Monitoring and Offending Behaviour – Reconviction Results for the Second Year of Trials of Curfew Orders*, Home Office Online Report, n° 59/04, 2001.

The Napoleon Code, Lumen Learning, 2024.

THOMAS, P. D. G., *Wilkes, John (1725–1797), Politician*, Oxford Dictionary of National Biography, 2004.

VAN ES, K., M. T. SCHÄFER (dir.), *The Datafied Society. Studying Culture through Data*, , Amsterdam University Press, 2017.

VANHAELEMEESCH, D., T. VANDER BEKEN, *Electronic Monitoring: Convicts' Experiences in Belgium*, in M. Cools et al. (dir.), *Social Conflicts, Citizens and Policing*, vol. 6, Anvers, Maklu, 2012.

WALSH J., *Kevin Mitnick, founder of Mitnick Security*, EBSCO Knowledge Advantage, 2024.

WEINGAST, B. R., *Adam Smith's Industrial Organization of Religion: Explaining the Medieval Church's Monopoly and Its Breakdown in the Reformation*, Economic History eJournal, 2015.

WEST, F., *The Colonial History of the Norman Conquest*, History, vol. 84, 1999.

WILLS, M., *WWII and the First Ethical Hacker*, JSTOR Daily, 2017.

WILSON, P. H., *New Approaches under the Old Regime*, in *Early Modern Military History*, London, Palgrave, 2004.

WINKEL, C., *The King and His Army: A New Perspective on the Military in 18th Century Brandenburg-Prussia*, International Journal of Military History and Historiography, 2019.

VI. Articles scientifiques, Sources juridiques

ABBAS, F., TAEIHAGH, A., *Unmasking Deepfakes: A Systematic Review of Deepfake Detection and Generation Techniques Using Artificial Intelligence*, *Expert Systems with Applications*, Elsevier Ltd, vol. 252, part B, 2024.

ABBOTT, R. B., SARCH, A.F., *Punishing Artificial Intelligence: Legal Fiction or Science Fiction*, UC Davis Law Review, vol. 53, 2019.

ABBOTT, R.B., *The Reasonable Computer: Disrupting the Paradigm of Tort Liability*, The George Washington Law Review, 2018.

ABRAHAMS, E., GINSBURG,G.S, SILVER, M, *The Personalized Medicine Coalition: Goals and Strategies*, American Journal of Pharmacogenomics, vol. 5, n° 6, 2005.

ABRAMSON, Y., BARAM G., *Saving Face in the Cyberspace: Responses to Public Cyber Intrusions in the Gulf*, Contemporary Security Policy, vol. 45, n° 2, 2023.

ABRUSE-RIOU C., *Filiation: généralités – notion de filiation*, Dalloz, 2009, ac. 2023.

ACQUISTI, A., BRANDIMARTE, L., LOEWENSTEIN, G., *Privacy and human behavior in the age of information*, Science, vol. 347, n° 6221, 2015.

ADAM, P., *Vie personnelle/vie professionnelle : une distinction en voie de dissolution ? (petit exercice de jardinage juridique*), Le Droit Ouvrier, vol. 780(7), 2013.

ADAMS, A., S. HOSELL, K. MURATA, *Following Snowden, German Uncertainty About Monitoring*, Journal of Information, Communication and Ethics in Society, vol. 15, 2017.

ADDA, H., *IA et vidéoprotection : quelles solutions pour les collectivités ?,* AJ Collectivités Territoriales (AJCT), 2025.

AEBI M. F., MOLNAR L., COCCO E., *Probation and prisons in Europe, 2023: key findings of the SPACE reports*, Lausanne, 2023.

AIMÉ, I., BERGER-REMY, F., LAPORTE, M.-E., *The brand, the persona and the algorithm : How datafication is reconfiguring marketing work,* Journal of Business Research, vol. 145, 2022.

AKBANOV, M., VASSILAKIS, V.G., LOGOTHETIS, M.D., *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention, and Propagation Mechanisms*, Journal of Telecommunications and Information Technology, n° 1, 2019.

AKDENIZ Y., TAYLOR N., WALKER C., *Regulation of Investigatory Powers Act 2000 (1): BigBrother.gov.uk: State surveillance in the age of information and rights*, Criminal Law Review, 2001.

AL ABDWANI, T., *The Rise of Thinking Machines: A Review of Artificial Intelligence in Contemporary Communication*, Journal of Business Communication & Technology, vol. 2, 2024.

AL QATAWNEH, I., MOUSSA, A., HASWA, M., JAFFAL, Z., BARAFI, J., *Artificial Intelligence Crimes*, Academic Journal of Interdisciplinary Studies, vol. 12, 2023.

ALAM, T., *A Reliable Communication Framework and Its Use in Internet of Things (IoT)*, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 3, n° 5, 2018.

ALHMIEDAT, T., ABOROKBAH, M., *Social Distance Monitoring Approach Wearable Smart Tags*, Electronics, 2021.

ALJANABI, Y. I., et al., *Detect and Mitigate Blockchain-Based DDoS Attacks Using Machine Learning and Smart Contracts*, Informatica, vol. 46, n° 7, 2022.

ALLHOFF, F., HENSCHKE, A., *The Internet of Things: Foundational Ethical Issues*, Internet of Things, vols. 1–2, 2018.

ÁLVAREZ, C., EL EMAM, K., *A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques*, International Data Privacy Law, vol. 5, n° 1, 2015.

ALVARO, C. et all., *Multinationals' misbehavior*, Journal of World Business, vol. 56, Issue 5, 2021.

AMANKWAA, A. O., MCCARTNEY, C., *The UK National DNA Database: Implementation of the Protection of Freedoms Act 2012*, Forensic Science International, vol. 284, 2018.

AMANKWAA, A., MCCARTNEY, C., *Gaughran vs the UK and Public Acceptability of Forensic Biometrics Retention*, Science & Justice, vol. 60, n° 3, 2020.

AMAR, A. R., *Fourth Amendment First Principles*, Harvard Law Review, vol. 107, 1994.

ANDERSON, S. L., *Asimov's Three Laws of Robotics and Machine Metaethics*, AI & Society, vol. 22, 2008.

ANDORNO, R., *The Oviedo Convention: A European Legal Framework at the Intersection of Human Rights and Health Law*, Journal of International Biotechnology Law, vol. 2, n° 4, 2005.

ANDRESEN, S. L., *John McCarthy: Father of AI*, IEEE Intelligent Systems, vol. 17, 2002.

ARCHER, F., *La criminologie confrontée aux nouvelles technologies*, Dalloz IP/IT, n° 11, 2024.

ARNAUD, M., *Authentification, identification et tiers de confiance*, Hermès, La Revue, 53(1), 2009.

ARONSON, S. J., REHM, H.L., *Building the Foundation for Genomics in Precision Medicine*, Nature, vol. 526, n° 7573, 2015.

ARTEAGA, C., *Parental Incarceration and Children's Educational Attainment*, The Review of Economics and Statistics, vol. 105, n° 6, 2023.

Assignation à résidence sous surveillance électronique (ARSE), Dalloz Actualité, 2021.

ATIAS, M., LINOTTE, D., *Le mythe de l'adaptation du droit au fait*, Recueil Dalloz, Chronique et législation, 1977, chron. XXXIV.

AUTIER E*., CEDH : absence de précédent jurisprudentiel et épuisement des voies de recours internes,* Dalloz Actualité, 2017.

AUTIER, E., *Cybercriminalité: Bruxelles Propose une Nouvelle Directive*, Dalloz, 2017.

AYVAZ, U., GÜRÜLER, H., DEVRIM, M. O., *Use of Facial Emotion Recognition in E-Learning Systems*, Information Technologies and Learning Tools, vol. 60, n° 4, 2017.

AZUBUIKE, C. F., *Cyber Security and International Conflicts: An Analysis of State-Sponsored Cyber Attacks*, Nnamdi Azikiwe Journal of Political Science, vol. 9, n° 1, 2023.

BACHMAIER WINTER, L., *Section III – Procédure pénale. Société de l'information et droit pénal. Rapport général,* Revue internationale de droit pénal, vol. 85(1), 2014.

BADA, M., NURSE, J.R.C., *Profiling the Cybercriminal: A Systematic Review of Research*, 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA), Dublin, 2021.

BADINTER R., *La protection de la vie privée contre l'écoute électronique clandestine*, Semaine Juridique, 1971, chronique 2435.

BADINTER R., *Le droit au respect de la vie privée*, JCP, 1968.

BAILENSON, J., *Protecting Non-Verbal Data Tracked in Virtual Reality*, JAMA Pediatrics, 2018.

BALDI P., HORNIK K., *Neural Networks and Principal Component Analysis: Learning from Examples without Local Minima*, Neural Networks, vol. 2, n° 1, 1989.

BALES, W., et al., *A Quantitative and Qualitative Assessment of Electronic Monitoring*, Washington, DC, National Institute of Justice, 2010.

BALKIN, J. M., *Information Fiduciaries and the First Amendment*, UC Davis Law Review, vol. 49, n° 4, 2016 (forthcoming).

BARDIN, M., *Le droit d'accès à internet: entre « choix de société » et protection des droits existants*, RLDI, n° 91, 2013.

BARRAUD, B., *Le droit en datas : comment l'intelligence artificielle redessine le monde juridique*, Revue Lamy Droit de l'Immatériel, 2019.

BASU T., *The metaverse has a groping problem already*, MIT Technology Review, 2021.

BAUDELIN A*., Chronique pénale du prélèvement d'ADN et du fichier national automatisé des empreintes génétiques (FNAEG),* en ligne, 2020.

BEAUDOUIN, V., *Comment s'élabore la mémoire collective sur le web ? Une analyse qualitative et quantitative des pratiques d'écriture en ligne de la mémoire de la Grande Guerre*, Réseaux, vol.214-215(2), 2019.

BEAUSSONIE, G., *L'essor des lois pénales inconstitutionnelles*, RSC, 2020.

BEAUSSONIE, G., *Les Bornes de la Personnalité Juridique en Droit Pénal*, Dr. Fam., Doss. 5, 2012.

BÉCOURT, D**.,** *Réflexions sur le projet de loi relatif à la protection de la vie privée*. Gazette du Palais, 1970.

BEECHER-MONAS, E., GARCIA-RILL, *Actus Reus, Mens Rea, and Brain Science: What Do Volition and Intent Really Mean?*, Kentucky Law Journal, 2017.

BEIGNIER B., *La vie privée: un droit des vivants*, Recueil Dalloz, 2000.

BELUR, J., et al., *A Systematic Review of the Effectiveness of the Electronic Monitoring of Offenders*, Journal of Criminal Justice, vol. 60, 2020.

BENABOU, V. L., *L'extension du domaine de la donnée*, LEGICOM, 59(2), 2017.

BENHAMOU, B., *Les conséquences démocratiques des mutations de la surveillance numérique,* Cahiers français, vol. 439(3), 2024.

BENJAMIN, G., *Privacy as a Cultural Phenomenon*, Journal of Media Critiques, vol. 3, 2017.

BENNETT, W. L., LIVINGSTON, S., *The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions*, European Journal of Communication, vol. 33, n° 2, 2018.

BENOIT N., *La mise en œuvre de la responsabilité des prestataires d'hébergement toujours incertaine*, Légipresse, 2015.

BENSAMOUN, A., LOISEAU, G**.**, *L'intégration de l'intelligence artificielle dans l'ordre juridique en droit commun : questions de temps*, Dalloz IP/IT, avril 2017.

BENSAMOUN, A., LOISEAU, G., *La gestion des risques de l'intelligence artificielle. De l'éthique à la responsabilité*, La Semaine juridique. Édition générale, 2017.

BENSOUSSAN, A., *Droit des robots: science-fiction ou anticipation ?*, Recueil Dalloz, n° 28, 2015.

BENSOUSSAN, A., *Vers un droit de propriété des données personnelles*, Annales des Mines – Réalités industrielles, vol. 3, 2022.

BERGEAT, M., BLUM, D., CUPPENS, N. et al., *Comment anonymiser les données : un panorama non exhaustif des méthodes d'anonymisation*, Dossiers Solidarité et Santé. Données de santé : anonymat et risque de ré-identification, n° 64, 2015.

BERNATCHEZ, S., *La Vente des Données Génétiques: Entre Confidentialité et Commerce*, Journal de Droit Médical et Éthique, vol. 4, n° 2, 2021.

BERRY, E., KAPUR, P., WILLIAMS, N., et al., *The use of a wearable camera, SenseCam, as a pictorial diary to improve autobiographical memory in a patient with limbic encephalitis*, Memory, vol. 15, n° 5, 2007.

BERTHIER, C., *Droit à l'image et la protection des photos*, fiche pratique n° FP-628046, Lexis 360 Intelligence, 2024.

BERTHOUD, G*., L'horizon d'une surveillance omniprésente* ?, Revue européenne des sciences sociales, XL(2), 2002.

BERTHOUD, G., *L'horizon d'une surveillance omniprésente ?*, Revue européenne des sciences sociales, XL(2), 2002.

BERTRAND, L., DE FREITAS PEREIRA, M., MARION, J. Y., *Les capacités offensives de l'intelligence artificielle dans le cyberespace*, Études françaises de renseignement et de cyber, 4(1), 2025.

BEYENS, K., ROOSEN, M., *Electronic Monitoring and Reintegration in Belgium*, European Journal of Probation, vol. 9, n° 1, 2017.

BHUSHAN, K., GUPTA, B.,B., *Distributed Denial of Service (DDoS) Attack Mitigation in Software Defined Network (SDN)-Based Cloud Computing Environment*, Journal of Ambient Intelligence and Humanized Computing, vol. 10, n° 5, 2019.

BIEVER C., *ChatGPT broke the Turing test - the race is on for new ways to assess AI,* Nature, 2023.

BISSON, T., *Cultures of Power: Lordship, Status, and Process in Twelfth-Century Europe*, Law and History Review, vol. 16, 1995.

BLACK, J.S., *Privacy, Ancient and Modern*, Academica, 2014.

BLAUTH, T., GSTREIN, O., ZWITTER, A., *Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI*, IEEE Access, vol. 10, 2022.

BLAYA, C., *Cyberviolence, cyberharcèlement et cyberhaine : conséquences et facteurs de protection*, Le Journal des psychologues, 382(10), 2020.

BLISSON, L., *Petits vices et grandes vertus du chiffrement*, Délibérée, 7(2), 2019.

BOACNĂ C., *Doctoriale 2024: Dezinformarea prin intermediul rețelelor de socializare – o provocare pentru dreptul francez în context european*, 2024.

BOËNISCH, G., *Josephe Pascal, La société immédiate*, Paris, Calmann-Lévy, Presses universitaires de Lorraine, n° 14, 2008.

BOENISCH, G., *Pascal Josèphe, La société immédiate,* Questions de communication, 2008.

BONNEVILLE P., GÄNSER C., ILJIC A., *Chronique de Jurisprudence de la CJUE – Enregistrement des Données Biométriques et Génétiques*, AJDA, 2023.

BONTA, J., WALLACE-CAPRETTA, S., ROONEY, S., *A Quasi-Experimental Evaluation of an Intensive Rehabilitation Supervision Program*, Criminal Justice and Behavior, vol. 27, n° 3, 2000.

BORRY, P., et al., *Legislation on Direct-to-Consumer Genetic Testing in Seven European Countries*, European Journal of Human Genetics, vol. 20, 2012, p. 715-721.

BOSSAN J., *La Protection de la Représentation à l'Ère du Numérique et du Deepfake : Le Délit de Montage Version 2.0*, Légipresse, 2024.

BOTÉ-VERICAD, J.-J., TÉRMENS, M., *Reusing Data: Technical and Ethical Challenges*, DESIDOC Journal of Library & Information Technology, vol. 39, n° 6, 2019.

BOUCHET M., *Décryptage et analyse de la loi du 30 juillet 2020 visant à protéger les victimes de violences conjugales,* La lettre juridique*,* 2020*.*

BOURCIER, D., DE FILIPPI, P., *Transparence des algorithmes face à l'open data : quel statut pour les données d'apprentissage ?,* Revue française d'administration publique, 167(3), 2018.

BOUTIN, C., *Le droit à l'oubli numérique : entre mémoire et identité*, Revue Lamy Droit de l'immatériel, n° 129, 2016.

BRADNER, S., *The End of End-to-End Security? [Internet Security]*, IEEE Security & Privacy, vol. 4, n° 2, 2006.

BRENNER, S. W., *Cybercrime Jurisdiction*, Crime, Law and Social Change, vol. 46, n° 4-5, 2006.

BRENNER, S. W., *The Trojan Horse Defense in Cybercrime Cases*, Santa Clara Computer & High Technology Law Journal, vol. 21, 2004.

BROADHEAD, S., *The Contemporary Cybercrime Ecosystem: A Multi-disciplinary Overview of the State of Affairs and Developments*, Computer Law & Security Review, vol. 34, 2018.

BROADHURST R., et al., *Illicit firearms and other weapons on darknet markets*, Australian Institute of Criminology, 2021.

BROSCH, A., *Sharenting – Why Do Parents Violate Their Children's Privacy?*, The New Educational Review, vol. 54, 2018.

BROWN, T. B., et al., *Language Models are Few-Shot Learners*, ArXiv, 2005.

BROWNE, K., *Who (or What) Is an AI Artist?*, Leonardo, vol. 55, n° 2, 2022.

BRUGUIÈRE, J.-M., DELTORN, J.-M., *Intelligences artificielles génératives. Y a-t-il exploitation des œuvres, au sens du droit d'auteur ? N'y aurait-il pas d'autres modèles à considérer ?*, Recueil Dalloz, 2023.

BRUGUIÈRE, J.-M., *La protection de l'entreprise sur les réseaux sociaux*, JurisClasseur Communication, Fasc. 620, 2022.

BRUNAUX, G., *Réseaux sociaux et professionnels du droit: le risque disciplinaire*, Dalloz IP/IT, 2019.

BRUNDAGE, M., *Taking Superintelligence Seriously: Superintelligence: Paths, Dangers, Strategies by Nick Bostrom*, Futures, vol. 72, 2015.

BRUNON-ERNST, A., *Les métamorphoses panoptiques : de Foucault à Bentham*, Cahiers critiques de philosophie, 4(2), 2017.

BRYSON, J. J., DIAMANTIS, M.E., GRANT, T.D., *Of, For, and By the People: The Legal Lacuna of Synthetic Persons*, Artificial Intelligence and Law, vol. 25, 2017.

BRYSON, J., THEODOROU, A., *How Society Should Regulate Autonomous Technologies: A Framework for Legal Reforms*, European Journal of Technology and Ethics, vol. 14, n°1, 2018.

BUBLITZ, C., *The Body of Law: Boundaries, Extensions, and the Human Right to Physical Integrity in the Biotechnical Age*, Journal of Law and the Biosciences, vol. 9, n° 2, 2022.

BUCHER, A., BLAZEK, E.S., SYMONS, C.T., *How Are Machine Learning and Artificial Intelligence Used in Digital Behavior Change Interventions? A Scoping Review*, Mayo Clinic Proceedings: Digital Health, vol. 2, n° 3, 2024.

BULLICH, V., CLAVIER, V., *Production des données, "production de la société". Les Big Data et algorithmes au regard des sciences de l'information et de la communication*, Les Enjeux de l'information et de la communication, vol. 19/2(2), 2018.

BUNGERFELDT, J., *Old and New Uses of Electronic Monitoring in Sweden*, Crime and Justice Matters (CJM), n° 95, 2014.

BUREAU, D., MOLFESSIS, N**.**, *L'asphyxie doctrinale*, in *Études offertes à Bruno Oppetit*, Paris, Litec, 2009.

BURGERS, J., M. DAMEN, *Feudal Obligation or Paid Service? The Recruitment of Princely Armies in the Late Medieval Low Countries*, The English Historical Review, vol. 133, n° 563, 2018.

BURGORGUE-LARSEN L., *Actualité de la convention européenne des droits de l'homme (janvier-juillet 2017) Vie privée, conservation des empreintes génétiques*, AJDA, 2017.

BURKELL J., FORTIER A., WONG L. Y. C., SIMPSON J. L., *Facebook: public space, or private space?*, Information, Communication & Society, vol. 17, n° 8, 2014.

CABOT-NADAL, M. À., et al., *Private Identity-Related Attribute Verification Protocol Using SoulBound Tokens and Zero-Knowledge Proofs*, 7th Cyber Security in Networking Conference (CSNet), Montréal, 2023.

CALISKAN, E., T. MINARIK, A.-M. OSULA, *Technical and Legal Overview of the Tor Anonymity Network*, Cooperative Cyber Defence Centre of Excellence (CCDCOE), 2015.

CALO, R., et al., *Is Tricking a Robot Hacking?*, University of Washington School of Law Research Paper, n° 05, 2018.

CALO, R., et al., *Robotics and the Lessons of Cyberlaw*, California Law Review, vol. 103, n° 3, 2015.

CALOGIROU, C., *L'espace du privé, l'espace du public. Frontières et rencontres*, Migrations Société, n° 107, 1996.

CAMPBELL M, JOSEPH-HOANE Jr. A.,FENG-HSIUNG H., *Deep Blue*, *Artificial Intelligence*, vol. 134, Elsevier, 2002.

CANDRIAN, C., SCHERER, A., *Rise of the Machines: Delegating Decisions to Autonomous AI*, Computers in Human Behavior, vol. 134, 2022.

CAPRIOLI, É. A., *Droit pénal et Dark Web*, LexisNexis JurisClasseur, 2017.

CAPRIOLI, É. A., *Régime juridique du ransomware ou prise d'otage numérique* , Revue de la Gendarmerie Nationale, 4e trim., 2016.

CAPRIOLI, É.-A**.**, *Surveillance des communications électroniques à des fins de sécurité – La CEDH invalide partiellement l'ancien système britannique de surveillance électronique*, Communication – Commerce électronique, LexisNexis, n° 1, 2019.

CARDON D., *Réseaux sociaux de l'Internet*, Communications, n° 88, 2011.

CARLSMITH, K. M., J. M. DARLEY, *Psychological Aspects of Retributive Justice*, in *Advances in Experimental Social Psychology*, vol. 40, Academic Press, 2008.

CARPENTER, C., *Privacy and Proportionality: Examining Mass Electronic Surveillance under Article 8 and the Fourth Amendment*, International and Comparative Law Review, vol. 20, n° 1, 2020.

CARROLL, T. J., HURLEY, M.C., *When Deep Faking Results Means Improving Diagnosis*, Radiology, vol. 303, n° 1, 2022.

CASTAÑEDA, J. A., MONTORO, F. J., *The effect of Internet general privacy concern on customer behavior*, Electronic Commerce Research, vol. 7, 2007, p. 117–141.

CASTETS-RENARD, C., EYNARD, J. (dir.), *Un droit de l'intelligence artificielle : entre règles sectorielles et régime général, perspectives comparées*, Bruxelles, Bruylant, 2023.

CAZÉ-GAILLARDE N., *Atteintes à la vie privée – Frontières incertaines de la vie privée,* Jurisprudence de la Cour européenne des droits de l'homme, 2019 (actualisé 2023).

CAZE-GAILLARDS N., *Secret et citoyen – Les risques technologiques de l'information*, Entretiens de Nanterre, 1996.

ČERKA, P., J. GRIGIENĖ, G. SIRBIKYTĖ, *Is it Possible to Grant Legal Personality to Artificial Intelligence Software Systems?*, Computer Law & Security Review, vol. 33, n° 5, 2017.

CEYHAN, A., *Enjeux d'identification et de surveillance à l'heure de la biométrie*, Cultures & Conflits, 64(4), 2006.

CHALLIER, R., PICAUD, M., CASTAGNINO, F., *De la 'safe city' aux dispositifs numériques de sécurité urbaine,* Réseaux, n° 251/3, 2025.

CHAMBON P., *Analyse et commentaire de la loi du 10 juillet 1991*, *ALD*, 1991.

CHARLES, G.-U., L. FUENTES-ROHWER, *Habermas, the Public Sphere, and the Creation of a Racial Counterpublic*, Michigan Journal of Race & Law, vol. 21, 2015.

CHARPENET J., TELLER M., *La régulation des technologies quantiques : un cas d'école pour la régulation des innovations « totales »,* Dalloz IP/IT, 2024.

CHARPENET, J., *Entre optimisation juridique des pouvoirs privés numériques et Digital Services Act, où en sommes-nous de l'application du principe du pays d'origine ?*, *Dalloz IP/IT*, 2024.

CHAUHAN, S., A. KEPRATE, *Standards, Ethics, Legal Implications & Challenges of Artificial Intelligence*, IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Kuala Lumpur, 2022.

CHAVANNES A., *Protection de la vie privée dans la loi du 17 juillet 1970*, *RSC*, 1971.

CHAVENT-LECLÈRE, A.-S**.**, *Loi n° 2024-449 du 21 mai 2024 sur l'espace numérique : durcissement des mesures de retrait et de blocage des contenus illicites en ligne*, Procédures, n° 1, 2025.

CHEN, X.-W., X. LIN, *Big Data Deep Learning: Challenges and Perspectives*, IEEE Access, vol. 2, 2014,.

CHESNEY, R., CITRON, D.K., *21st Century Style Truth Decay: Deep Fakes and the Challenge for Privacy, Free Expression, and National Security*, Maryland Law Review, vol. 78, 2019, p. 887-930.

CHESNEY, R., CITRON, D.K., *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, California Law Review, vol. 107, 2019.

CHNG, S., LU, H.Y., KUMAR, A., YAU, D., *Hacker Types, Motivations and Strategies: A Comprehensive Framework*, Computers in Human Behavior Reports, vol. 5, 2022.

CHORAŚ, M., M. WOŹNIAK, *The Double-Edged Sword of AI: Ethical Adversarial Attacks to Counter Artificial Intelligence for Crime*, AI Ethics, vol. 2, 2022.

CHRISTOPHERSON, K., *The Positive and Negative Implications of Anonymity in Internet Social Interactions: On the Internet, Nobody Knows You're a Dog*, Computers in Human Behavior, vol.23, 2007.

CİMEN, H., et al., *Smart-Building Applications: Deep Learning-Based, RealTime Load Monitoring*, IEEE Industrial Electronics Magazine, vol. 15, n° 2, juin 2021.

CÎRDEI, I., *The Use of Artificial Intelligence and Autonomous Weapon Systems in Military Operations*, International Conference Knowledge-Based Organization, vol. 30, 2024.

CLARK A., CHALMERS D. J., *The Extended Mind*, *Analysis*, Oxford University Press, vol. 58, n° 1, 1998.

CLARKE, R. A., *The Digital Persona and Its Application to Data Surveillance*, Information Society, vol. 10, n° 2, 1994.
CLAYTON, K., S. BLAIR, J. A. BUSAM et al., *Real Solutions for Fake News? Measuring the Effectiveness of General Warnings and Fact-Check Tags in Reducing Belief in False Stories on Social Media*, Political Behavior, vol. 42, 2020.
CLÉMENT-FONTAINE M., *Panorama rapide de l'actualité "Technologies de l'information" de la semaine du 29 mai 2023*, Dalloz Actualité, 2023.
CLUZEL-MÉTAYER, L., *Le droit de l'intelligence artificielle*, 1re éd., Paris, Dalloz, coll. À savoir, 2025.
COLIN, M., BEUVELET, K., VAVASSORI, D., HARRATI, S., *L'agir violent numérique : aux frontières du réel*, Adolescence, t. 38, n° 1(1), 2020.
CONTE Ph., *Atteinte à la vie privée – Diffusion d'une photographie sans le consentement de l'intéressé*, Droit pénal, Lexis360 Intelligence.
CONTE, Ph., *Atteinte à l'intimité de la vie privée – Absence de consentement à la fixation de l'image*, Droit pénal, n° 7-8, 2023.
CONWAY, P., *Survey of Agencies Using Electronic Monitoring Reveals a Promising Future*, Journal of Offender Monitoring, vol. 16, n° 2, 2003.
CORIOLAND S., *Responsabilité pénale des personnes publiques : infractions intentionnelles*, Revue de droit pénal, 2022.
COSTAZ, C., *Le droit à l'oubli*, Gazette du Palais, vol.2, 1995.
COULON, C., *Du robot en droit de la responsabilité civile : à propos des dommages causés par les choses intelligentes*, Revue de droit de la responsabilité civile et des assurances (RCA), 2016, Étude 6.
COURRÈGES A., *L'Agence de la Biomédecine, un Modèle Original au Service de la Loi de Bioéthique.* Dalloz Actualité, 2021.
COURRÈGES, A., *Un an après*, Revue Droit administratif, n° 8-9, LexisNexis, 2025.
CRAGG, W., *H.L.A. Hart and the Justification of Punishment*, Canadian Journal of Law & Jurisprudence, vol. 5, n° 1, 1992, p. 43-55.
CRANOR, L. F., EGELMAN, S., SHENG, S., MCDONALD, A.M., CHOWDHURY, A., *P3P Deployment on Websites*, Electronic Commerce Research and Applications, vol. 7, n° 3, 2008.
CRICHTON C., *« Droit à l'oubli » sur les moteurs de recherche : état des lieux,* Dalloz Étudiant, 2019.
CRICHTON C., *Inconventionnalité de la collecte systématique de données biométriques d'un mis en examen : quelles conséquences sur le droit français ?*, Dalloz Actualité, 2023.

D'APONTE, M., *Les nouvelles technologies et le respect de la vie privée du travailleur dans la jurisprudence de la CEDH*, Revue de droit comparé du travail et de la sécurité sociale, n° 2, 2021.

DAHMANI, A., *Les technologies numériques dans les pays en développement. Quel paradigme ?,* Communication, technologies et développement, vol. 6, 2018.

DAMAR, M., *Metaverse Shape of Your Life for Future: A Bibliometric Snapshot*, Journal of Metaverse, 2021.

DANA, S., *Beyond Retroactivity to Realizing Justice: A Theory on the Principle of Legality in International Criminal Law Sentencing*, Journal of Criminal Law & Criminology, vol. 99, 2009.

DANAHER, J., *Robots, Law and the Retribution Gap*, Ethics and Information Technology, vol. 18, 2016.

DANESHJOU, R., SMITH, M. P., SUN, M. D., ROTEMBERG, V., ZOU, J., *Lack of transparency and potential bias in artificial intelligence data sets and algorithms: a scoping review*, JAMA Dermatol, 157(11), 2021.

DASKAL, J., *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, Journal of National Security Law and Policy, vol. 8, 2016.

DE HERT P., GUTWIRTH S., *Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action*, in *Reinventing Data Protection*, Springer, 2009.

DE MAURO, A., M. GRECO, M. GRIMALDI, *What is Big Data? A Consensual Definition and a Review of Key Research Topics*, dans les actes de la 4e International Conference on Integrated Information, AIP Conference Proceedings, vol. 1644, 2015.

DE MONTJOYE, Y. A., RADAELLI, L., SINGH, V. K. et al., *Unique in the shopping mall : on the reidentifiability of credit card metadata*, Science, n° 347, 2015.

DE VAUPLANE, H., *La personnalité juridique des robots*, in *Mélanges en l'honneur de Jean-Jacques Daigre*, Lextenso, 2017.

DEANDREA D. C., TONG S. T., LIANG Y. J., *When do people misrepresent themselves to others? The effects of social desirability, ground truth, and accountability on deceptive self-presentations*, Journal of Communication, vol. 62, n° 3, 2012.

DÉCHAUX, J.-H., *L'individualisme génétique: Marché du test génétique, biotechnologies et transhumanisme*, Revue Française de Sociologie, vol. 60, n° 1, 2019.

DECHEPY-TELLIER J., *La confidentialité de la correspondance échangée entre un avocat et son client: une exigence du procès équitable,* Revue Internationale de Droit Comparé, vol. 71, n° 2, 2019.

DEMICHELE, M., *Electronic Monitoring: It Is a Tool, Not a Silver Bullet*, Criminology & Public Policy, vol. 13, 2014.

DENIZOT A., *Petites rectifications et grandes avancées en droit des victimes*, RTDCiv. Revue Trimestrielle de Droit Civil, n° 4, 2020.

DENNY, J. C., COLLINS, F.S., *Precision Medicine in 2030, Seven Ways to Transform Healthcare*, Cell, 2021.

DERIEUX, E., *Vie privée et données personnelles – Droit à la protection et « droit à l'oubli » face à la liberté d'expression*, Les Nouveaux Cahiers du Conseil constitutionnel, vol. 2015, n° 3, 2015.

DESGARDIN-BOURDEAU, V., *Révision des lois de bioéthique : adoption par l'Assemblée nationale du projet de loi*, Dalloz Actualité, 2011.

DESLÉE, A., *La vie privée en ligne : utopie ou réalité ? Comprendre la vulnérabilité perçue relative aux données personnelles*, Décisions Marketing, vol. 111(3), 2023.

DEUMIER, P., *Rapport sur la lutte contre l'inflation législative*, Dalloz, 2013.

DIAZ, B., DIAZ, J.-L., *Le siècle de l'intime*, Itinéraires. Littérature, textes, cultures, n° 4, 2009.

DIAZ, F., *"Coproduction" de la sécurité : une nouvelle forme de l'interventionnisme étatique ?*, Déviance et Société, vol. 27, n° 4, 2003.

DILMAÇ, J. A., KOCADAL, O., *Prévenir le cyberharcèlement en France et au Royaume-Uni : une tâche impossible ?*, Déviance et Société, 43(3), 2019.

DILMAÇ, J.A., KOCADAL, Ö., *Exchanging Glances With Big Brother: Diffuse Surveillance in Orwell's Nineteen Eighty-Four and Today*, Sciences & Actions Sociales, vol.12(2), 2019.

DING, W., CHEN, L., *Regulating the Use of Big Data: Justifications, Perspectives, and the Chinese Way Forward*, Computer Law & Security Review, vol. 46, 2022.

DINGLEDINE, R., MATHEWSON, N., SYVERSON, P., *Tor: The Second-Generation Onion Router*, Proceedings of the 13th USENIX Security Symposium, San Diego, 2004.

DIONISI-PEYRUSSE, A., *30 ans de lois de bioéthique: une grande œuvre inachevée,* Recueil Dalloz, 2024.

DIONISI-PEYRUSSE, A*., Actualité de la bioéthique,* AJ Fam., 2024.

DORSNER-DOLIVET, A., *Les dispositions de la loi du 15 juin 2000 renforçant les garanties judiciaires en matière de détention provisoire*, Droit pénal, Chronique, n° 39, 2000.

DOURNEAU-JOSETTE, P., *Interceptions de correspondances émises par la voie des télécommunications électroniqu*es, Dalloz, 2016 (actualisé 2020).

DOUSSOT, J.-P., *Quis custodiet ipsos custodes ? ou de la nécessité d'évaluer l'évaluateur*, La Semaine Juridique, Administrations et Collectivités territoriales, LexisNexis, n° 20, 2005.

DOUVILLE, Th**.**, *De l'amputation discutable de la compétence des États membres de l'Union européenne pour encadrer le secteur numérique* , Dalloz, 2024.

DREMLIUGA, R., KUZNETCOV, P., MAMYCHEV, A., *Criteria for Recognition of AI as a Legal Person*, Journal of Politics and Law, vol. 12, 2019.

DREMLIUGA, R., PRISEKINA, N., *The Concept of Culpability in Criminal Law and AI Systems*, Journal of Politics and Law, vol. 13, 2020.

DREYER, E., *Existe-t-il une conception pénale de la vie privée* ?, Archives de politique criminelle, n° 43, 2021/1.

DREYER, E., *La subsidiarité du droit pénal*, en J H Robert, *Mélanges*, LexisNexis, 2012.

DUAN, Y., EDWARDS, J.S., DWIVEDI, Y.K., *Artificial Intelligence for Decision Making in the Era of Big Data: Evolution, Challenges and Research Agenda*, International Journal of Information Management, vol. 48, 2019.

DUBET, F., *Ce Que les Discriminations Font aux Individus et aux Sociétés*, Mélanges de la Casa de Velázquez, vol. 47, n° 2, 2017.

DUBUISSON, F., *La Cour européenne des droits de l'homme face à la surveillance de masse (obs. sous Cour eur. dr. h., Gde Ch., arrêt Big Brother Watch et autres c. Royaume-Uni, 25 mai 2021)*, Revue trimestrielle des droits de l'Homme, vol. 129(1), 2022.

DUCU, C., *Integrarea tehnologiilor noi și emergente în sistemul educațional românesc*, Policy Brief, Asociația Centrul Syene pentru Educație, București, 2018.

DUELUND, P., *Jürgen Habermas, The Structural Transformation of the Public Sphere: An Inquiry Into a Category of Bourgeois Society*, International Journal of Cultural Policy, vol. 16, 2010.

DUINA, F., RAUNIO, T., *The Open Method of Co-Ordination and National Parliaments: Further Marginalization or New Opportunities?*, Journal of European Public Policy, vol. 14, n° 4, 2007.

DUMONT, J., *Fasc. 20: Contrôle judiciaire et détention provisoire, Art. 137 à 150* , J.-Cl. proc. pén., 2001.

DÜNKEL, F., et al, *Electronic Monitoring in Europe - A Panacea for Reforming Criminal Sanctions Systems? A Critical Review*, Kriminologijos Studijos, vol. 6, 2018.

DÜNKEL, F., et al, *European Penology: The Rise and Fall of Prison Population Rates in Europe in Times of Migrant Crises and Terrorism*, European Journal of Criminology, vol. 14, 2017.

DÜNKEL, F., et al, *You'll Never Stand-Alone: Electronic Monitoring in Germany*, European Journal of Probation, vol. 9, n° 1, 2017.

DYEVRE, V., *Génétique et Enquêtes Policières*, Les Tribunes de la Santé, vol. 17, n° 4, 2007.

EDER, N., *Privacy, Non-Discrimination and Equal Treatment: Developing a Fundamental Rights Response to Behavioural Profiling*, Springer 2021.

EDWARDS, J., et al., *The Internal Morality of Criminal Law*, Oxford Journal of Legal Studies, vol.43, 2023.

EKANAYAKE, I. U., MEDDAGE, D.P.P, RATHNAYAKE, U., *A Novel Approach to Explain the Black-Box Nature of Machine Learning in Compressive Strength Predictions of Concrete Using Shapley Additive Explanations (SHAP)*, Case Studies in Construction Materials, vol. 16, 2022.

ELISEEV E. D., MARSH E. J., *Externalizing autobiographical memories in the digital age*, Trends in Cognitive Sciences, vol. 25, n° 12, 2021.

ELIZALDE, L. H., et al., *The Structural Transformation of the Public Sphere*, Church, Communication and Culture, vol. 8, 2023.

ENCAOUA, D*., Repenser les politiques d'innovation en France ?,* Revue française d'économie, XXXII(3), 2017.

EOCH-DUVAL C., *Un "mal français: son e-norme" production juridique ?*, Revue du droit public (RDP), n° 2, 2022.

ERBSCHLOE, M., *Lessons from Love Crimes*, Information Systems Security, vol. 9, n° 6, 2001.

ERDURAN, S., *Deepfakes and Students' Deep Learning: A Harmonious Pair in Science?*, Science, vol. 385, 2024.

ERWIN, C., et al., *Perception, Experience, and Response to Genetic Discrimination in Huntington Disease: The International RESPOND-HD Study*, American Journal of Medical Genetics B Neuropsychiatric Genetics, vol. 153B, 2010.

ESAYAS, S. Y., *The role of anonymisation and pseudonymisation under the EU data privacy rules : beyond the all or nothing approach*, European Journal of Law and Technology, vol. 6, n° 2, 2015.

ESPER, C., *Introduction du Colloque « Loi de Bioéthique du 2 Août 2021. Quel Impact sur Nos Vies ? »*, Journal du Droit de la Santé et de l'Assurance-Maladie (JDSAM), n° 32, 2022.

ÉTUDES PLATONICIENNES, « Studies on Plato », OpenEdition Journals, 2023.

EVANS, A., *Pros and Cons of Virtual Reality in the Classroom*, Chronicle of Higher Education, 2018.

EVEILLARD, G*., Rejet par ordonnance – La possibilité de rejeter par ordonnance le recours contre un acte non encore né,* Droit administratif, n° 4, comm. 12, 2024.

EWALD, F., *Les Normes de Protection des Données Génétiques en France*, Revue de Droit Sanitaire et Social, vol. 60, n° 3, 2018.

EWALD, F., *Les Technologies CRISPR et Leur Application dans les Maladies Génétiques*, Revue de Droit Sanitaire et Social, vol. 60, n° 3, 2019.

EYMARD, O., *Questions de cryptologie*, Délibérée, 3(1), 2018.

FALQUE-PIERROTIN, I., *La Constitution et l'internet*, N3C, vol. 3, n° 36, 2012.

FARWELL, J. P., ROHOZINSKI, R., *Stuxnet and the Future of Cyber War*, Survival, vol. 53, n° 1, 2011.

Fasc. 1010: *Personnes - Famille. – Personnalité juridique*, JurisClasseur Roulois, Lexis360 Intelligence, 2022

FAVREAU, A., *Mort numérique. Quel sort juridique pour nos informations personnelles?*, Revue Lamy Droit Civil, vol. 125, 2015.

FÉLIX, J., *Profit, Embezzlement, Restitution. The Role of the Traîtants in the Nine Years' War and Chamillart's Tax on Financial Benefits*, Revue Historique, 2015.

FÉLIX, J., *Profits, Malversations, Restitutions. Les Bénéfices des Financiers Durant la Guerre de la Ligue d'Augsbourg et la Taxe de Chamillart*, Revue Historique, n° 676(4), 2015.

FERNER, R. E., *Medication Errors That Have Led to Manslaughter Charges*, BMJ, vol. 321, 2000.

FERRARA, E., *The Butterfly Effect in Artificial Intelligence Systems: Implications for AI Bias and Fairness*, Machine Learning with Applications, vol. 15, 2024.

FILIOL, E., *Les risques concernant l'utilisation des algorithmes dits prédictifs dans le domaine sensible de la justice*, Archives de philosophie du droit, 2018.

FINN, M., S. MUIRHEAD-STEVES, *The Effectiveness of Electronic Monitoring with Violent Male Parolees*, Justice Quarterly, vol. 19, 2002, p. 293-312.

FLOREA, D., S. FLOREA, *Big Data and the Ethical Implications of Data Privacy in Higher Education Research*, Sustainability, vol. 12, 2020.

FLORIDI, L., *Group Privacy: A Defense and an Interpretation*, SSRN Electronic Journal, 2017.

FLYNN, A., *Image-Based Sexual Abuse*, Oxford Research Encyclopedia of Criminology, 2023.

FOSTER, R., *Review: A New Structural Transformation of the Public Sphere and Deliberative Politics by Jürgen Habermas*, Oxford Political Review, 2024.

FRANÇOIS, L., *SPARà l'épreuve de la liberté d'information, CEDH 28 juin 2018, nos 60798/10 et 65599/10, M.L. et W.W. c/ Allemagne*, AJ Pénal, 2018.

FRASER N., *Repenser la sphère publique : une contribution à la critique de la démocratie telle qu'elle existe réellement*, in CALHOUN C. (dir.), *Habermas and the Public Sphere*, Cambridge, MIT Press, 1992.

FRONCZAK, S., *Ransomware : le dossier comprendre l'ennemi*, Revue Cyber & Conformité, 1(1), 2021.

G'SELL, F., *Les réseaux sociaux ou la privatisation de l'espace informationnel en ligne*, Revue de droit international et de droit comparé appliqué (RDIA), n° 5, 2022.
GALUSTIAN, G., *La protection des données personnelles à l'épreuve du numérique*, Revue du droit public, 2018.
GAMAGE, D., CHEN, J., SASAHARA, K., *The Emergence of Deepfakes and Its Societal Implications: A Systematic Review*, Hacks/Hackers, TTO, virtual, 2021.
GAMBÍN, Á. F., YAZIDI, A., VASILAKOS, A., *Deepfakes: Current and Future Trends*, Artificial Intelligence Review, vol. 57, 2024.
GANASCIA, J.-G., *Le mythe de la singularité : faut-il craindre l'intelligence artificielle ?*, Paris, Seuil, 2017.
GANDIA, R. M., et al., *The Quintuple Helix Model and the Future of Mobility: The Case of Autonomous Vehicles*, 25th International Colloquium of Gerpisa-R/Evolutions: New Technologies and Services in the Automotive Industry, 2017.
GANDOMI, A., HAIDER, M., *Beyond the Hype: Big Data Concepts, Methods, and Analytics*, International Journal of Information Management, vol. 35, n° 2, 2015.
GANNON, C., et al., *Child Sexual Abuse Material on the Darknet*, Forensische Psychiatrie Psychologie Kriminologie, vol. 17, 2023.
GARAPON, A, LASSÈGUE, J.L., *Justice numérique : révolution graphique et rupture anthropologique*, Paris, Presses universitaires de France (PUF), 2018.
GARAPON, A., *Un nouveau modèle de justice: efficacité, acteur stratégique, sécurité*, Esprit, 2008.
GARDINER, M., *Wild Publics and Grotesque Symposiums: Habermas and Bakhtin on Dialogue, Everyday Life and the Public Sphere*, The Sociological Review, vol. 52, 2004.
GAUTIER, P-Y., *De l'influence des réseaux sociaux sur l'édiction du droit*, Dalloz IP/IT, 2019.
GELLER, L., ALPER, J., BILLINGS, P., BARASH, C., BECKWITH, J., NATOWICZ, M., *Individual, Family, and Societal Dimensions of Genetic Discrimination: A Case Study Analysis*, Science and Engineering Ethics, vol. 2, 1996.
GEMMELL, J., BELL, G., LUEDER, R., *MyLifeBits : a personal database for everything*, Communications of the ACM, vol. 49, n° 1, 2006.
GÉRARDIN, S. *Plusieurs mises en demeure pour l'utilisation du logiciel Briefcam,* Dalloz actualité, 2024.
GERARDS, J., *How to Improve the Necessity Test of the European Court of Human Rights*, International Journal of Constitutional Law, vol. 11, 2013.
GERKEN M., *Outsourced Cognition*, *Philosophical Issues*, Wiley-VCH, vol. 24, n° 1, 2014.
GHUEKOU, V., *Facebook rendrait-il l'homo numericus éternel* ?, Village de la Justice, 2013.

GIBBS, A., KING, D., *Home Detention with Electronic Monitoring: The New Zealand Experience*, Criminology & Criminal Justice, vol. 3, n° 2, 2003.

GIRGIS, S., AMER, E., GADALLAH, M., *Deep Learning Algorithms for Detecting Fake News in Online Text*, IEEE International Conference on Computer Engineering and Systems, 2018.

GLANCY, D. J., *The Invention of the Right to Privacy*, Arizona Law Review, 1979.

GLASSMAN, R. M., *From the Theocratic State to the Kingly-Bureaucratic State*, in *State Formation, Nation-Building, and Mass Politics in Europe*, Springer, 2017.

GLÉNARD, G., *La dignité de la personne humaine: un ordre de valeurs*?, Revue française de droit administratif (RFDA), 2015.

GLESS, S., SILVERMAN, E., WEIGEND, T., *If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability*, SSRN Working Paper, 2016.

GOERTZEL, B., *Artificial General Intelligence: Concept, State of the Art, and Future Prospects*, Journal of Artificial General Intelligence, 2014.

GONZÁLEZ, R., *Hacking the Citizenry?: Personality Profiling, "Big Data" and the Election of Donald Trump*, Anthropology Today, vol. 33, 2017.

GOODMAN, D., *Public Sphere and Private Life: Toward a Synthesis of Current Historiographical Approaches to the Old Regime*, History and Theory, vol. 31, n° 1, 1992.

GOODMAN, M., *The Emerging Consensus on Criminal Conduct in Cyberspace*, International Journal of Law and Information Technology, vol. 10, 2002.

GOODMAN, N. J., *Ethical Decision Making during Automated Vehicle Crashes*, Transportation Research Record, vol. 2424, n° 1, 2014.

GOSTIN, L. O., HODGE, J.G., *Genetic Privacy and the Law: An End to Genetics Exceptionalism*, Jurimetrics Journal, vol. 40, 1999.

GOULEMOT, J.-M., *Tensions et contradictions de l'intime dans les pratiques des Lumières*, Littérales, L'invention de l'intimité au Siècle des Lumières, n° 17, Université Paris X-Nanterre, 1995.

GOUTTENOIRE, A., *Autorité parentale – Délégation de l'exercice de l'autorité parentale*, Répertoire de droit civil, LexisNexis, juillet 2024 (actualisation : mars 2025).

GOZZI, M.-H., *Sed quis custodiet ipsos custodes ? – À propos de la loi du 24 juillet 2015 relative au renseignement*, La Semaine Juridique – Édition Générale, n° 38, 2015.

GRENET, J., H. GRÖNQVIST, S. NIKNAMI, *The Effects of Electronic Monitoring on Offenders and Their Families*, Journal of Public Economics, vol. 230, 2024.

GRIDEL, J.P., LACABARATS, A., *Droit à la vie privée et liberté d'expression: fond du droit et action en justice*, Gaz. Pal., doctr.1632, 2002.

GRIMMELMANN, J., *Regulation by Software*, Yale Law Journal, vol. 114, 2005.

GRYNBAUM, L., *Chap. 3 : responsabilité du fait d'une intelligence artificielle*, in *Traité de droit civil – Responsabilité civile et assurance*, Paris, Dalloz, 2023.

GUEDJ A*., L'apport de la loi SREN en matière de deepfake : une obsolescence annoncée ?,* Dalloz IP/IT, 2024.

GUÉGUEN H., *Les contradictions paradoxales de l'expressivité numérique. L'étude des modèles identitaires au sein des espaces numériques*, Réseaux, vol. 193, n° 5, 2015.

GUERRINI, M., *Les droits et libertés de l'homo numericus*, communication au colloque Les droits et libertés numériques, Université Côte d'Azur, 7 oct. 2021.

GUGLIELMI, *Homo numericus, un citoyen digitalisé et numérisé conscientisé*, in Drôle d'en-droit – Droits de l'Homme et des Libertés fondamentales, 2009.

GUILHEM, J. (dir.), *Sciences et sens de l'intelligence artificielle*, Paris, Dalloz, coll. Thèmes & Commentaires, 2020.

GUPTA A., *A Tale of Two UN Resolutions on Cyber-security*, Vivekananda International Foundation (VIF), 2019.

GUPTA, S., et al., *Forensic Analysis of E-Mail Address Spoofing*, in Proceedings of the 2014 5th International Conference – Confluence: The Next Generation Information Technology Summit, 2014.

HABERMAS, J., *The Public Sphere: An Encyclopedia Article (1964)*, The New German Critique, 1974.

HADDAWAY R., *Anatomy Act*, in *The Palgrave Encyclopedia of Victorian Women's Writing*, Palgrave Macmillan, Cham, 2021.

HAFTEL, B., *Protection des données personnelles : autorité de contrôle compétente et loi applicable*, Revue critique de droit international privé, vol. 2(2), 2016.

HAIN, D., et al., *Machine Learning and Artificial Intelligence for Science, Technology, Innovation Mapping and Forecasting: Review, Synthesis, and Applications*, Scientometrics, vol. 128, 2023.

HAKIM, F., MELLERAY, F., *La belle époque de la pensée juridique française*, in *Le renouveau de la doctrine française*, Paris, Dalloz, 2009.

HAKLI, R., MÄKELÄ, P., *Robots, Autonomy, and Responsibility*, Oxford University Press, 2016.

HALLEVY, G., *The Basic Models of Criminal Liability of AI Systems and Outer Circles*, SSRN Electronic Journal, 2019.

HALLEVY, G., *The Criminal Liability of Artificial Intelligence Entities: From Science Fiction to Legal Social Control*, Akron Intellectual Property Journal, vol. 4, 2010.

HALLEVY, G., *The Punishibility of Artificial Intelligence Technology*, in *Liability for Crimes Involving Artificial Intelligence Systems*, Springer, 2014.
HALLEVY, G., *Virtual Criminal Responsibility*, The Original Law Review, vol. 6, n° 1, 2010.
HAMELEERS, M., *Cheap Versus Deep Manipulation: The Effects of Cheapfakes Versus Deepfakes in a Political Setting*, International Journal of Public Opinion Research, vol. 36, 2024.
HAMET, J., MICHEL, S., *Les questionnements éthiques en systèmes d'information*, Revue française de gestion, vol. 271(2), 2018.
HAN, Y., *Evolution of mediated memory in the digital age: tracing its path from the 1950s to the 2010s*, Humanities and Social Sciences Communications, vol. 10, no 603, 2023.
HANNAH-MOFFAT, K., P. MAURUTTO, *Re-contextualizing Pre-sentence Reports: Risk and Race*, Punishment and Society, vol. 12, n° 3, 2010.
HARDEVELD, G., WEBBER, C., O'HARA, K., *Deviating from the Cybercriminal Script: Exploring Tools of Anonymity (Mis)Used by Carders on Cryptomarkets*, American Behavioral Scientist, 2017.
HARE F., *Borders in cyberspace: can sovereignty adapt to the challenges of cyber security?*, Analele Universității George Mason, 2009.
HASELAGER, W., *Robotics, Philosophy and the Problems of Autonomy*, Pragmatics & Cognition, vol. 13, n° 3, 2005.
HASNAIN, Z., STOJANOVIĆ PRELEVIĆ, I., *Aesthetics of Deepfake: Sphere of Art and Entertainment Industry*, Facta Universitatis – Series Visual Arts and Music, 2024.
HASSANI, N., *Le paradoxe de la protection des données personnelles à l'heure de la libre circulation des informations*, Terminal, OpenEdition, 2019.
HASSIJA, V., et al., *Interpreting Black-Box Models: A Review on Explainable Artificial Intelligence*, Cognitive Computation, vol. 16, 2024.
HASSLER, T., *Droits de la personnalité: rediffusion et droit à l'oubli*, *Dalloz*, 2007.
HEIDE, L., *Monitoring People: Dynamics and Hazards of Record Management in France*, *1935-1944*, Technology and Culture, vol.*45*(1), 2004.
HEILMAN, K. M., et al., *Creative Innovation: Possible Brain Mechanisms*, Neurocase, vol. 9, n° 5, 2003, p. 369-379.
HENNEGUELLE, A., et al., *Better at Home than in Prison? The Effects of Electronic Monitoring on Recidivism in France*, The Journal of Law and Economics, vol. 59, n° 3, 2016, p. 629-667.
HERZOG-EVANS, M., *Application des peines: la prétendue « bonne partie » de la loi pénitentiaire*, AJ Pénal, 2009.

HIROLIKAR, D., et al., *Intelligent Movie Recommendation System Using AI and ML*, International Journal for Research in Applied Science and Engineering Technology, vol. 10, 2022.

HOBSON Z., et al., *Alcohol Abstinence Monitoring Requirement: A Review of Process and Performance from Year 2*, Greater London Authority, Londres, 2020.

HO-DAC, M., *Législation européenne sur l'intelligence artificielle : point d'étape après la présidence française de l'Union européenne*, Dalloz IP/IT, 2022.

HOFMANN, M., *Political Deliberation vs. Social Media Branding in Crisis-Prone Capitalist Democracies*, Journal of Political Sociology, 2023.

HOFMANN, M., *Theoretical and Practical Influences of Habermas's Global Academic Bestseller: Structural Transformation of the Public Sphere in the United States*, Kybernetes, vol. 50, 2020.

HOLT, T., D. STRUMSKY, O. SMIRNOVA, M. KILGER, *Examining the Social Networks of Malware Writers and Hackers*, International Journal of Cyber Criminology, vol. 6, 2012.

HOPKINS, J., *Managing the Right to Disconnect - A Scoping Review*, Sustainability, vol. 16, n° 12, 2024.

HÖRNLE, J., et al., *How to Control Interception: Does the UK Strike the Right Balance?*, Computer Law & Security Review, vol. 26, 2010.

HOWARD, H. C., P. BORRY, *Is There a Doctor in the House?: The Presence of Physicians in the Direct-to-Consumer Genetic Testing Context*, Journal of Community Genetics, vol. 3, n° 2, 2012.

HU, M., *Cambridge Analytica's Black Box*, Big Data & Society, vol. 7, 2020.

HUANG, Y., Y. J. LI, Z. CAI, *Security and Privacy in Metaverse: A Comprehensive Survey*, Big Data Mining and Analytics, vol. 6, n° 2, 2023.

HUCKLESBY, A., et al., *Creativity and Effectiveness in the Use of Electronic Monitoring: A Case Study of Five Jurisdictions*, University of Leeds, Centre for Criminal Justice Studies, 2016.

HUCKLESBY, A., *Understanding Offenders' Compliance: A Case Study of Electronically Monitored Curfew Orders*, Journal of Law and Society, vol. 36, n° 2, 2009.

HUCKLESBY, A., *Vehicles of Desistance? The Impact of Electronically Monitored Curfew Orders*, Criminology and Criminal Justice, vol. 51, n° 8, 2008.

HUEZ, O., *Ethique et Conséquences Juridiques des Utilisations Abusives des Données Génétiques*, Cahiers de Droit Européen, vol. 57, n° 1, 2018.

HUEZ, O., *La Non-Discrimination Génétique: Perspectives Juridiques*, Cahiers de Droit Européen, vol. 57, n° 1, 2020.

HUEZ, O., *Les Enjeux de la Législation en Génétique: Vers une Protection Globale*, Cahiers de Droit Européen, vol. 57, n° 1, 2020.
HUSTINX P., *EU data protection law: the review of Directive 95/46/EC and the proposed General Data Protection Regulation*, European University Institute, Academy of European Law, 2013.
HUSZTI-ORBÁN K., NÍ AOLÁIN F., *Use of biometric data to identify terrorists: best practice or risky business?*, Human Rights Center, University of Minnesota, 2020.
HUTMACHER F., APPEL M., SCHWAN S., *Understanding Autobiographical Memory in the Digital Age: The AMEDIA-Model*, Psychological Inquiry, vol. 35, n° 2, 2024.
INFOREG, *Sécurité des données personnelles. Le nouvel audit cybersécurité*, Cahiers de droit de l'entreprise, n° 3, 2022.
INGRAO, C., *Jeroen Duindam. Vienna and Versailles: The Courts of Europe's Dynastic Rivals, 1550–1780*, Austrian History Yearbook, Cambridge University Press, 2003.
IONIȚĂ-NICULESCU, M., *Impactul modernității asupra vieții private*, Analele Universității „Constantin Brâncuși" din Târgu Jiu, Seria Litere și Științe Sociale, n° 2, 2010.
JAHA, S., S. THRUN, *Artificial Intelligence and Its Legal Personhood in Criminal Law: A Systematic Review*, Research Gate, working paper, 2024.
JAIN, A., ROSS, A., PRABHAKAR, S., *An Introduction to Biometric Recognition*, IEEE Xplore, 2004.
JAIN, P., PONNURANGAM, K., ANUPAM, J., *Identifying Users Across Multiple Online Social Networks*, ACM Digital Library, 2013.
JAMISON M., GLAVISH M., *The Dark Side of the Metaverse, Part I*, AEIdeas, American Enterprise Institute, 2022.
JAMISON M., GLAVISH M., *The Dark Side of the Metaverse, Part II: Potential Solutions*, AEIdeas, American Enterprise Institute, 2022.
JASHUA, J., *Information Bodies: Computational Anxiety in Neal Stephenson's Snow Crash*, Interdisciplinary Literary Studies, 2017.
JAUTROU, H., *Les Tests Génétiques en Libre Accès - Régulation par le Marché, ou Régulation Médicale*, Med Sci (Paris), vol. 36, n° 2, 2020.
JEANDIDIER, W., *Détention provisoire, Convention européenne des droits de l'homme et Code de procédure pénale, ou valse-hésitation de la Chambre criminelle,* RS crim. 1986.
JEGO, *Les conséquences de la surpopulation en détention*, AJ Pénal, vol. 344, 2018.
JOLY, Y., I. NGUENG FEZE, J. SIMARD, *Genetic Discrimination and Life Insurance: A Systematic Review of the Evidence*, BMC Medicine, vol. 11, n° 25, 2013.

JONES, M. L., LEE, J., *Comparing Consent to Cookies: A Case for Protecting Non-Use* Cornell International Law Journal, vol. 53, 2020.

KAHLER, E., *The Origins of the Total State*, The German Quarterly, vol. 14, n° 2, 1941.

KALPOKAS, I., *Problematising Reality: The Promises and Perils of Synthetic Media*, SN Social Sciences, vol. 1, n° 1, 2021.

KALYVAKI M., *Navigating the metaverse business and legal challenges: intellectual property, privacy, and jurisdiction*, Journal of Metaverse, vol. 3, 2023.

KAMINSKI M. E., et al., *Averting robot eyes*, Maryland Law Review, vol. 76, p. 983, 2017.

KAPPLER K., *Consequences of the German Constitutional Court's ruling on Germany's foreign intelligence service: the importance of human rights in the cooperation of intelligence services*, German Law Journal, vol. 23, 2022.

KARAGYOZOVA, T., *Liability of the Indirect Perpetrator in the Absence of Identity Between What Was Done by 'The Tool' and What It Was Intended to Do*, De Jure, vol. 12, 2021.

KARALE, A., *The Challenges of IoT: Addressing Security, Ethics, Privacy, and Laws*, Internet of Things, vol. 15, Elsevier, 2021.

KASAP, A., *Artificial Intelligence and Legal Personhood: Current Developments in Turkish Law*, Turk-Alman Universitesi Hukuk Fakultesi Dergisi, vol. 4, n° 2, 2022.

KELLY, Y., al., *Social media use and adolescent mental health: findings from the UK Millennium Cohort Study* , The Lancet, vol. 6, 2018.

KENSEY, A., et al., *Le Développement de la Surveillance Électronique en France et ses Effets sur la Récidive*, Criminologie, vol. 43, n° 2, 2010.

KESKIN, A. E., *Digitalization of Memories – An Analysis Relationship Between Autobiographical Memory and Digital Photography*, Media Literacy and Academic Research, vol. 3, n° 1, 2020.

KING J., MEINHARDT C., *Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World*, White Paper, Stanford University, 2024.

KING, G., PAN, J., ROBERTS, M.E., *How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument*, American Political Science Review, vol. 111, n° 3, 2017.

KING, T. C., et al., *Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions*, Science and Engineering Ethics, vol. 26, n° 1, 2020.

KLOPPENBURG S., VAN DER PLOEG I., *Security Identities*: Biometric Technologies and the Enactment of Human Bodily Differences, Science as Culture, vol. 29, n° 1, 2020.

KNIGHT, E. J., GEKKER, A., *Mapping Interfacial Regimes of Control: A Qualitative Analysis of America's Post-9/11 Security Technology Infrastructure*, Surveillance & Society, 2020.

KOO, J., KANG, G., KIM, Y.G., *Security and Privacy in Big Data Life Cycle: A Survey and Open Challenges*, Sustainability, vol. 12, n° 10571, 2020.

KOOPS B.-J., HILDEBRANDT M., JAQUET-CHIFFELLE D.-O., *Bridging the accountability gap: rights for new entities in the information society?*, Minnesota Journal of Law, Science & Technology, vol. 11, n° 2, 2010, pp. 497-561.

KORF R. E., *Does Deep-Blue use AI?*, Computer Science Department, University of California, 1997.

KOTLIAR D. M., GROSLIK R., *On the Contesting Conceptualisation of the Human Body: Between Homo-Microbis and Homo-Algorithmicus*, Body & Society, vol. 29, n° 3, 2023.

KOVAČ, V. B., et all., *The Why, What and How of Deep Learning: Critical Analysis and Additional Concerns*, Education Inquiry, 2023.

KRANTZ, S. G., *The Proof Is in the Pudding: The Changing Nature of Mathematical Proof*, New York, Springer, 2011.

KROLL, J., HUEY, J., BAROCAS, S., FELTEN, E., REIDENBERG, J., ROBINSON, D., YU, H., *Accountable Algorithms*, University of Pennsylvania Law Review, vol. 165, 2017.

KUBICA, M. L., *Autonomous Vehicles and Liability Law*, The American Journal of Comparative Law, vol. 70, suppl. 1, 2022.

KUKUTLA, T. R., *A Deep Dive into DNS Spoofing and Security Measures*, ResearchGate, 2023.

L. G., *Review of Jurisprudence, by J. Salmond*, The Cambridge Law Journal, vol. 2, n° 1, 1924.

LABBÉ X., *Respect et protection du corps humain. – L'homme nouveau*, JurisClasseur Civil Code, art. 16 à 16-14, fasc. 56, LexisNexis, 2021.

LABBÉE X., *Le sujet de droits sujet connecté ?*, Gazette du Palais, vol.31, n° 37, 2017.

LACOMBE, D., *Génétique Médicale et Éthique*, Journal International de Bioéthique, vol. 23, n° 2, 2012.

LAGIOIA, F., SARTOR, G., *AI Systems Under Criminal Law: A Legal Analysis and a Regulatory Perspective*, Philosophy & Technology, vol. 33, 2019, p. 433-465.

LAMBERTERIE I. *Débat éthique et juridique relatif à l'accès aux données génétiques,* Éthique Publique*,* vol. 6, n° 2, 2004.

LAMI, H., *1984, une dystopie devenue réalité? De l'écran à l'algorithme : une brève analyse juridique*, Revue française de droit administratif (RFDA), 2025.

LAMY C., *Publication de la loi SREN sans le délit d'outrage en ligne, Observations sous Conseil constitutionnel,* Dalloz IP/IT, 2024.

LAND M. K., ARONSON J. D., *Human rights and technology: new challenges for justice and accountability*, Annual Review of Law and Social Science, 2020.

LANG, G., *Éléments pour une histoire du Numéro de sécurité sociale,* Statistique et société, n°6, 2018.

LANGER, M., HUNSICKER, T., FELDKAMP, T., KÖNIG, C. J., GRGIĆ-HLAČA, N., *Look! It's a Computer Program! It's an Algorithm! It's AI! Does Terminology Affect Human Perceptions and Evaluations of Algorithmic Decision-Making Systems?*, in *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, ACM Press, New York, 2022.

LASLIER, P.-F., *La responsabilité pénale du fait de l'intelligence artificielle : une approche par les risques ?*, Recueil Dalloz, 2025.

LASSALE, A., *De Big Brother à Big Data: l'avenir de la police administrative à l'ère de la vidéosurveillance intelligente*, RFDA 2024.

LATIL, A., *Droit de l'intelligence artificielle (droit international et droit européen)*, JurisClasseur Communication, fasc. 988, LexisNexis, 2024.

LATIL, A., *Droit de l'intelligence artificielle (droit international et droit européen)*, JurisClasseur Communication, fasc. 988, LexisNexis, 2024.

LATOUR X., *La loi relative au renseignement: un État de surveillance*, La Semaine Juridique – Administrations et Collectivités Territoriales, n° 40, 2015.

LATOUR, X., *Sécurité intérieure: un droit "augmenté?*, Actualité juridique – Droit administratif (AJDA), 2018.

LAVRIC S., *Tests ADN illégaux: quelles solutions ?,* Dalloz Actualité, 2010.

LE GALÈZE, P., WESTEEL, W. I., *Conserver les documents numérisés*, in CLAERR, T., WESTEEL, I. (éd.), *Numériser et mettre en ligne*, Presses de l'Enssib, 2010.

LE MAIGAT P., *Du bon usage de la cryptologie en droit pénal*, Actu-Juridique.fr, 2022.

LE ROY, M., *Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique: analyse des articles visant à protéger les personnes physiques*, Communication – Commerce électronique, n° 2, 2025.

LECLERCQ-VANDELANNOITTE, A., ISAAC, H., *Technologies de l'information, contrôle et panoptique : pour une approche deleuzienne*, Systèmes d'information & management, 18(2), 2013.

LECUN, Y., BENGIO, Y., HINTON, G., *Deep learning*, Nature, vol.521, 2015.

LEE, J.A., LIU, C.Y*,* *Real-Name Registration Rules and the Fading Digital Anonymity in China*, Washington InternatIonal Law Journal, vol.25, no.1, 2019.

LEE, L.-H., BRAUD, T., ZHOU, P, WANG, L., XU, D., LIN, Z., KUMAR, A., BERMEJO, C., HUI, P., *All One Needs to Know about Metaverse: A Complete Survey on Technological Singularity, Virtual Ecosystem, and Research Agenda*, arXiv, 2021.

LEMAITRE, F., et al., *Comment Faire Entrer la Médecine de Précision dans la Décision Thérapeutique de Routine au Lit du Malade?*, Therapies, vol. 79, n° 1, 2024.

LÉNA M., *Conservation des empreintes génétiques en cas d'acquittement ou de classement sans suite*, Dalloz, 2008.

LEONHARD, J., *La Place de l'ADN dans le Procès Pénal*, Cahiers Droit, Sciences & Technologies, vol. 9, 2019.

LEPAGE, A., *Droit au respect de la vie privée – Quand la balance entre le droit au respect de la vie privée et la liberté d'expression penche en faveur du premier*, Communication Commerce électronique, n° 10, comm. 72, Lexis 360 Intelligence, 2023.

LEPAGE, A., *Droits de la personnalité – De certains droits de la personnalité en particulier*, Répertoire de droit civil, LexisNexis, juillet 2022 (actualisation : mars 2024).

LEPAGE, A**.**, *L'alinéa 2 de l'article 226-2-1 du Code pénal passe et obtient son brevet de constitutionnalité : Atteinte à l'intimité de la vie privée – paroles ou images présentant un caractère sexuel – QPC – principe de la légalité – interprétation*, Communication – Commerce électronique, n° 12, 2021.

LEQUESNE, C., *L'intelligence artificielle et l'ordre public,* RFDA*,* 2025.

LEQUESNE, V. C.(dir.), KELLER, J., *Surveiller les foules. Pour un encadrement des IA « physiognomoniques »*, Rapport pour l'Observatoire de l'éthique publique, 2023.

LÉVY, M., *Le numéro d'identité, Population et Sociétés*, n° 232, Paris, INED, 1989.

LÉVY, R., *Electronic Monitoring in France and Lessons Learned (2001–2004)*, Déviance et Société, vol. 28, n° 4, 2004.

LÉVY, R., *L'expérimentation du placement sous surveillance électronique en France et ses enseignements (2001–2004)*, Déviance et Société, vol. 28, n° 4, 2004.

LI, J., Z. YE, C. ZHANG, *Study on the Interaction between Big Data and Artificial Intelligence*, Systems Research and Behavioral Science (SRES*)*,2022.

LI, X., QIN, Y., *Research on Criminal Jurisdiction of Computer Cybercrime*, ScienceDirect, Elsevier, 2018.

LIEW, A., *Understanding Data, Information, Knowledge and Their Inter-Relationships*, Journal of Knowledge Management Practice, vol. 7, 2007.

LILLY, J. R., *The 2014 Council of Europe Recommendation on Electronic Monitoring: An American Perspective*, Crime Law Soc Change, vol. 62, 2014, p. 511-513.

LIMA, G., CHA, M., JEON, C., PARK, S.K., *Explaining the Punishment Gap of AI and Robots*, arXiv, 2020.

LIN, P., ABNEY, K, BEKEY, G., *Robot Ethics: Mapping the Issues for a Mechanized World*, Artificial Intelligence, vol. 175, n° 5-6, 2011.

LIU, X., TITURUS, B., JIANG, J.Z., *Generalisable Model Development for Fluid-Inerter Integrated Damping Devices*, Mechanism and Machine Theory, vol. 137, 2019.
LODDER, A. R., *Dutch Supreme Court 2012: Virtual Theft Ruling a One-Off or First in a Series?*, Journal of Virtual Worlds Research, vol. 6, no. 3, 2013.
LOHMANN M., *Roboter als Wundertüten – eine zivilrechtliche Haftungsanalyse*, Aktuelle Juristische Praxis, vol. 2, 2017.
LOISEAU, G., *La personnalité juridique des robots : une monstruosité juridique*, JCP G (La Semaine juridique – Édition générale), 2018, n° 22, Actu. 597.
LOISEAU, G., *La personnalité juridique des robots : une monstruosité juridique*, La Semaine juridique. Édition générale (JCP G), n° 22, 2018
LOISEAU, G., *La valeur contractuelle des conditions générales d'utilisation des réseaux sociaux*, Comm. com. électr., n° 7-8, 2012.
LOKIEC, P*., L'intelligence artificielle est porteuse d'une profonde transformation de l'exercice du pouvoir dans l'entreprise, Gestion du personnel*, ActuELRH, 2024.
LONGFELLOW, E., *Public, Private, and the Household in Early Seventeenth-Century England*, Journal of British Studies, vol. 45, 2006.
LUM, C., NAGIN, D.S., *Reinventing American Policing*, Crime and Justice, vol. 46, n° 1, 2017.
LYCETT, M., '*Datafication': Making sense of (big) data in a complex world*, European Journal of Information Systems, vol. 22, 2013.
LYON, D., *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007.
M'CHAREK, A., et al., *Equal before the Law: On the Machinery of Sameness in Forensic DNA Practice*, Science, Technology, & Human Values, vol. 38, n° 4, SAGE Publications, 2013.
MACIEL-HIBBARD, M., *Protection des données personnelles et cyber(in)sécurité*, Politique étrangère, Été(2), 2018.
MACKAY, A. W., *Law as an Ally or Enemy in the War on Cyberbullying*, University of New Brunswick Law Journal, vol. 66, 2015.
MAES, E., B. MINE, *Some Reflections on the Possible Introduction of Electronic Monitoring as an Alternative to Pre-trial Detention in Belgium*, Howard Journal, vol. 52, n° 2, 2013.
MAHDAVINEJAD, M. S., et al., *Machine Learning for Internet of Things Data Analysis: A Survey*, Digital Communications and Networks, vol. 4, n° 3, 2018.
MAHMUD, H., et al., *What Influences Algorithmic Decision-Making? A Systematic Literature Review on Algorithm Aversion*, Technological Forecasting and Social Change, vol. 175, 2022.
MAINZ, J. T., *Inferences and the Right to Privacy*, The Journal of Value Inquiry, 2022.
MAISNIER-BOCHÉ, L., *Données personnelles. Anonymisation : que faire pour sortir de l'impasse ?*, Expertises, 2016.

MALEK S., et al., *Legal and human rights issues in the use of electronic monitoring (using GPS 'tracking' technology) in forensic mental health settings in the UK*, Medicine, Science and the Law, vol. 63, n° 4, 2023.

MALLET-POUJOL, N., *Protection des données personnelles et droit à l'information*, LEGICOM, 59(2), 2017.

MALLET-POUJOL, N., *Vie privée et droit à l'image : les franchises de l'histoire*, Legicom, n° 20, 1999.

MANEA T., TIUGAN H. Ș., *Sancționarea exploatării sexuale prin imagini – dezideratul protecției penale și carențele incriminării*, Revista Universul Juridic, n° 6, 2023.

MANN, S., NOLAN, J., WELLMAN, B., *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, Surveillance & Society, vol. 1, n° 3, 2003.

MAPLE, C., *Security and Privacy in the Internet of Things*, Journal of Cyber Policy, vol. 2, n° 2, 2017.

MARCHAND, A., P. MARX, *Automated Product Recommendations with Preference-Based Explanations*, Journal of Retailing, vol. 96, n° 3, 2020.

MARCUS, G., *Deep Learning: A Critical Appraisal*, ArXiv preprint, 2018.

MARELLI, L., LIEVEVROUW, E., VAN HOYWEGHEN, I., *Fit for Purpose? The GDPR and the Governance of European Digital Health*, Policy Studies, vol. 41, n° 5, 2020.

MARGUÉNAUD J.-P., ROETS D., *Droits de l'Homme. Jurisprudence de la CEDH*, Revue de science criminelle et de droit pénal comparé, vol. 2015, n° 1.

MARIETTA C., MCGUIRE A. L., *Direct-to-consumer genetic testing: is it the practice of medicine?*, Journal of Law, Medicine & Ethics, vol. 37, n° 2, 2009.

MARINO L., *Le droit d'accès à internet, nouveau droit fondamental*, Recueil Dalloz, 2009.

MARKLUND, F., S. HOLMBERG, *Effects of Early Release from Prison Using Electronic Tagging in Sweden*, Journal of Experimental Criminology, vol. 5, 2009.

MARON, A., *Quis custodiet ipsos custodes?*, Droit pénal, LexisNexis, n° 5, 2023.

MARTI G., CLUZEL MÉTAYER L., MERABET S., *Intelligence artificielle – Droit et intelligence artificielle*, JCP éd. gén., n° 25, 2024.

MARTINEZ, M., J., ALDEA, A., *Emotions in human and artificial intelligence*, Computers in Human Behavior, vol. 21, 2005.

MARTINEZ, V. J., *La conception française des « surtransposition s » des directives,* RDP 2021.

MARTINEZ-ARANDA, M. G., *Extended Punishment: Criminalising Immigrants through Surveillance Technology*, Journal of Ethnic and Migration Studies, vol. 48, n° 1, 2020.

MARTÍNEZ-DÍAZ, M., SORIGUERA, F., *Autonomous Vehicles: Theoretical and Practical Challenges*, Transportation Research Procedia, vol. 33, 2018.

MARY L., *Présentation de la loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales*, AJ fam., 2020.

MASCALA, C., *Consentement de la victime*, in *JurisClasseur Pénal Code*, App. art. 122-4 à 122-7, fasc. unique, LexisNexis, 1re publ., 2013.

MASSIS DE SOLERE, C., *La délicate frontière entre le délit d'usurpation d'identité numérique et la loi de 1881*, Légipresse, 2019.

MASTOPOULOU H., *La transposition dans le droit permanent des principales mesures de l'État d'urgence*, JCP, 2017.

MATTHIAS, A., *The Responsibility Gap: Ascribing Responsibility for the Actions of Learning Automata*, Ethics and Information Technology, vol. 6, 2004.

MATTHIOS, F. J., *Le Parlement autorise une expérimentation de caméras dites "augmentées": enjeux et garanties*, Revue pratique de la prospective et de l'innovation, n° 1, 2023, dossier 5, 2023.

MAURI, L., DAMIANI, E., *Hardening Behavioral Classifiers Against Polymorphic Malware: An Ensemble Approach Based on Minority Report*, Information Sciences, vol. 689, 2025.

MAYAUD Y., *Perte et violation du domicile conjugal*, Dalloz Actualité, 1997.

MCCALLUM, A., *Information Extraction: Distilling Structured Data from Unstructured Text*, Queue, vol. 3, n° 9, 2005.

MCCORNACK, S. A., *Information Manipulation Theory*, Communications Monographs, 1992.

McNAIR, A. D., *The Functions and Differing Legal Character of Treaties*, British Yearbook of International Law, vol. 11, 1930.

MEHTA, P., et al., *Can Deepfakes Be Created on a Whim?*, Companion Proceedings of the ACM Web Conference 2023 (WWW '23 Companion), Association for Computing Machinery, 2023.

MEHTA, P., et al., *Ethics Committees: Structure, Roles, and Issues*, Journal of Korean Medical Science, vol. 38, n° 25, 2023.

MELLERAY, F., *Relativité des exigences de la dignité de la personne humaine*, Actualité juridique. Droit administratif (AJDA), 2024.

MÉNARD, A., *La garantie des droits fondamentaux dans les États d'exception sous la Ve République,* Revue française de droit constitutionnel, 128(4), 2021.

MERABET, S., *Des vertus et des vices du règlement sur l'intelligence artificielle*, Recueil Dalloz, n° 41, 2024.

MERABET, S., *Vers un droit de l'intelligence artificielle*, Paris, Dalloz, coll. Nouvelle Bibliothèque de Thèses (NBT), 2020.

MEYNAUD-ZEROUAL, A., *Roger Latournerie, itinéraire d'une conscience juridique au service de l'État*, Revue française de droit administratif (RFDA), 2017.

MILANOVIC M., *Human rights treaties and foreign surveillance: privacy in the digital age*, Harvard International Law Journal, vol. 56, 2015.

MIRANDA V. D., *Détention provisoire et surpopulation carcérale*, AJ pénal, 2018.

MIRKOVIC A., *La ratification (enfin !) de la convention d'Oviedo sur les droits de l'homme et la biomédecine*, Recueil Dalloz, 2012.

MOLINER-DUBOST, M., *Le Droit à l'Oubli Génétique*, Journal International de Bioéthique et d'Éthique des Sciences, vol. 31, n° 2, 2019.

MONAHAN, J., SKEEM, J.L., *Risk Assessment in Criminal Sentencing*, Annual Review of Clinical Psychology, vol. 12, 2016.

MONOT-FOULETIER, M., CLÉMENT, M., *Véhicule autonome : vers une autonomie du régime de la responsabilité civile ?*, Dalloz, 2018.

MONTECLER M.-C., *Conservation des données: la Cour de justice de l'Union européenne persiste et signe*, Dalloz, 2022.

MOORE, M., *Fake Accounts on Social Media, Epistemic Uncertainty and the Need for an Independent Auditing of Accounts*, Journal of Media Studies, 2023.

MOPARI, B., S. G. PUKALE et M. L. DHORE, *Detection and Defense Against DDoS Attack with IP Spoofing*, 2008 International Conference on Computing, Communication and Networking, 2008.

MOURON P., *Coronavirus et fausses informations. Les aléas de la liberté d'expression en période de crise sanitaire*, RDLF, 2020.

MOURON P., *La loi visant à sécuriser et à réguler l'espace numérique est promulguée*, Revue européenne des médias et du numérique, n° 69-70, 2024.

MOUSSA T., BOURDILLAT J.-J., *L'expulsion d'un époux du domicile conjugal: des procédures civiles d'exécution au droit pénal*, Procédures, 2002.

MUHANNA S. E. J., *Penal protection of the right to digital oblivion*, 3rd International Humanitarian Conference, vol. 1, n° 1, Baghdad, 2024.

MUREȘAN A., *Violarea vieții private în noul Cod penal*, Caiete de drept penal, n° 3, 2012.

MURPHY, R., D. WOODS, *Beyond Asimov: The Three Laws of Responsible Robotics*, IEEE Intelligent Systems, vol. 24, 2009.

MUSSON M., MOULIN J., JOSSERAND L., *Loi SREN : renforcement des pouvoirs de l'ARCOM et de la CNIL au service de la protection des internautes*, Dalloz Actualité, 2024.

NAEF, T., *The Global Reach of the Right to Data Protection*. en: *Data Protection without Data Protectionism*, European Yearbook of International Economic Law, vol 28. Springer, 2023.

NAGAR, G., *The Evolution of Ransomware: Tactics, Techniques, and Mitigation Strategies*, SSRN, 2024.

NARAYANAN, A., SHMATIKO, V., *Robust De-Anonymization of Large Sparse Datasets*, IEEE Symposium on Security and Privacy (S&P 2008), Oakland, CA, États-Unis, 2008.

NEFF, G., NAGY, P., *Talking to Bots: Symbiotic Agency and the Case of Tay*, International Journal of Communication, vol. 10, 2016.

NELLIS, M., *Understanding the Electronic Monitoring of Offenders in Europe: Expansion, Regulation and Prospects*, Crime, Law, and Social Change, vol. 62, 2014, p. 489-510.

NERANTZI, E., SARTOR, G., *"Hard AI Crime": The Deterrence Turn*, Oxford Journal of Legal Studies, vol. 44, n° 3, 2024, p. 673-701.

NESTOR R. A., *Utilizarea datelor stocate în Sistemul național de date genetice judiciare : restrângere necesară adusă vieții private sau protecție dincolo de limitele convenționale ?*, Jessentials, 2024.

NEVEJANS N., *L'appréhension de l'IA générative par le règlement sur l'IA*, Dalloz IP/IT, 2024.

NGUYEN, T. T., et al., *Deep Learning for Deepfakes Creation and Detection: A Survey*, Computer Vision and Image Understanding, 2022.

NICAUD B., *Restrictions à la conservation des données de connexions et à leur accès : la Cour de cassation tire les conséquences de la jurisprudence de la CJUE*, Dalloz, 2022.

NIORÉ V., DUSSEAU L., *Le cœur de la Défense*, Gaz. Pal., éd. Prof., 2015.

NISHNIANIDZE, A., *Surveillance in the Digital Age*, European Scientific Journal, vol. 20, 2024.

NISSENBAUM, H., *Privacy in Context, Technology, Policy and the Integrity of Social Life*, Standford University Press, 2010.

NISTOR, S., et al., *Building a Twitter Sentiment Analysis System with Recurrent Neural Networks*, Sensors, vol. 21, 2021.

NITSCH, N*., L'inflation juridique et ses conséquences*, Archives de philosophie du droit, 1982.

NKONGOLO, M., *Navigating the Complex Nexus: Cybersecurity in Political Landscapes*, arXiv, 2023.

NORTH-SAMARDZIC, A., *Biometric Technology and Ethics: Beyond Security Applications*. Journal of Business Ethics vol.167, no. 3, 2020.

NOTHAFT, E., *Medieval Europe's Satanic Ciphers: On the Genesis of a Modern Myth*, British Journal for the History of Mathematics, vol. 35, n° 2, 2020.

O'FLYNN M. A., *Harmonisation and cybercrime jurisdiction: uneasy bedfellows? An analysis of the jurisdictional trajectories of the Council of Europe's Cybercrime Convention*, Queen Mary University of London, 2015.

OCHOA, N., *Pour en finir avec l'idée d'un droit de propriété sur ses données personnelles : ce que cache véritablement le principe de libre disposition*, Revue française de droit administratif (RFDA), 2015.

OHM, P., *Broken Promises of Privacy : Responding to the Surprising Failure of Anonymization*, UCLA Law Review, vol. 57, 2010.

OLIVIER DE MAISON ROUGE, *Le droit français du renseignement – Sect. 2 : Techniques de renseignement prévues par la loi*, Dalloz, 2019.

ONSTWEDDER, S.M., JANSEN, M.E., CORNEL, M.C., RIGTER, T., *Policy. Guidance for Direct-to-Consumer Genetic Testing Services: Framework Development Study*, Journal of Medical Internet Research, vol. 26, 2024.

ORTIZ-FREULER, J., *Datafication, Identity, and the Reorganization of the Category Individual*, Temple Law Review, vol. 65, n° 4, 2023.

OST F., GARAPON A., LASSÈGUE J., *Justice digitale. Révolution graphique et rupture anthropologique*, Paris, PUF, Revue interdisciplinaire d'études juridiques, vol.81(2), 2018.

ØSTER M. K., ROKKAN T., *The Norwegian approach to electronic monitoring: changing the system and making a difference*, Federal Sentencing Reporter, vol. 31, n° 1, 2018.

OVIEDO-TRESPALACIOS, O., et al., *The Risks of Using ChatGPT to Obtain Common Safety-Related Information and Advice*, Safety Science, vol. 167, 2023.

PAGE J. A., *Liability for unreasonably and unavoidably unsafe products: does negligence doctrine have a role to play*, Georgetown Law Faculty Publications, vol. 1141, 1996.

PALOMBO D., *Extraterritorial, universal, or transnational human rights law?*, Israel Law Review, vol. 56, n° 1, 2023.

PAMART D., *FAED et FNAEG à l'épreuve du droit de l'Union*, Dalloz, 2024.

PAN, Z., et al., *Data- and Management-Driven Metaverse Research*, Data Science and Management, vol. 7, n° 2, 2024.

PASTOR J.-M., *Loi bioéthique : le gouvernement avance avec précaution*, Dalloz Actualité, 2019.

PATEL S., VARLEY I., *Exploring the regulation of genetic testing in sport*, The Entertainment and Sports Law Journal, vol. 17, n° 1, 2019.

PAUTREL V. C., PARTOUCHE B., *Le voyeur et le droit pénal : quelle qualification se cache sous les jupes des filles ?*, Gazette du Palais, 2012.

PAYNE, B. K., D. C. MAY, P. B. WOOD, *The "Pains" of Electronic Monitoring: A Slap on the Wrist or Just as Bad as Prison?*, Criminal Justice Studies, vol. 27, n° 2, 2014.

PELLETIER H, BEAUVAIS D., *Art. 226-1 à 226-3-1*, *Fasc. 20* : *Atteinte à la vie privée – Enregistrement de la parole ou de l'image – Fabrication, détention, location ou vente d'appareils d'enregistrement*, JurisClasseur Pénal Code Lexis 360 Intelligence, 2022.

PELTIER, V., *Détention. – Exécution des peines privatives de liberté. – Surveillance judiciaire des auteurs de crimes et délits sexuels*, in JurisClasseur Procédure pénale, art. 723-29 à 723-37, fasc. 20, LexisNexis, 1re publ. 2011.

PERCONTI, P., PLEBE, A., *Deep Learning and Cognitive Science*, Cognition, vol. 203, 2020.

PERETTI M., *Le bracelet électronique : boulet moderne ou outil d'insertion ?*, AJ pénal, 2007.

PÉREZ LAGOS, C*., Rendre visibles les conséquences de la surveillance numérique : le cas du "scandale" Cambridge Analytica* , Communication, vol. 37, n° 2, 2020.

PERRAY, R, *Données à caractère personnel. – Bases juridiques applicables aux traitements de données à caractère personnel. Dispositions spécifiques imposant le recueil du consentement*, Répertoire de droit civil, Dalloz, Fasc. 932-72, 1re ed., 2025.

PERRIAULT, J., ARNAUD, M., JUANALS, B., *Les identifiants numériques humains : éléments pour un débat public*, Les Cahiers du numérique, 3(2), 2002.

PERRIER J.-B., ROUSSEAU F., *Revue de droit science criminelle et de droit pénal comparé*, Lefebvre Dalloz, Doctrine 243, 2024.

PERRIER, J.-B**.**, *Faits justificatifs – Lanceur d'alerte*, JurisClasseur Pénal Code, art. 122-9, fasc. 20, LexisNexis, 1re publ., 2024.

PESTER R., *Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act (BIPA) Violation Suit*, Harvard Law School – JOLT Digest, 2020.

PETERSEN, M. B., OSMUNDSEN, M., ARCENEAUX, *K., "Need for Chaos" and the Sharing of Hostile Political Rumours in Advanced Democracies*, PsyArXiv Preprints, 2018.

PETIT, *Guided Tour of the Cybercriminal Dark Web*, Dalloz IP/IT, n° 2, févr. 2017.

PHILLIPS, A. M., *Only a Click Away – DTC Genetics for Ancestry, Health, Love… and More: A View of the Business and Regulatory Landscape*, Applied & Translational Genomics, vol. 8, 2016.

PICARD, R., *Médecine personnalisée : de quoi parle-t-on ? Une vision prospective*, Annales des Mines – Réalités industrielles, nov. 2014(4).

PIERRON, J.-P., *Le chemin trouble du consentement. Du consentement formel au consentement existentiel*, Les Cahiers de la Justice, vol. 4, n° 4, 2021.

PIN, X., *Le consentement à la lésion de soi-même. Vers la reconnaissance d'un fait justificatif?*, Droits, n° 49, 2009.

PIREYRE, B., *Allocution d'ouverture*, in BLANC, N., MEKKI, M. (dir.), *Le juge et le numérique : un défi pour la justice du XXIe siècle*, Paris, Dalloz, 2019.

PLAISANT O., GUERTAULT J., COURTOIS R., RÉVEILLÈRE C., MENDELSOHN G. A., JOHN O. P., *Histoire des « Big Five »: OCEAN des cinq grands facteurs de la personnalité. Introduction du Big Five Inventory français ou BFI-Fr*, Annales Médico-psychologiques, vol. 168, n° 7, 2010.

PLANQUE, V. J.-C., *Robotum delinquere potest ? L'intelligence artificielle et la responsabilité pénale*, Droit pénal, 2022, n° 6, Étude 14.

PLÖCKINGER, U., ERNST-AUGA, U., *Bioethics and the Human Body*, Religions, vol. 15, 2024.

POLLOCK F., *Has the common law received the fiction theory of corporations?*, Law Quarterly Review, vol. 27, 1911.

POPEL, M., et al., *Transforming Machine Translation: A Deep Learning System Reaches News Translation Quality Comparable to Human Professionals*, Nature Communications, vol. 11, 2020.

PORRET, M., *Panoptique, de Jeremy Bentham*, Mensuel, n° 468, 2020.

PORTMESS, L., TOWER, S., *Data Barns, Ambient Intelligence and Cloud Computing: The Tacit Epistemology and Linguistic Representation of Big Data*, Ethics and Information Technology, vol. 17, n° 1–9, 2015.

POSTMES,T., SPEARS, R., *Deindividuation and Antinormative Behavior: A Meta-Analysis*, Psychological Bulletin, 1998.

POULLET, Y., *Le RGPD face aux défis de l'intelligence artificielle*, Bruxelles, Larcier, coll. CRIDS, 2020.

PRADEL J., *Un exemple de restauration de la légalité criminelle: le régime des interceptions de correspondances émises par la voie des télécommunications (commentaire de la loi n° 91-646 du 10 juillet 1991)*, Recueil Dalloz, 1992.

PRADEL,J*., La réforme de la détention provisoire (commentaire de la loi n. 70-643 du 17 juillet 1970),* Gaz. Pal. 1972.

PRINCE J. T., WALLSTEN S., *How much is privacy worth around the world and across platforms?*, Journal of Economic Management Strategy, Wiley, 2019.

PRINCE, A. E. R., *Disclosing Privacy and Discrimination Protections in Informed Consent*, Health Matrix, vol. 33, 2023.

PRIOU-ALIBERT L., *Précisions sur l'élément intentionnel du délit d'atteinte au secret des correspondances*, Dalloz Actualité, 2018.

PROVOST, F., T. FAWCETT, *Data Science and Its Relationship to Big Data and Data-Driven Decision Making*, Big Data, vol. 1, n° 1, 2013.

PUGLISI, S., D. REBOLLO-MONEDERO, J. FORNÉ, *On the Anonymity Risk of Time-Varying User Profiles*, Entropy, vol. 19, n° 5, 2017.

PUIGELIER, C**.**, note sous N. Anciaux*, Essai sur l'être en droit privé,* thèse de droit privé, dir. B. Teyssié, Université Panthéon-Assas (Paris II), 2018, 607 p., Revue trimestrielle de droit civil (RTD civ.), 2019.

PY B., *Secret professionnel: le syndrome des assignats ?*, Actualité juridique pénal, vol. 4, 2004.

QUÉMÉNER M., *Haine en ligne: présentation de la circulaire du Garde des Sceaux relative à la lutte contre ce fléau*, Dalloz IP/IT, 2021.

RABEHARISOA V., PATERSON F., *Matérialité et juridicité: à propos du fichier national automatisé des empreintes génétiques*, Droit et société, vol. 110, 2022.

RANQUET, M., *Le droit à l'oubli : vers un nouveau droit fondamental de l'individu?*, Communications, no 104, 2019.

RAPPORT D'INFORMATION n° 441 (2008-2009), *La vie privée à l'heure des mémoires numériques. Pour une confiance renforcée entre citoyens et société de l'information*, Commission des lois, Sénat, 2009.

REAY, I., S. DICK, J. MILLER, *A Large-Scale Empirical Study of P3P Privacy Policies: Stated Actions vs. Legal Obligations*, ACM Transactions on the Web (TWEB), vol. 3, n° 2, 2009.

RECOTILLET M., *FNAEG (refus du prélèvement) : respect au droit à la vie privée*, Dalloz, 2019.

REHMA, A. A., AWAN, M.J., BUTT, I., *Comparison and Evaluation of Information Retrieval Models*, VFAST Transactions on Software Engineering, vol. 6, n° 1, 2018.

REIDENBERG, J. R., *Lex Informatica: The Formulation of Information Policy Rules through Technology* , vol.76, Tex. L. Rev. 553, 1997-1998.

REIS, O, et all., *Privacy law challenges in the digital age: a global review of legislation and enforcement*, International Journal of Applied Research in Social Sciences, vol.6, no.1, 2024.

REISMAN S., SILVER J., SHAH R., *R. v. Jarvis: privacy is not an "all-or-nothing" concept*, Ontario Bar Association, 2019.

RENZEMA, M., E. MAYO-WILSON, *Can Electronic Monitoring Reduce Crime for Moderate to High-Risk Offenders?*, Journal of Experimental Criminology, vol. 1, 2005, p. 215–237.

RÉPERTOIRE DE DROIT PÉNAL ET DE PROCÉDURE PÉNALE, *Fichier national des empreintes génétiques*, chap. 2, sect. 3, art. 1, Paris, Dalloz, 2020.

RÉSEAUX, *Protéger la vie privée à l'ère numérique*, Réseaux, vol. 189, n° 1, 2015.

RICHARD, J., *Le numérique et les données personnelles : quels risques, quelles potentialités ?,* Revue du droit public, 2016.

ROBERTS, J. S., J. OSTERGREN, *Direct-to-Consumer Genetic Testing and Personal Genomics Services: A Review of Recent Empirical Studies*, Current Genetic Medicine Reports, vol. 1, n° 3, 2013.

ROCHER L., HENDRICKX J. M., DE MONTJOYE Y.-A., *Estimating the success of re-identifications in incomplete datasets using generative models*, Nature Communications, vol. 10, n° 3069, 2019.

ROCHFELD, J., *Données à caractère personnel – Données des mineurs* , Répertoire IP/IT et Communication, LexisNexis, 2025.

ROGISTER J., *Venality: the sale of offices in eighteenth-century France*, American Journal of Legal History, vol. 42, n° 3, 1998.

ROJSZCZAK M., *Extraterritorial bulk surveillance after the German BND Act judgment*, European Constitutional Law Review, vol. 17, n° 1, 2021.

ROSE, D., *Faut-il une responsabilité pénale appliquée à l'intelligence artificielle?*, Dalloz IP/IT, n° 11, 2024.

ROSENBLATT, F., *Principles of neurodynamics : perceptrons and the theory of brain mechanisms*, Spartan Books, 1962.

ROSENTHAL, J.-L., *The Fruits of Revolution: Property Rights, Litigation, and French Agriculture, 1700–1860*, The Journal of Economic History, vol. 50, n° 2, 1990.

ROTHENBERG, K. H., et S. F. TERRY, *Human Genetics: Before It's Too Late—Addressing Fear of Genetic Information*, Science, vol. 297, n° 5579, 2002.

ROUVROY, A., BERNS, T., *Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ?*, Réseaux, n° 177, 2013.

ROUVROY, A., et al., *Gouvernementalité algorithmique et perspectives d'émancipation: Le disparate comme condition d'individuation par la relation?*, Réseaux, vol.1 ,n°177, 2013.

RUBINSTEIN, I., *Big Data: The End of Privacy or a New Beginning?*, International Data Privacy Law*,* vol. 3, 2013.

SAENKO, V. L., DETRAZ, S., *La loi nº2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes : les femmes et les enfants d'abord,* Dalloz. 2018

SAINT-PAU J.-Ch., *Droit au respect de la vie privée et droit pénal*, Dr. pénal, 2011.

SAINT-PAU J.-Ch., *Jouissance des droits civils: régime, actions*, Lexis 360 Intelligence, JurisClasseur Code civil, fasc. 20.

SAINT-PAU J.-Ch., *L'article 9 du Code civil : matrice des droits de la personnalité*, Recueil Dalloz, vol. 37, 1999.
SAINT-PAU J.-Ch., *L'enregistrement clandestin d'une conversation téléphonique amicale relative à l'activité professionnelle*, Recueil Dalloz, 2007, n° 17.
SAINT-PAU J.-Ch., *Le délit d'atteinte à l'intimité de la vie privée exige-t-il une atteinte effective à l'intimité de la vie privée ?*, Dalloz, 1999.
SAINT-PAU J.-Ch., *Les investigations numériques et le droit au respect de la vie privée*, AJ pénal, 2017.
SAINT-PAU J.-Ch., *Répertoire V° Vie privée, Fasc. 15 â: Jouissance des Droits civils. „Droit au respect de la vie privée. Consentement à une atteinte à la vie privée ,*JurisClasseur notarial, Lexis 360 Intelligence, 2017.
SAINT-PAU, J.-Ch., *Jouissance des Droits Civils, Droit au respect de la vie privée: Régime, Actions*, Lexis 360 Intelligence - JurisClasseur Civil Code - Encyclopédies - Art. 9 - Fasc. 20, 2024.
SAINT-PAU, J.-Ch., *L'Enregistrement Clandestin d'une Conversation Téléphonique Amicale Relative à l'Activité Professionnelle*, Recueil Dalloz, n° 17, 2007.
SAINT-PAU, J.-Ch., *L'article 9 du Code Civil: Matrice des Droits de la Personnalité*, Recueil Dalloz, vol. 37, 1999.
SAINT-PAU, J.-Ch., *Le Délit d'Atteinte à l'Intimité de la Vie Privée Exige-t-il une Atteinte Effective à l'Intimité de la Vie Privée?*, Dalloz, 1999.
SAINT-PAU, J.-Ch., *Les investigations numériques et le droit au respect de la vie privée*, AJ pénal, 2017.
SAINT-PAU, J.-Ch., *Vie Privée*, JurisClasseur Notarial Répertoire, Fasc. 15 â., 2024.
SALVAGE, Ph., *Le consentement en droit pénal*, Revue de science criminelle et de droit pénal comparé, 1991.
SANDERS M., *Genomic research in Indian Country: the new road to termination?*, Oklahoma City University Law Review, vol. 39, 2014.
SANFILIPPO, P. G., et al., *Current Landscape of Direct-to-Consumer Genetic Testing and Its Role in Ophthalmology: A Review*, Clinical and Experimental Ophthalmology, 2015.
SANLAVILLE, D., et al., *Plan France médecine génomique 2025: La France entre dans l'ère de la médecine génomique*, La Revue du Praticien, vol. 71, n° 10, 2021.
SARITEPECI, M., et al., *The Role of Digital Literacy and Digital Data Security Awareness in Online Privacy Concerns: A Multi-Group Analysis with Gender*, Online Information Review, vol. 48, n° 5, 28 février 2024,.

SARKER, I. H., *Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions*, SN Computer Science, vol. 2, 2021.

SARKER, I. H., *Machine Learning: Algorithms, Real-World Applications and Research Directions*, SN Computer Science, vol. 2, n° 3, 2021.

SARKER, I., M. FURHAD, R. NOWROZY, *AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions*, SN Computer Science, vol. 2, 2021.

SAULIER, M., *Garantir le respect du droit à l'image des enfants : un objectif ambitieux, une efficacité douteuse?*, AJ famille, 2024.

SAUVAGE, G., *Quel(s) outil(s) juridique(s) contre la diffusion de "fake news"?*, Légipresse, 2017.

SAVA, R., *Protecția datelor în România prin Regulamentul GDPR : care sunt cele mai importante aspecte ?*, LegalUp, 2 2023.

SAVATIER, R., *L'inflation législative et l'indigestion du corps social*, Dalloz, Chronique, n° 43, 1977.

SCANTAMBURLO, T., et al., *Artificial Intelligence across Europe: A Study on Awareness, Attitude and Trust*, arXiv, 2023.

SCHAFER, B., *The German Constitutional Court on the right in confidentiality and integrity of information technology systems – a case report on BVerfG, NJW 2008, 822*, SCRIPT-ed, 2009.

SCHALLER, C., *Strategic surveillance and extraterritorial basic rights protection: German intelligence law after Snowden*, German Law Journal, vol. 19, 2018.

SCHMIDHUBER, J., *Deep Learning in Neural Networks: An Overview*, Neural Networks, vol. 61, 2015.

SCOTT, C. R., *To Reveal or Not to Reveal: A Theoretical Model of Anonymous Communication*, Communication Theory vol. VIII, n° 4, 1998.

SEARLE, R., *Minds, brains, and programs*, *Behavioral and Brain Sciences*, vol. 3, no. 3, 1980.

SEILLER, B., La notion de police administrative, *Revue française de droit administratif* (RFDA), 2015.

SEISSA, I. G., *Cyber-Terrorism: Definition, Patterns, and Mitigation Strategies: A Literature Review,* International Journal of Science and Research (IJSR*)*, vol. 6, n° 1, 2017.

SELBST, A. D., *Disparate impact in big data policing*, Georgia Law Review, vol. 52, 2017.

SELBST, A. D., *Negligence and AI's human users*, Boston University Law Review, vol. 100, 2020.

SELMY, H. A., et al., *Big Data Analytics Deep Learning Techniques and Applications: A Survey*, Information Systems*,* vol. 120, 2024.

SELTZER, W., ANDERSON, M., *The dark side of numbers: the role of population data systems in human rights abuses*, Social Research, vol. 68, n° 2, 2001.

SEONGHAK, K., *L'écologie déséquilibrante de l'oubli chez Homo Numericus*, Sociétés, n° 116, 2012.

SERINET, D., *L'instauration d'une répression des atteintes à l'intimité sexuelle par la loi pour une République numérique*, Point de vue, 2016.

SEUVIC, J., *André Vitu (6 juillet 1920 - 27 octobre 2013)*, Revue de science criminelle et de droit pénal comparé, vol. 4, n° 4, 2013.

SHAH, M., SUREJA, N., *A Comprehensive Review of Bias in Deep Learning Models: Methods, Impacts, and Future Directions*, Archives of Computational Methods in Engineering, 2024.

SHARKEY, A., N. SHARKEY, *We Need to Talk About Deception in Social Robotics!*, Ethics and Information Technology, vol. 23, 2021.

SHIRI, M., F. PERUMAL, T. M. RAIHANI*, A Comprehensive Overview and Comparative Analysis on Deep Learning Models: CNN, RNN, LSTM, GRU,* Journal of Artificial Intelligence, 2023.

SILVER, D., HUAN, A., MADDISON, C., *et al*., *Mastering the game of Go with deep neural networks and tree search*. Nature, vol.529, 2016.

SIMESTER, A.P, von HIRSCH, A., Hirsch, *Crimes, Harms, and Wrongs: On the Principles of Criminalisation*, Oxford, Hart Publishing, 2011.

SIMITIS, S., *Reviewing Privacy in an Information Society*, University of Pennsylvania Law Review, vol. 135, nr. 3, 1987.

SIMON, D., *Directive*, Répertoire de droit européen, Dalloz, n° 76, 2018.

SIMON, D., *La "surtransposition" du droit de l'Union: mythe ou réalité ?*, Europe, Mensuel d'actualité du droit de l'Union européenne, LexisNexis, n° 12, 2024.

SINGH, S., S. PANWAR, H. DAHIYA, K. KHUSHBOO, *Artificial Intelligence Voice Assistant and Home Automation*, International Journal of Science and Research Archive, vol. 12, 2024, p. 2006-2017.

SLĂVOIU R., *Infracțiunea de violarea vieții private – o noutate în legislația penală din România*, Dreptul, n° 10, 2013.

SMART, W. D., C. GRIMM, W. HARTZOG, *An Education Theory of Fault for Autonomous Systems*, Notre Dame Journal on Emerging Technologies, vol. 33, 2021.

SMIRNOVA, Y., TRAVIESO-MORALES, V., *Understanding challenges of GDPR implementation in business enterprises: a systematic literature review,* International Journal of Law and Management*,* vol. 66, n° 3, 2024.

SOLAIMAN, S. M., *Legal Personality of Robots, Corporations, Idols and Chimpanzees: Quest for Legitimacy*, Artificial Intelligence and Law, vol. 25, n° 2, 2017.
SOLUM, L. B., *Legal personhood for artificial intelligences,* North Carolina Law Review, vol. 70, n° 4, 1992.
SOLUM, L. B., *Legal personhood for artificial intelligences*, North Carolina Law Review, vol. 70, 1992, p. 1231.
SONTAG-KOENIG, S., *Sonorisation et fixation d'images : que reste-t-il de la vie privée ?*, AJ pénal, 2023.
SORDINA, M.-C., *Les collectivités territoriales face au risque pénal en cas d'atteinte à la cybersécurité,* La Semaine juridique – Administrations et collectivités territoriales, n° 21, 27 mai 2024, étude 2150.
SOSKIN, I., « *Atteinte à l'intimité de la vie privée : dans l'attente de la loi pour une République numérique, débats autour de l'interprétation de l'article 226-1 du Code pénal, Cour de cassation (crim.), 16 mars 2016, n° 15-82.676* », Légipresse, 2016.
SPARROW B., LIU J., WEGNER D. M., *Google Effects on Memory: Cognitive Consequences of Having Information at Our Fingertips*, Science, vol. 333, n° 6043, 2011.
SPENCER, J. R., M.-A. BRAJEUX, *Criminal Liability for Negligence—A Lesson from Across the Channel?*, The International and Comparative Law Quarterly, vol. 59, n° 1, 2010.
STARR, S. B., *Evidence-Based Sentencing and the Scientific Rationalization of Discrimination*, Stanford Law Review, vol. 66, 2014.
STEEL, C. M., *Technical Soddi Defenses: The Trojan Horse Defense Revisited*, Journal of Digital Forensics, Security and Law, vol. 9, n° 4, 2014.
STEINERTE, E., D. van ZYL SMIT, S. SNACKEN, *Principles of European Prison Law and Policy: Penology and Human Rights*, Human Rights Law Review, vol. 11, n° 2, 2011.
STIEGLITZ, S., M. MIRBABAIE, B. ROSS, C. NEUBERGER, *Social Media Analytics: Challenges in Topic Discovery, Data Collection, and Data Preparation*, International Journal of Information Management, vol. 39, 2018.
SULE, M.-J., M. ZENNARO, G. THOMAS, *Cybersecurity through the Lens of Digital Identity and Data Protection: Issues and Trends*, Technology in Society, vol. 67, nov. 2021.
SULER, J., *The Online Disinhibition Effect*, Cyberpsychology & Behavior, vol. 7, n° 3, 2004.
SULLIVAN, C., *The Future of Foreign Intelligence, Privacy and Surveillance in a Digital Age by Laura K. Donohue,* Oxford University Press, 2016.
SUPIOT, E., *Empreintes génétiques et droit pénal: quelques aspects éthiques et juridiques*, Revue de Science Criminelle et de Droit Pénal Comparé, vol. 2015, n° 4, 2015, p. 827-835.
SURREL, H., *Droit à l'effacement et liberté de la presse,* JCP, 2018.

SUSEN, S., *A new structural transformation of the public sphere? With, against, and beyond Habermas*, Society, vol. 60, 2023.

SWEENEY, L., *Simple Demographics Often Identify People Uniquely*, Data Privacy Working Paper 3, Carnegie Mellon University, Pittsburgh, 2000.

SYLVESTER, D. J., Lohr, S., "*The Security of Our Secrets: A History of Privacy and Confidentiality*", in Law and Statistical Practice, Denver University Law Review, vol. 83, 2005.

SZNYCER, D., CARLTON, P., *The origins of criminal law*, Nat Hum Behav, vol.4, 2020.

TADDEO, M., L. FLORIDI, *The case for e-trust*, Ethics and Information Technology, vol. 13, 2011.

TAHRI C., *Les limites à la confidentialité des correspondances de l'avocat*, La Lettre juridique, 2010.

TALEB KARLSONN A., *La procédure pénale numérique*, Colloque Doctoriales, Toulon, 2021.

TANGHE, H., GIBERT, P. O., *L'enjeu de l'anonymisation à l'heure du big data*, Revue française des affaires sociales, 2017.

TAQUET F, *Trib. police Paris, 25 mai 1984 ; Ministère public c. Nanos*, Lexis 360 Intelligence, La Semaine Juridique - Édition générale, n° 6, du 5 février 1986.

TATARINOV, M., *The territorial jurisdiction principle in theoretical and comparative law aspects*, International Public and Private Law, vol. 1, 2021.

TELLIER-CAYROL V., *Loi du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes*, AJ pénal, 2018.

TENE, O., J. POLONETSKY, *Big data for all: privacy and user control in the age of analytics*, Northwestern Journal of Technology and Intellectual Property, vol. 11, n° 5, 2013.

TEXIER, B., *Anonymisation et pseudonymisation au cœur de l'open data judiciaire*, Archimag, 368(8), 2023.

TEXIER, B., *Anonymisation et pseudonymisation au cœur de l'open data judiciaire*, Archimag, 368(8), 2023.

THÉVENOT, F., *L'open data et la justice prédictive*, in FERRAND, F., KNETSCH, J., ZWICKEL, M. (dir.), *Le droit civil et la justice civile à l'ère de la numérisation en France et en Allemagne*, Erlangen, FAU University Press, 2020.

THOMASEN, K., S. DUNN, *Reasonable expectations of privacy in an era of drones and deepfakes: expanding the Supreme Court of Canada's decision in R v Jarvis*, ResearchGate, 2021.

THOMAZ, F., *The Digital and Physical Footprint of Dark Net Markets*, Journal of International Marketing, vol. 28, n° 1 (special issue), 2020.

THORNHILL, C., *Before the Law?, in The Sociology of Law and the Global Transformation of Democracy,* Cambridge, Cambridge University Press, 2018.

THOUVENIN, D., *Les lois françaises de bioéthique: leur construction, leurs évolutions*, Médecine/Sciences, vol. 35, 2019.

TOMKINS, A., *Intercepted evidence: now you hear me, now you don't*, The Modern Law Review, vol. 57, 1994.

TONRY, M., *Prediction and Incapacitation,* in *Doing Justice, Preventing Crime*, Oxford Academic, 2020.

TOWNEND, D., TAYLOR, M. J., WRIGHT, J., et al., *Privacy interests in biobanking: a preliminary view on a European perspective*, Taylor and Francis, 2016.

TRANDAFIR, A.-R., *Violarea sediului profesional. Obiectul protecției. Comparație cu violarea de domiciliu*, Analele Științifice ale Universității „Alexandru Ioan Cuza" din Iași, Științe juridice, vol. LXVII, n° 2, 2021.

TROPINA T., *Structura în evoluție a criminalității online : cum se organizează criminalitatea cibernetică*, Rev. Eucrim, n° 4, 2012.

TRUBOWITZ, A., *Montesquieu's gentle prince: the law of majesty and the moderation of despotism in The Spirit of the Laws*, History of European Ideas, vol. 44, 2017.

TRUCHET D., *Correspondance et communication*, Dalloz, 2014.

TUDORAN, M.V., *Analiza modificărilor aduse de Legea nr. 201/2023 în materia supravegherii tehnice*, Dreptul, n° 1, 2025.

TURGIS, S., *La Convention européenne des droits de l'homme et la protection des droits et libertés à l'ère du numérique* , Civitas Europa, vol. 49(2), 2022.

TURING, A. M., *Computing machinery and intelligence*, Mind, vol. LIX, n° 236, Oxford University Press, 1950.

TÜRK, P., *L'État plateforme numérique*, Revue du droit public, 2020.

TURPIN, D., *20 ans de lois de bioéthique*, Journal International de Bioéthique et d'Éthique des Sciences, vol. 26, 2015.

TUSSEAU, G., *Jeremy Bentham et le contrôle de constitutionnalité: du refus des formes fortes à l'anticipation des formes atténuées*, Droits, vol. 70(2), 2019.

TUSSEAU, G., *Sur le panoptisme de Jeremy Bentham*, Revue Française d'Histoire des Idées Politiques, vol. 19, n° 1, 2004.

TZOUFIS, V., N. PETROPOULOS, *The commission of crimes using autonomous weapon systems: issues of causation and attribution*, TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, vol. 33, 2024.

UBEROI, D., N. PALMOUR, Y. JOLY, *The Advent of Forensic DNA Databases: It's Time to Agree on Some International Governance Principles!*, Elsevier, vol. 72, 2024.

UDROIU M., *Sinteza modificărilor legislative operate prin Legile 171/2023, n° 213/2023, n° 217/2023 și n° 248/2023 în cazul infracțiunilor contra persoanei și a celor contra patrimoniului*, Analele Universității din București – seria Drept, Forum juridic, n° 2, 2023.

UFFELMANN, E., et al., *Genome-Wide Association Studies*, Nature Reviews Methods Primers, vol. 1, n° 1, Springer Nature, 2021.

VACCARI, C., A. CHADWICK, *Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News*, Social Media + Society, vol. 6, n° 1, 2020.

VALLET, C., *Le dévoilement de la vie privée sur les sites de réseau social. Des changements significatifs*, Droit et société, vol. 80(1), 2012.

VAN DEN HOVEN VAN GENDEREN R., *Cybercrime investigation and the protection of personal data and privacy*, Project on Cybercrime, Council of Europe.

van DIJCK, J., *Digital Photography: Communication, Identity, Memory*, Visual Communication, vol. 7, n° 1, 2008.

VAN DROOGHENBROECK S., *Droit pénal et droits de l'Homme : le point de vue de la Cour européenne des droits de l'Homme*, in *Les droits de l'Homme, bouclier ou épée du droit pénal*, Bruxelles, Facultés universitaires Saint-Louis, coll. « Publications des Facultés universitaires Saint-Louis », 2007.

VAN EIJK, G., *Socioeconomic Marginality in Sentencing: The Built-In Bias in Risk Assessment Tools and the Reproduction of Social Inequality*, Punishment and Society, vol. 19, n° 4, 2017.

VAN HOECKE, M., OST, F., *Legal Doctrine in Crisis: Towards a European Legal Science*, Legal Studies, vol. 18, n° 2, 1998.

VANHAELEMEESCH, D., T. VANDER BEKEN, S. VANDELVELDE, *Punishment at Home: Offenders' Experiences with Electronic Monitoring*, European Journal of Criminology, vol. 11, n° 3,2014.

VARGAS, C., *The Relevance of Artificial Intelligence in Realizing Leibniz's Dream of Justice,* ResearchGate, 2021.

VERGÈS É., *Géolocalisation en temps réel d'un téléphone : sauvetage d'une preuve illicite*, AJ pénal, n° 23-81, 2024.

VERGÈS, É., BAZZOLI, C., VIAL, G., *La modélisation des décisions de justice à partir des faits. Comment l'intelligence artificielle imite les raisonnements des juges à partir d'une grille de critères*, La Semaine Juridique – Édition générale, suppl. au n° 6, LexisNexis, 2025.

VERGÈS, V.-E., *Le juge face à la boîte noire : l'intelligence artificielle au tribunal*, *Dalloz* 2022.

VERLY, N., *Usurpation d'identité numérique, cyberharcèlement, revenge porn… : éclairages sur la nouvelle criminalité de l'internet*, Légipresse, 63(HS3), 2020.

VON BOGDANDY, A., *The Past and Promise of Doctrinal Constructivism: A Strategy for Responding to the Challenges Facing Constitutional Scholarship in Europe*, International Journal of Constitutional Law, vol. 7, n° 3, juillet 2009.

VUARIN, L., GOMES LOPES, P., MASSÉ, D*., L'intelligence artificielle peut-elle être une innovation responsable ?*, Innovations, 72(3), 2023.

WACHTER, S., B. MITTELSTADT, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, SSRN, 2018.

WACHTER, S., *Data Protection in the Age of Big Data*, Nature Electronics, vol. 2, 2019.

WACHTER, S., *Privacy: Primus Inter Pares — Privacy as a Precondition for Self-Development, Personal Fulfillment and the Free Enjoyment of Fundamental Human Rights*, SSRN, 2017.

WANG, H., et al., *Can AI Be as Creative as Humans?*, arXiv, 2024.

WANG, X., Q. DUAN, M. LIANG, *Understanding the Process of Data Reuse: An Extensive Review*, Journal of the Association for Information Science and Technology, vol. 72, 2021.

WARREN, S., BRANDEIS, L., *The Right to Privacy*, Harvard Law Review, vol. 4, n° 5, 1890.

WAUTERS, A., I. VAN HOYWEGHEN, *Global Trends on Fears and Concerns of Genetic Discrimination: A Systematic Literature Review*, Journal of Human Genetics, vol. 61, 2016.

WEISBURD, K., et al., *Electronic Prisons: The Operation of Ankle Monitoring in the Criminal Legal System*, GWU Legal Studies Research Paper, n° 2021-41, 2021.

WHITE J., *Dismiss, distort, distract, and dismay: continuity and change in Russian disinformation*, Institute for European Studies, 2016.

WICKENHEISER, R. A., *Expanding DNA Database Effectiveness*, Forensic Science International: Synergy, vol. 4, 2022.

WILLICK M. S., *Constitutional law and artificial intelligence: the potential legal recognition of computers as persons*, International Joint Conference on Artificial Intelligence, 1985.

WINROTH, A., Wei, J.C.(dir.), *The Cambridge History of Medieval Canon Law*, Cambridge–New York, Cambridge University Press, 2022.

WINTER, R., et al., *Evaluation of Project Vigilance: Electronic Monitoring of Family Violence Offenders*, Tasmanian Institute of Law Enforcement Studies (TILES), University of Tasmania, 2021.

WOHLERS, W., *Criminal Law as a Regulatory Tool*, en DYSON, M., VOGEL, B. (dir.), *The Limits of Criminal Law: Anglo-German Concepts and Principles*, Oxford, Hart Publishing, 2020.

WOJCIK, S., *La démocratie numérique : illusion ou réalité ?*, Cahiers français, vol. 420-421(2), 2021.

WOLSWIJK, H., *Theft: Taking a Virtual Object in RuneScape: Judgment of 31 January 2012, Case No. 10/00101 J.,* The Journal of Criminal Law, vol. 76, n° 6, 2012.

WONG, R., *The Shape of Things to Come: Swedish Developments on the Protection of Privacy.* Script-Ed, Vol. 2, No. 2, 2005.

WOOD, G. S., *The Great Demarcation Between Public and Private*, Oxford University Press, 2021.

WOSZCZYNA, K., K. MANIA, *The European Map of Artificial Intelligence Development Policies: A Comparative Analysis*, International Journal of Contemporary Management, vol. 59, n° 3, 2023.

YADAV, D., S. SAXENA, B. BHUSHAN, *The Dark Web: A Dive into the Darkest Side of the Internet*, ICICC, 2020.

ZEDNIK, C., *Solving the Black Box Problem: A Normative Framework for Explainable Artificial Intelligence*, Philosophy & Technology, vol. 34, 2019.

ZHANG, J., D. WOLFRAM, F. MA, *The Impact of Big Data on Research Methods in Information Science*, Data and Information Management, vol. 7, n° 2, 2023.

ZHANG, L., I. PENTINA, Y. FAN, *Who Do You Choose? Comparing Perceptions of Human vs Robo-Advisor in the Context of Financial Services*, Journal of Services Marketing, 2021.

ZHAO, S., *Theoretical Preconditions of Criminal Imputation for Negligence Crime Involving AI*, Springer, 2024.

ZHOU, Z., et al., *Edge Intelligence: Paving the Last Mile of Artificial Intelligence with Edge Computing*, Proceedings of the IEEE, vol. 107, n° 8, 2019.

ZHU, M., *Jennifer Doudna and Emmanuelle Charpentier's Experiment About the CRISPR/Cas9 System's Role in Adaptive Bacterial Immunity*, Embryo Project Encyclopedia, 2017.

ZOLLINGER, A., *Creations generated by artificial intelligence in literary and artistic property: the new death of the author?*, Eastern Journal of European Studies, 2024.

ZOLYNSKI, C., LE ROY, M., *La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée*, LEGICOM, 59(2), 2017.

ZORN, C., *Le Chiffrement des Communications Protège les Droits de l'Homme, en Russie et Ailleurs* , Dalloz Actualité, 2024.

VII. Rapports institutionnels/Guides techniques/Documents officiels

AARON, D.M., KAHN, R., *Foundation of the Internet*, Encyclopedia Britannica,2020.

ABNORMAL AI, *What Is a Data Leak? How They Happen and How to Prevent Them.*

ADJUST, *What Is Ad Stacking and How Does It Work?*

ADJUST, *What Is Click Injection?*.

ADNOVUM, *Digital Identity: The Complete Guide to Digital Identification*, 2024.

AI NOW INSTITUTE, *AI Now 2018 Report*, 2018.

ANSSI, *Avis scientifique et technique sur la migration vers la cryptographie post-quantique*, Paris, 2022.

APPSFLYER, *What is ad stacking?*, AppsFlyer mobile glossary.

ARNTZ P., *Notorious Data Leak Site BreachForums Seized by Law Enforcement*, Malwarebytes, 2024.

ASSEMBLÉE NATIONALE, *Délégation aux droits des femmes et à l'égalité des chances entre les hommes et les femmes, Rapport d'information n° 3348 sur le projet de loi pour une République numérique (n° 3318), XIVe législature,* 2015.

ASSEMBLÉE NATIONALE, *Rapport d'information n° 1833 : Lutte contre le financement du terrorisme international*, Paris, 2019.

ASSEMBLÉE NATIONALE, *Rapport d'information n° 532*, Paris.

ASSEMBLÉE NATIONALE, *Rapport d'information sur le fichier national automatisé des empreintes génétiques*, Paris, 2002.

AUSWÄRTIGES A., *Déclaration du ministère des Affaires étrangères sur la résiliation de l'accord avec la France*, Newsroom, 2013.

AVIESAN (Alliance nationale pour les sciences de la vie et de la santé), *Francee Médecine Génomique,* 2025.

AZÉMA, J.-P., LÉVY-BRUHL, R., TOUCHELAY, B., *Mission d'analyse historique sur le système statistique français. [*Rapport de recherche*],* INSEE. 1998.

AZURE NETWORK SECURITY TEAM, *Anatomy of a DDoS Amplification Attack*, Microsoft Security Blog, 2022.

BENSAMOUN, A., FARCHY, J., *Intelligence artificielle et culture : Rapport final de la mission du Conseil supérieur de la propriété littéraire et artistique*, Paris, CSPLA, 2020.

BIG COMMERCE, *What Is Click Fraud? How to Identify and Prevent Fraudulent Clicks.*

BIGAID, *What Is Ad Stacking? Ad Stacking Definition*.

BIT SENTINEL, *Instruction et sensibilisation à la cybersécurité*, blog.

BMJ, *The Nuremberg Code (1947)*, vol. 313, 1996.
BONNEMAISON, G. *La Modernisation du Service Public Pénitentiaire*, rapport au Premier Ministre et au Garde des Sceaux, ministère de la Justice, 1989.
BOUCHER P., *Artificial intelligence: how does it work, why does it matter, and what can we do about it?*, Scientific Foresight Unit (STOA), Parlement européen, Bruxelles, 2020.
BOUCHET P., *Écoutes Téléphoniques,* Institut Paul Bouchet,1995.
BOULARD, J.C., LAMBERT, A., *Rapport de la mission de lutte contre l'inflation normative*, Paris, La Documentation française, 2013.
BUZZARD, J., GOLDBERG, T., *2021 Identity Fraud Study: Shifting Angles*, Javelin Strategy & Research 2021.
CABANEL P.-G., *Pour une meilleure prévention de la récidive.* Rapport au Premier ministre, Paris, La Documentation française, coll. « Rapports officiels », 1996.
CALCUTT D., *Report of the Committee on Privacy and Related Matters*, Londres, HMSO, 1990.
CARTER W., SILVER H. J., *The EU Artificial Intelligence (AI) Act: A Pioneering Framework for AI Governance*, Womble Bond Dickinson, 2024.
CASTELLUCCIA C., LE MÉTAYER D., *Understanding algorithmic decision-making: opportunities and challenges*, Scientific Foresight Unit (STOA), Parlement européen, 2019.
CATO INSTITUTE, *The Balance Between Encryption and National Security*, Washington D.C., 2021.
CATTELL J., et al., *Community orders with punitive requirements: results from the Offender Management Community Cohort Study*, Ministry of Justice, Londres, 2014.
CEC, *Test ADN sur Internet: Est-ce Légal? Quels Sont les Risques?,* France, 2023.
CENTER FOR COUNTERING DIGITAL HATE, *Facebook's Metaverse: One Incident of Abuse and Harassment Every 7 Minutes*, 2021.
CGT-INSEE-GENES, *La gestion des fichiers individuels par la statistique publique : des précédents et des controverses (3/3*), Statistique publique – Histoire, 2021.
CHARPENTIER, E., DOUDNAM, J.A., *The Nobel Prize in Chemistry 2020 – Genetic Scissors: A Tool for Rewriting the Code of Life*, Nobel Prize Outreach, 2020.
CHIRILA, R., *Identitatea Digitală Auto-Suverană pe Înțelesul Tuturor*. LinkedIn.
CHURCH A., DUNSTAN S., *Home detention: the evaluation of the home detention pilot programme, 1995–1997*, Ministry of Justice, Wellington, 1997.
CISA, *CryptoLocker Ransomware Infections*, 2016.
CISOMAG, *Hackers Take Over Smart Home*, CISO Mag, 2019.

CLASEN, A., *L'Espagne présente un nouveau «pacte quantique» européen*, Euractiv, Bruxelles, 2023.
CLOUD4C, *Top Technology Innovations in the 21st Century*, Timeline Blog, 2024.
CLOUDFLARE, *What Is Ad Fraud?*
CLOUDFLARE, *What Is Email Spoofing?* Cloudflare.
CNCDH, *Alternatives à la détention : du contrôle judiciaire à la libération conditionnelle*, Paris, La Documentation française, 2007.
CNCDH, Avis *Protection de la vie privée à l'ère numérique*, Assemblée plénière, Paris, 2018.
CNCTR, *8e Rapport d'activité*, Paris, 2023.
CNCTR, *L'instauration progressive d'un contrôle de l'activité des services de renseignement*, Paris, CNCTR, 2020.
CNIL, *Caméras dites « intelligentes » ou « augmentées » dans les espaces publics – Position sur les conditions de déploiement*, 2022.
CNIL, *Comprendre les grands principes de la cryptologie et du chiffrement*, Paris, 2016.
CNIL, *Droits numériques des mineurs, Consultation publique*, Paris, janvier 2021.
CNIL, *Entrée en Vigueur du Règlement Européen sur l'IA: Les Premières Questions-Réponses de la CNIL.*
CNIL, *IA: La CNIL publie ses premières recommandations sur le développement des systèmes d'intelligence artificielle*, Paris, 8 avril 2024.
CNIL, *Intelligence Artificielle: Le Plan d'Action de la CNIL*, 2023.
CNIL, *La navigation privée pour limiter les risques de piratage de vos comptes en ligne*, 2016.
CNIL, *La sécurité des données personnelles*, Les Guides de la CNIL, 2018.
CNIL, *Le droit à l'effacement: supprimer vos données en ligne*, 2018.
CNIL, *Tests Génétiques sur Internet: La CNIL Appelle à la Vigilance*. Mars 2024.
COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ, *Réflexion éthique sur l'évolution des tests génétiques liée au séquençage de l'ADN humain à très haut débit*, 2016.
COMMISSION EUROPÉENNE, *Développement de l'Internet des objets en Europe*, SWD(2016) 110 final, 2016.
COMMISSION EUROPÉENNE, État de l'Union 2017 — Cybersécurité : la Commission dote l'UE de moyens supplémentaires pour répondre aux cyberattaques, Dalloz Actualité, 2017.
COMMISSION EUROPÉENNE, *Identité numérique européenne*, Bruxelles.
COMMISSION JUSTICE PÉNALE ET DROITS DE L'HOMME, *La mise en état des affaires pénales*, La Documentation Française, 1991.
COMPULYNX, *Benefits of Using Biometrics in Educational Institution,* CompuLynx, 2021.

CONFÉRENCE INTERNATIONALE DES COMMISSAIRES À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE (ICDPPC), *Résolution sur la vie privée comme droit fondamental et condition préalable à la démocratie*, Tirana, 2019.

CONSEIL D'ÉTAT, *Le numérique et les droits fondamentaux*, Paris, La Documentation française, 2014.

CONSEIL D'ÉTAT, Section du rapport et des études, *Révision de la loi de bioéthique : quelles options pour demain ?*, Paris, La Documentation française, 2018.

CONSEIL DE L'EUROPE & IEE SA, *The Metaverse and Its Impact on Human Rights, the Rule of Law and Democracy*, 2024.

CONSEIL DE L'EUROPE, *Case Law of the European Court of Human Rights Concerning the Protection of Personal Data*, Strasbourg, 2017.

CONSEIL DE L'EUROPE, *CM/Rec (2010)1 – Règles européennes de probation*, Strasbourg, 2010.

CONSEIL DE L'EUROPE, Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD), *Convention n° 108*, Strasbourg, 1981.

CONSEIL DE L'EUROPE, *Déclaration sur la liberté de la communication sur Internet*, adoptée par le Comité des ministres, 28 mai 2003.

CONSEIL DE L'EUROPE, DEPARTMENT FOR THE EXECUTION OF JUDGMENTS, *France Reinforces the Guarantees Around the FNAEG (National Automated Genetic Fingerprints Database)*, 2022.

CONSEIL DE L'EUROPE, *Le droit au respect de la vie privée et familiale*, Strasbourg, 2007.

CONSEIL DE L'EUROPE, *Partie 1. Les opérations de surveillance massive*, in *Surveillance de masse : quel contrôle démocratique ?*, 2016.

CONSEIL DE L'EUROPE, *Rapport de Mme Liliane Maury Pasquier, Commission des questions sociales, de la santé et du développement durable*, Doc. 13215, 2013.

CONSEIL DE L'EUROPE, *Standards and Ethics in Electronic Monitoring: Handbook for Professionals Responsible for the Establishment and the Use of Electronic Monitoring*, 2014.

CONSEIL DE L'EUROPE, *Statistiques pénales annuelles du Conseil de l'Europe (SPACE)*, Université de Lausanne, 2023.

CONSEIL DE L'EUROPE, *Surveillance de masse : quel contrôle démocratique ?*, Conseil de l'Europe, 2016.

CONSEIL DES DROITS DE L'HOMME DES NATIONS UNIES, *Rapport du Haut-Commissariat aux droits de l'homme*, A/HRC/17/27, Genève, 2011.

CONSORTIUM INTERNATIONAL DU GÉNOME HUMAIN, *Annonce de l'achèvement du Projet génome humain*, 2003.

CSO ONLINE, *SolarWinds Attack Explained: And Why It Was So Hard to Detect*, 2020.

D&AD, *Harness the Power of Hacking*, D&AD Publicatications.

D'ACQUISTO G., DOMINGO-FERRER J., KIKIRAS P., TORRA V., DE MONTJOYE Y.-BOURKA A., *Privacy by Design in Big Data: An Overview of Privacy Enhancing Technologies in the Era of Big Data Analytics*, rapport technique, European Union Agency for Network and Information Security (ENISA), 2015.

DATAREPORTAL, *Digital 2023: Global Overview Report*, Global Digital Insights, 2023.

DÉFENSEUR DES DROITS, *Déclaration: Algorithmes, prévenir l'automatisation des discriminations*, 2020.

DÉFENSEUR DES DROITS, *Report Biometrics – The Urge to Safeguard Fundamental Rights*, 2021.

DIGITAL SKILLS, JOBS PLATFORM, *Learning How a Scam Works*.

DIICOT, *Criminalitatea informatică*.

DIRECTION NATIONALE DU RENSEIGNEMENT (DNI), *Worldwide Threat Assessment*, 2013.

DOBRINOIU M., *Legile Internetului: Infracțiunea de interceptare ilegală a unei transmisii de date informatice*.

DPO EUROPE, *Navigating the Jurisdictional Chaos: An International Law Perspective on the Extraterritorial Application of Data Protection Laws*, 2024.

DUBOV, A., *Ethics of Digital Contact Tracing to Contain the COVID-19 Pandemic*. Institute for Health Policy Leadership, 2021.

DUCASSE, C.J. *Philosophy and Wisdom in Punishment and Reward*, Encyclopedia Britannica, 2024.

DUIGNAN, B. *Trolley Problem*. Encyclopedia Britannica, 2024.

DÜNKEL F., THIELE C., TREIG J., *Electronic Monitoring in Germany*, CEP, 2016.

DUTTA N., MOJTAHEDI S., *Navigating the Risks and Rewards of Digital ID Systems*, Open Government Partnership, 2024.

EASAC, FEAM WORKING GROUP, *Direct-to-Consumer Genetic Testing for Health-Related Purposes in the European Union*, 2012.

EASTWEST INSTITUTE, *Modernizing International Procedures against Cyber-Enabled Crimes*, 2024.

EDPS, European Data Protection Supervisor, *14 misunderstandings with regard to identification and authentication*, juin 2020.

EDWARDS, J., *What Is Sophisticated Invalid Traffic (SIVT), and How to Block It*, CHEQ blog, 15 2022.

EFF (Electronic frontier foundation), *Creating Strong Passwords*, Surveillance self-defense, 2023.

EL SHAMSY A., COULSON N. J., *Sharia*, Encyclopedia Britannica, 2024.

ENISA, *Threat Landscape 2022*, report study, 2021.

EREZ, E., IBARRA, P.R., BALES, W.D., GUR, O.M., *GPS Monitoring Technologies and Domestic Violence: An Evaluation Study*, National Institute of Justice, Washington DC, 2012.

EUREPOC, *Advanced Persistent Threat Profile: APT29*., 2023.

EUROGENTEST, *Overview of countries who have ratified the European Convention on Human Rights and Biomedicine*, 2002.

EUROPEAN COMMISION, *What Personal Data Is Considered Sensitive?*.

EUROPEAN COMMISSION, *What Personal Data Is Considered Sensitive*?

EUROPEAN COMMISSION., *What Does Data Protection 'by Design' and 'by Default' Mean?*

EUROPEAN PATENT OFFICE, *Scenarios for the Future. How Might IP Regimes Evolve by 2025? What Global Legitimacy Might Such Regimes Have?*, Munich, 2007.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (FRA), *La surveillance par les services de renseignement : mesures de protection et voies de recours concernant les droits fondamentaux*, vol. II, 2020.

EUROPOL – ENISA, *On Lawful Criminal Investigation That Respects 21st Century Data Protection*, 2016.

EUROPOL, *Child Sexual Exploitation*, La Haye, 2024.

EUROPOL, *Dismantling Encrypted Criminal EncroChat Communications Leads to Over 6 500 Arrests and Close to EUR 900 Million Seized*, 2020.

EUROPOL, *European Union Terrorism Situation and Trend Report 2024 (EU TE-SAT)*, La Haye, 2024.

EUROPOL, *Internet Organised Crime Threat Assessment (IOCTA)*, 2024.

EUROPOL, *Internet Organised Crime Threat Assessment (IOCTA)*, The Hague, European Police Office, 2016.

EUROPOL, *Malicious Uses and Abuses of Artificial Intelligence*, 2020.

EUROPOL, *Opération "Emma 95"*, communiqué, 2020.

EUROPOL, *Trafic illicite d'armes à feu*, 2024.

EUROPRIS, *Electronic Monitoring in Europe*, Bruxelles, 2016.

FACEBOOK, *Founder's Letter*, Meta, 2021.

FATF, *Guidance on Digital Identity – Identitatea Digitală*, 2020.
FBI (Federal Bureau of Investigation), *Romance Scams*, Washington D.C., 2022.
FDIC, *Avoiding Scams and Scammers*, 2021.
FEDERAL TRADE COMMISSION, USA, *Consumer Sentinel Network Data Book*, Washington D.C., 2020.
FENECH G., *Le Placement sous Surveillance Électronique. Rapport de la Mission Confiée par le Premier Ministre à Georges Fenech*, Paris, Ministère de la Justice, 2005.
FIPR, *Report of the Committee of Privy Councillors appointed to inquire into the interception of communications, (Birkett),* London, 1957.
FIREWEB, Qu'est-ce que la fraude au clic ou les clics invalides et comment on peut s'en protéger?, Blog, 2022.
FLEUREAU, G., *Onze pays membres de l'Union européenne, dont la France, renforcent leur collaboration en informatique quantique*, Siecle digital, 2023.
FNAEG: La Chambre Criminelle Sourcilleuse Quant à la Portée des Arrêts de Condamnation de la CEDH. Dalloz, 2019.
FRANCE, Ministère des Solidarités et de la Santé, *Réduction du délai de droit à l'oubli pour faciliter l'accès au crédit pour les anciens malades du cancer*, communiqué de presse, 2022.
FRANCE, Présidence de la République, *Livre blanc sur la défense et la sécurité nationale*, Paris, La Documentation française, 2008.
Fraud: What Exactly Is Digital Identity Theft?, IN Groupe.
FRAYSSINET, J., *La régulation des données personnelles*, *Legicom*, vol. 42, 2009.
FTC, (Federal Trade Commission), *How to Avoid a Scam | Consumer Advice*, Washington D.C.
GARTNER, *Internet of Things: Unlocking True Digital Business Potential*, Gartner Insights, 2023.
GARTNER, *Predicts 25% of People Will Spend at Least One Hour per Day in the Metaverse by 2026*, 2022.
GEEKS FOR GEEKS, *Difference Between Artificial Intelligence and Human Intelligence*, 2024.
GENDARMERIE NATIONALE (France), *Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée*, 2020.
GITLAN, D. *Ce Este Conștientizarea Securității Cibernetice?* SSL Dragon, 2023.
GLOBAL REACH, *6 Scan-Savvy Tips For Avoiding Online Traps*.
GLOBE NEWS WIRE, Global Biometrics Market Report 2021, *Market to Reach $44.1 Billion by 2026 - Increasing Significance of Biometrics Technology in Facilitating Contactless Passenger Journey Post-COVID-19 Pandemic*, Research and Markets, 2021.

GOIAN, I. *End User Security Awareness: Soluții Securitate*, Dendrio Blog, 2021.
GOOGLE, *Set up DMARC,* Google Workspace Admin Help.
GORCE, G., PILLET, F., *La protection des données personnelles dans l'open data : une exigence et une opportunité*, Rapport d'information fait au nom de la Commission des lois n° 469, 2014.
GORDON, S., *How to Protect Yourself From Cyberstalking*. Verywell Mind, 2024.
GOVERNMENT OF SCOTLAND, *Electronic Monitoring: Uses, Challenges and Successes*, rapport de recherche, 2019.
GRANNAN C. *What's the Difference Between the Deep Web and the Dark Web,* Encyclopedia Britannica.
GREENGARD, S., *Internet of Things, Electronic Network*, Encyclopedia Britannica, 2024.
GREENGARD, S., *Internet of Things*, Encyclopedia Britannica, 2024.
GREVIO, *Baseline Evaluation Report on Legislative and Other Measures Giving Effect to the Provisions of the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention): Romania*, Conseil de l'Europe, Strasbourg, 2022.
HEADER BIDDING, *Invalid Traffic (IVT): Everything You Need to Know*.
HOELSCHER, P*., What Is the Difference Between the Surface Web, the Deep Web, and the Dark Web?* Infosec Institute, 2018.
HUMAN RIGHTS WATCH, *China: Minority Region Collects DNA from Millions*, New York, 2017.
IATA, *Key Trends in Passenger Behavior: Insights from the IATA Global Passenger Survey 2024*, International Air Transport Association, 2024.
IBM*, Qu'est-ce que la Cryptographie Post-Quantique*?
IBM, *Quantum Case Studies*, IBM Publications, 2023.
IBM, *What Is Blockchain?*.
IBM, *What Is Spear Phishing?,* 2024.
ICRC, *A Legal Perspective: Autonomous Weapon Systems Under International Humanitarian Law*, Genève, 2016.
IEEE SPECTRUM, *Content Credentials Will Fight Deepfakes in the 2024 Elections*, décembre 2023.
IEEE Website. IEEE. https://www.ieee.org/
IMPERVA, *What is DNS Spoofing Cache Poisoning Attack Example*.
IMPRIVATA, *Understanding Digital Identity*, consulté le 12 septembre 2024.

INDEED*, Quelle est l'importance de la publicité ? (Définition et conseils*), Indeed Career Guide.
INFLUENCER MARKETING HUB, *48 Metaverse Statistics: Market Size & Growth*, 2023.
INFORMATION COMMISSIONER'S OFFICE, *Anonymisation : managing data protection risk code of practice*, 2012.
INNOVATRICS, *Biometric Identification*.
INSEE, *The National Register for the Identification of Individuals (RNIPP) at the core of French administrative life* − Courrier des statistiques n° 8, 2023.
INTEGRAL AD SCIENCE, *What Is Click Fraud?,*2024.
INTERNET SOCIETY, *Fiche sur les politiques publiques: Introduction à la confidentialité sur l'Internet,* blog, 2015.
INTERPOL*, ChatGPT: Impacts on Law Enforcement*, Innovation Centre, 2023.
INTERPOL, *Interpol Launches First Global Police Metaverse*, Lyon, 2022.
ITREX, *Biometrics in Healthcare: Applications, Advantages, Challenges*, blog, 2021.
IYER, A., *Lottery and Sweepstakes Scams: Recognize and Outsmart Scammers*, Fraude Awareness, 2024.
JAIMAN, A., *AI Generated Synthetic Media, aka Deepfakes*. Medium, 2020.
JEANGÈNE VILMER J.-B., ESCORCIA A., GUILLAUME M., HERRERA J., *Les manipulations de l'information : un défi pour nos démocraties*, Rapport CAPS–IRSEM, Ministère de l'Europe et des Affaires étrangères et Institut de recherche stratégique de l'École militaire, 2018.
JILLSON, E., *The DNA of Privacy and the Privacy of DNA*, FTC Division of Privacy & Identity Protection, 2024
KASPERSKY, *Business on the Dark Web: Deals and Regulatory Mechanisms*, 2024.
KASPERSKY, *Qu'est-ce qu'un VPN? Son fonctionnement et les types de VPN*, Kaspersky Resource Center.
KASPERSKY, *What Is Spoofing and How to Prevent It,* Kaspersky Resource Center, 2020.
KISTERS, S., *Ethical Dilemma of Online Anonymity: Impact, Challenges, and Solutions*. 2023.
KISTERS, S., *Protecting Digital Identity: Ensuring Human Rights Online – Practical Strategies and Cybersecurity Measures*. 2023.
KNOWBE4, *Phishing, History of Phishing*.
LA RUE F., *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, Nations Unies, A/HRC/26/30, 2014.
LEGALUP, *Qu'est-ce que le profilage et comment respecte-t-on le RGPD*?, 2023.

LENAERTS-BERGMANS B., *Deep Web vs Dark Web: What's the Difference?*, CrowdStrike, 2022.

LIBERTIES, *The End of Mass Surveillance: German Constitutional Court Strengthens Basic Rights Abroad,* Society for Civil Rights, 2020.

LOCALIZATION LAB, Înțelegerea și Evitarea Cenzurii în Rețea, 2020.

LYNCH, O., *What Is Invalid Traffic (IVT)?,* CHEQ blog, 2022.

M.A.I. – D.E.P.A.B.D. – CEI, *Direcții de acțiune pe linia punerii în circulație a cărții electronice de identitate*, Ministerul Afacerilor Interne, București, 2024.

MADIEGA T., et al., *Metaverse Opportunities, Risks and Policy Implications*, European Parliamentary Research Service (EPRS), Bruxelles, 2022.

MAHENDU, P., *The State of Ransomware in Financial Services*, Sophos, 2024.

MARTIN P., *L'inflation législative et la qualité de la réglementation*, rapport pour le Conseil d'État, 2017.

MAURER, T., NELSON, A., *The Global Cyber Threat to Financial Systems*, *Finance & Development*, IMF F&D, 2021.

MCKINSEY & COMPANY, *Value Creation in the Metaverse: The Metaverse Does Actually Impact the Environment*, McKinsey Insights, 2022.

MICROSOFT, *Digital Defense Report*, 2021.

MICROSOFT, *Protect Yourself from Tech Support Scams*,2021.

MICROSOFT, *Qu'est-ce que la cybersécurité?*, Microsoft Security.

MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE, *France 2030: Point d'Étapes Trois Ans Après le Lancement de la Stratégie Nationale des Technologies Quantiques et Lancement du Programme Proqcima*, 2024.

MINISTÈRE DE L'INTÉRIEUR (France), *Les infractions liées au numérique enregistrées par la police et la gendarmerie de 2016 à 2023: panorama d'une criminalité hétérogène*, Paris, 2023.

MINISTÈRE PUBLIC, *Privation de Liberté et Possibilités de Pénétrer dans le Domicile Privé en Vue d'Arrêter un Suspect*, Bruxelles, 2011.

MITNICK SECURITY, *Common Hacking Techniques in 2023 and Predictions for 2024*, 2024, blog, 2024.

MOREY, T., *Customer Data: Designing for Transparency and Trust*, Harvard Business Review, 2015.

NAIR S., ABBOTT N., *The Role of Transparency in Digital Trust*, TechTarget – SearchSecurity, 2022.

NATIONS UNIES, *A/HRC/51/17: Le droit à la vie privée à l'ère numérique*, Haut-Commissariat des Nations Unies aux droits de l'homme, 2022.
NATIONS UNIES, *A/RES/79/1: Resolution Adopted by the General Assembly on 22 September 2024*, ONU, New York, 2024.
NATIONS UNIES, *Convention against Transnational Organized Crime*, article 4 « Protection of Sovereignty, 2000.
NATIONS UNIES, *Convention on the Rights of Persons with Disabilities*, 2006.
NATIONS UNIES, *Governing AI for Humanity: Interim Report*, Advisory body on artificial intelligence, 2023.
NATIONS UNIES, *Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems*, Bureau des affaires de désarmement des Nations Unies (UNODA), Genève, 2023.
NATIONS UNIES, *Pacte international relatif aux droits civils et politiques*, Assemblée générale des Nations Unies, 1966.
NATIONS UNIES, *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, Conseil des droits de l'homme, 2011.
NATIONS UNIES, *Report OL FRA 4/2020*, 2020.
NATIONS UNIES, *Résolution du 22 décembre 2018, Favoriser le comportement responsable des États dans le cyberespace dans le contexte de la sécurité internationale*, New York, 2018.
NATIONS UNIES, *Road Map for Digital Cooperation: Implementation of the Recommendations of the High-level Panel on Digital Cooperation*, New York, 2020.
NATIONS UNIES, *Spyware and Surveillance: Threats to Privacy and Human Rights Growing,* UN Report Warns, 2022.
NATIONS UNIES, *Standard Minimum Rules for the Treatment of Prisoners (The Nelson Mandela Rules)*, 1955 (révisé 1977).
NATIONS UNIES, *Summit of the Future*, New York, 2024.
NATIONS UNIES, *Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?*, 2019.
NELLIS M., *Survey of Electronic Monitoring in Europe*, EuroPris, 2017.
NIST (National Institute of Standards and Technology), *Small business cybersecuriturity corner Ransomware*, Washington, D.C., 2023.
NIST, *Secial Publication 800-12: an introduction to Computer Security, Chapter 13: Awareness, Training and Education*, Washington D.C., 2004.
NORTON, *How to Create a Secure Password*.
NSA (National Security Agency), *United States Agency*, Encyclopaedia Britannica, 2023.

OCDE (Organisation de Coopération et de Développement Économiques), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris, 1980.
ODNI (Office of the director of National Intelligence), *Annual Threat Assessment*, Washington D.C., 2007, 2011, 2024.
OLSSON A. R., *Access to Official Documents — Issue Discussion Paper, CommDH(2012)7*, Discussion Paper du Commissaire aux Droits de l'Homme, Conseil de l'Europe, Strasbourg, 2012.
ONE IDENTITY, *What Is a Digital Identity?*.
OPC (Office of the Privacy Commissioner of Canada), *Statement on Generative AI*, Canada, 2023.
OPTICKS SECURITY, *What Is Ad Stacking and How to Prevent It*, blog, 2021.
ORACLE, *Qu'est-ce que c'est Blockchain*?
ORGANISATION DES ÉTATS AMÉRICAINS, Département du droit international, *Principes actualisés relatifs à la vie privée et à la protection des données personnelles*, Washington, D.C., 2022.
PALFREY J., *Misinformation and disinformation*, Encyclopedia Britannica, 2024.
PARLEMENT EUROPÉEN, *Artificial Intelligence (AI) Is Set to Be a "Defining Future Technology", but What Exactly Is AI and How Does It Already Affect Our Lives?* 2020.
PARLEMENT EUROPÉEN, *EncroChat's Path to Europe's Highest Courts*, Étude EPRS, 2022.
PARLEMENT EUROPÉEN, *Le droit au respect de la vie privée : les défis digitaux, une perspective de droit comparé*, Service de recherche, Bruxelles, 2018.
PARLEMENT EUROPÉEN, *Rapport avec recommandations à la Commission sur les règles de droit civil en matière de robotique (2015/2103(INL))*, 2017.
PAYNE, L., *Deepfake*, Encyclopedia Britannica, 2024.
PEREZ, S., L., *The European Court of Human Rights Concludes Encryption Backdoor Mandates Violate the Right to Private Life of All Users Online*, Center for democracy and technology 2022.
PETERSON K., *5 Tips to Prevent Online Fraud*, Banner Bank, s.d.
POLIȚIA DE FRONTIERĂ ROMÂNĂ, *Sinteza Activităților Poliției de Frontieră Desfășurate în Anul 2022*, 2023.
POLONA C., ANDRÉ M., N. MARIA, *Metaverse: Opportunities, Risks, and Policy Implications*, European Parliamentary Research Service, Bruxelles, 2022.
POLYTECHNIQUE INSIGHTS, *L'ordinateur quantique: tout comprendre en 15 minutes*, 2023.

PRISON REFORM TRUST, Trust*, Offender Management and Sentence Planning,* 2019.
PUBLICIS SAPIENT, *Privacy or convenience: what's the tradeoff*, Insights, 2023.
PwC, *Impactul Tehnologiilor Emergente Asupra Datelor cu Caracter Personal și Posibile Soluții de Reducere a Riscurilor*, blog, România, 2022.
QUACH K., *Europol warns ChatGPT already helping folks commit crimes. There is no honor among chatbots*, The Register, 2023.
QUANN R., *Check Out SS8's Latest Lawful & Location Intelligence Insights*, SS8, 2024.
RAINIE L., KIESLER S., KANG R., MADDE M., *Anonymity, privacy, and security online*, Pew Research Center, 2013.
RAINIE, L., M. DUGGAN, *Privacy and Information Sharing*. Pew Research Center, 2016.
Rapport d'activité 2012 du Contrôleur général des lieux de privation de liberté, Dalloz, 2013.
RECI, *Prévention des Discriminations et Choix d'Orientation – Quels Enjeux, Quelles Alliances*, Paris, 2024.
REPORTERS SANS FRONTIÈRES, *Criticism of the BND Act*, 2020.
ROBOTICS OPEN LETTER, *Open Letter to the European Commission on Artificial Intelligence and Robotics*, 2017.
ROMANIAN PARLIAMENT, *Aviz asupra proiectului de lege privind utilizarea responsabilă a tehnologiei deepfake*, Bucarest, 2024.
ROTENBERG M., BUTLER A., DAVISSON J., *Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) in Support of Plaintiffs-Appellees*, EPIC, 2018.
SAGE, *Chapter 3: Punishment and Sentencing*, Sage Edge.
SERVICE PUBLIC, *Écoutes téléphoniques*, France, 2023.
SERVICE PUBLIC, *Passage rapide aux frontières: comment utiliser un sas Parafe ?,*2024.
SGG, (Secrétariat général du Gouvernement), *Indicateurs de suivi de l'activité normative,* Paris, 2025.
SHAUKAT E., *Our Partnership with Ascension*, Google Cloud Blog, 2019.
SIGNATURIT, *What Defines Your Digital Identity and What Legal Rights Are Associated with It?,* 2024.
SINGULAR, *Ad Stacking*.
SMADJA D., *Les tests génétiques peuvent-ils conduire à l'eugénisme?*, *La Lettre de l'Espace éthique*, n°2, Assistance Publique – Hôpitaux de Paris, 2003.
SMITH K., *Understanding State-Sponsored Cyber Attacks*, Phoenix Software, 2024.
SMITHS, J., JACKSON, G., RAJ, S, *Designing Against Misinformation*. Medium, 2017.
SPOONER, D., *Mainstream AI: Redefining Business and Daily Life in 2024*, Scrums, 2024.

STATISTICA *Nombre d'utilisateurs actifs de Meta Horizon Worlds dans le monde en octobre 2022,* Research Department, 2025. f

STISC,(Serviciul Tehnologia Informației și Securitate Cibernetică), *Importanța conștientizării securității cibernetice*, Comunicat de presă, Chișinău, 2022.

SUMSUB, *Global Deepfake & Fraud Insights*, 2023.

SUMSUB, *Global Deepfake Incidents Surge Tenfold from 2022 to 2023*, Research Report, 2023.

TECH TARGET, *What is cyberstalking and how to prevent it?*.

TERRELL, K., WRIGHT, G., YASAR, K., *What Is Social Networking and How Does It Work?*, TechTarget Definition, 2024.

THALES, *Biometrics: Definition, Use Cases and Latest News*, 2023.

THE INVESTOPEDIA TEAM, *Qu'était la route de la soie en ligne* ? Histoire et fermeture par le FBI, 2025.

TRUVERE, *Blockchain Identity Management: Complete Guide,* 2024.

U.S. DEPARMENT OF LABOR, *FAQ relative au Genetic Information Nondiscrimination Act (GINA)*, 2021.

U.S. DEPARTMENT OF JUSTICE, *Investigation Leads to Shutdown of Largest Online Darknet Marketplace*, 2022.

U.S. PROOFPOINT, *What Is Phishing? Definition, Types of Attacks and More*, 2021.

UK, MINISTRY OF JUSTICE, *Electronic Monitoring Caseload*, Justice Data, Royaume-Uni, 2023.

UNESCO, *Global Survey on Internet Privacy and Freedom of Expression*, UNESCO Publishing, 2011.

UNESCO, *The Swedish Freedom of the Press Ordinance of 1766: The world's first legislation guaranteeing free communication of information*,

UNION EUROPÉENNE, *Compendium de l'audit : la cybersécurité dans l'Union européenne et ses États membres*, Luxembourg, 2024.

UNION EUROPÉENNE, *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, COM/2021/206 final, Bruxelles, 2021.

UNION EUROPÉENNE, *Rapport sur l'utilisation de la surveillance électronique des délinquants*, 2014.

UNODC *Comprehensive Study on Cybercrime*, 2013.

UNODC, *Handbook of Basic Principles and Promising Practices on Alternatives to Imprisonment*, 2010.

UNODC, *Manuel d'introduction pour la prévention de la récidive et la réinsertion sociale des délinquants*, Série de manuels sur la justice pénale, 2012.
USA.GOV, *Identity Theft*, 2024.
VANWELL J., *IoT Security Breaches: 4 Real-World Examples*, Conoscom, 2021.
VERIZON, *Data Breach Investigations Report*, 2024.
VERIZON, *The History of Phishing Attacks*, consulté le 27 novembre 2024.
VIE PUBLIQUE, *Les questions de bioéthique : chronologie 1983-2023*, La Documentation française, 2023.
VIE PUBLIQUE, *Loi République numérique du 7 octobre 2016 (Loi Lemaire) : quels changements,* 2016.
VIE PUBLIQUE, *Mission exploratoire sur les métavers*, 2022.
VILLANI C., BONNET Y., RONDEPIERRE B., *For a Meaningful Artificial Intelligence: Towards a French and European Strategy*, Conseil National du Numérique, 2018.
VILLEDIEU, A.L., CHALMETON, H., *Usurpation d'identité numérique*. *Premiers enseignements de la jurisprudence,* CMS LAW, 2017.
VOOR MENSENRECHTEN, L., *Nos empreintes digitales sur les cartes d'identité ? Une mesure inutile et dangereuse*, Ligue des Droits Humains, 2019.
WAVE NETWORK, *Fact Sheet Istanbul Convention*, 2016.
WEEDON J., et al., *Information Operations and Facebook*, Facebook Security, 2017.
WILKINS, S., *A Brief Introduction of Online Anonymity*, Medium, 2018.
WOLFORD, B., *What Is GDPR, the EU's New Data Protection Law?,* GDPR.eu, 2018.
WORLD ECONOMIC FORUM, *The Global Competitiveness Report 2017-2018,* Genève, 2017.
X HELP, *About Community Notes*.
YOUR EUROPE, *Protection des données et de la vie privée en ligne*.

VIII. Presse et médias

ABEL, O., *Le chemin du consentement, ou L'adolescence du consentement*, blog Olivier Abel, 2022.
ABU DHABI MEDIA OFFICE ,*Abu Dhabi Airports and ICP Partner to Launch the World's First-of-Its-Kind Smart Travel Project. Abu Dhabi Media Office*, 2024.
ACTION FRAUD, *Stay Safe Online After £1.4 Million Lost from Email and Social Media Account Hacking in the Last Year*. 2024.
ACTON, B., *The Origins and History of the Dark Web,* IdentityIQ, 2024.

ANCT, *What relationships do the French have with artificial intelligence?*, Labo Société Numérique, 2025.

ANGHELUS, A., *Rolul Esențial al Educației în Securitatea Cibernetică*, Cyber Security Services, 2024.

ANTJE, *Disinformation and 7 Common Forms of Information Disorder*, The Commons, 2024.

ARASEC, *Cybersécurité: Défis et perspectives en éducation*, Ministerul Educației și Cercetării, 2020.

AUIRE, B., et al*., Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (blog), 2019.

AVRAM, A., *Explorarea Echilibrului între Date Deschise și Confidențialitate*, InfoCons blog, 2024.

BBC BITESIZE *, Avantages et inconvénients des nouvelles technologies - Influence de la technologie sur l'activité commerciale*, (*Advantages and Disadvantages of New Technology - Technological Influence on Business Activity)*, Eduqas Business Revision.

BBC, *ISIS Militants Using Encrypted Apps to Evade Detection,* 2020.

BBC, *Ransomware et cryptage : une menace croissante*.

BBC, *The CalExit Campaign Is Another Illustration of Russian Disinformation Campaign*, „*Russian Trolls" Promoted California Independence*, 2017.

BBC, *The Vaccine Misinformation Battle Raging in France*. BBC trending, 2021.

BÉCHADE, C., *Les Portes Dérobées Dans Le Chiffrement Sont Incompatibles Avec Une Société Démocratique, Juge La Cour Européenne des Droits de l'Homme*, Clubic, 2024.

BELAMMIRE, J., *My First Virtual Reality Groping*, Medium, 2016.

BERCEA, A., *Le vol d'identité a augmenté de 354% par rapport à l'année précédente. L'augmentation du nombre d'interactions dans l'espace numérique est l'une des principales raisons,* Libertatea, 2024.

BERTUZZI, L., *Italian Data Protection Authority Bans ChatGPT Citing Privacy Violations*, Euractiv, 2023.

BIDSCUBE, *General Invalid Traffic (GIVT)*, blog, consulté le 27 novembre 2024.

BIERMANN, K., *Hallo BND, das Grundgesetz gilt auch für euch!,* Die Zeit, 2020.

BLAKEMORE, E., *Why the Navajo Nation Banned Genetic Research*, A&E Television Networks, 2017.

BONNET, S., *The Dangers of Social Media Manipulation and Its Impact on Society*, LinkedIn, 2023.

BOUCHER, P., *Une division de l'informatique est créée à la chancellerie "Safari" ou la chasse aux Français,* Le Monde, 1974.

BREEDEN, A, et al., *Macron Campaign Says It Was Target of 'Massive' Hacking Attack,* N.Y. Times, 2017.
CERF, V., *Internet Access Is Not a Human Right,* New York Times, 2012.
CHEN, A., *The Agency*, New York Times, 2015.
CIESLAK, M., GERKEN, T*., Interpol Working Out How to Police the Metaverse*, BBC Click, 2023.
CIMPANU, C., *French Authorities Seize Their Third Dark Web Marketplace*, 2021.
CIVIC SPACE WATCH, *France: Plagued by Mass Protests and New AI Surveillance Law*, 2023.
COHEN, J*., Google, Ascension Data Partnership Sparks Federal Probe*, Modern Healthcare, 2019.
CONFESSORE, N., *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, The New York Times, 2018.
CONSTANTINESCU, V., *Étude de cas : une attaque du type ransomware frappe une petite clinique*, Hot for Security, 2024.
COOBAN, A., *ChatGPT Can Be Tricked Into Telling People How to Commit Crimes, a Tech Firm Finds,* CNN, 2024.
COOKSON, C., *Scientists Appeal for Ethical Use of Robots*, The Financial Times, UK, 2015.
Deepfake technology brings the Mona Lisa to life and it's too spooky, Russian researchers are blurring the lines between art and reality, Dazed, 2019.
DEFENSE ROMANIA TEAM, *Le manuel des cybermenaces – Thales*, 2022.
Désinformation et division. Le cercle vicieux de la méfiance, Magazine Intelligence (blog), 2023.
Despre Tor Browser, TOR Manual.
Détention à Domicile Sous Surveillance Électronique (DDSE), Citoyens & Justice.
DGDDI, Direction générale des douanes et droits indirects, *Démantèlement du Forum « Le Monde Parallèle » sur le Darknet.* Actualités – douane.gouv.fr, 2021.
DNA PASS, *Pourquoi la France maintient l'interdiction des tests de généalogie génétique.*
DNI, *La surveillance en masse et le modelage du comportement à l'ère numérique. Qu'est-ce qu'on peut encore en faire ?,* Département du Renseignement National (Roumanie), 2016.
DOBREANU, C., *Filtre anti-désinformation, utilisé par Facebook en Roumanie. Expert : les Roumains sont relativement vulnérables aux fake news*, Europe Libre, 2020.
DOC DU JURISTE*, Arrestation de Pavel Durov, patron de Telegram*, 2024.
DOFFMAN, Z., *New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report*, Forbes, 2019.

Du fake news au désordre informationnel. magazine Intelligence (blog), 2023.
DUPRIEZ, J., Gafam, *Le Parlement Européen s'attaque au « Far-West » du Numérique*, Public Sénat, 2022.
DURACH, F., *Expériment : fake news et nos émotions. Comment la colère devient le sentiment le plus important*, spotmedia.ro, blog, 2022.
DW, *Annulation des concessions de surveillance*, 2013.
EDELMAN, G., *Facebook and Twitter Want to Keep the Justice System Stacked Against Defendants*, Wired, 2020.
EHRAC, European Human Rights Advocacy Centre*, Journalist Wins Decision Establishing 'Arbitrary and Abusive' Secret Mobile Phone Surveillance in Russia,* 2015.
EL PAIS, *The Backup Driver in the 1st Death by a Fully Autonomous Car Pleads Guilty to Endangerment,* 2023.
ESET, *Le droit à la vie privée à l'ère numérique,* blog, 2017.
EUROPE 1, *Le Parlement adopte définitivement la proposition de loi controversée sur la "sécurité globale".*
EXECUTIVE VC., Managing Your Digital Footprint.
FACEBOOK, *Comment fonctionne l'authentification en deux étapes sur Facebook,* Facebook Help Center.
FACEBOOK, *Le coronavirus a-t-il été créé en laboratoire?*.
FACEBOOK, *The Metaverse May Be Virtual, But the Impact Will Be Real,* Meta, 2022.
FACEBOOK, *Vous ne croirez pas ce que dit Obama dans cette vidéo, 2018.*
FADILPAŠIĆ S., *Europol Warns ChatGPT Is Being Used to Commit Crime*, TechRadar, 2023.
FISCHER, D., *Germany's New Surveillance Laws Raise Privacy Concerns*, Human Rights Watch, 2024.
FNAEG: la chambre criminelle sourcilleuse quant à la portée des arrêts de condamnation de la CEDH, Dalloz, 2019.
FRANCE 24, *Des Milliers de Personnes ont Manifesté Contre la Loi "Sécurité Globale*, 2020.
FRANCE INFO, *Stupéfiants, Faux Documents, Armes: La Plateforme 'Le Monde Parallèle' Qui Proposait Ses Activités Illégales sur le Darknet Démantelée par les Douaniers*, 2021.
FRANCE INTER, *L'astroturfing, ou comment bidonner des initiatives citoyennes,* 2016.
GALLAGHER, R., NSA Surveillance Played Little Role in Foiling Terror Plots, Experts Say, The Guardian, 2013.
GARANTE PRIVACY, *Artificial Intelligence: Stop to ChatGPT by the Italian SA*, *Personal data is collected unlawfully, no age verification system is in place for children,* Garante per la Protezione dei Dati Personali, 2023.

GERSHGORN, D., *Deepfake Music Is So Good It Might Be Illegal,* OneZero, 2020.
GOODRICH, J., *Jay-Z's YouTube Strike Attempt Raises Audio Deepfakes Copyright Debate*. Screen Rant, 2020.
GOTH, G., *Medical Deepfakes Are the Real Deal: Can Deepfakes Be Beneficial in Healthcare?*, MD+DI Online, 2022.
GOULET, N*., Définir et Sanctionner les Fausses Nouvelles ou "Fake News", no 470,* Sénat, 2017.
GRAHAM, J., K., *The Dark Web and Human Trafficking,* Liberty University, 2022.
GREENWALD, G., et all., *Microsoft Handed the NSA Access to Encrypted Messages,* The Guardian, 2013.
GUCCIONE, D., *What Is the Dark Web? How to Access It and What You'll Find*, CSO, 2024.
HALE, C., *Using AI and Brain Implants, Researchers Reconnect ALS Patient with Their Lost Voice* , Fierce Biotech, 2023.
HARWELL, D, TIKU, N., OREMUS, W., *Stumbling with Their Words, Some People Let AI Do the Talking,* Washington Post, 2022.
HENNINGER, M., AUPPERLEE, A., *Former CMU Faculty Geoffrey Hinton Awarded 2024 Nobel Prize in Physics,* Carnegie Mellon University, 2024.
INSTITUT PASTEUR, *Coronavirus: Institut Pasteur Warns Against False Information Circulating on Social Media, 2020.*
INTELLIGENCE, *Désinformation, pandémie de l'ombre*, blog, 2021.
INTELLIGENCE, *La désinformation, une arme pour tous les fronts*, blog, 2020.
INTELLIGENCE, *Manipulation à travers les médias*, magazine Intelligence, blog, 2010.
JUANALS, B., PERRIAULT, J., *L'homme numérique et son double*, dossier de 50 minutes dans *Le cercle des médiologues*, émission de France Culture, 2001.
KASTERN, E., *History of the Dark Web,* Timeline, 2020.
KIRAT, T**.**, *L'intelligence artificielle, l'avocat et le juge*, *La Tribune*, 2017.
KLEINMAN, Z., *What Does Prism Tell Us About Privacy Protection?,* BBC News, 2013.
KOP M., WADHW, V., *How to Prevent Quantum-A.I. Hybrids from Taking Over the World,* Fortune, 2023.
KRISHNADEV, C*., Did Russian Hackers Target Qatar?,* The Atlantic, 2017.
KUHN, M., *Das Recht auf Anonymität im digitalen Raum*, Humanistische Union, no 225/226, 2019.
KUHN, M., *Le droit à l'anonymat dans l'espace numérique,* Humanistische Union, 2019.
KUMAR, C., *Government Surveillance and the Erosion of the Right to Privacy,* LinkedIn, 2023.

LA MONDE DU DROIT*, La différence entre Diffamation et Injurie*.
LAVIN, W., *NFT Collector Spends $450,000 to Live as Snoop Dogg's Virtual Neighbor*. NME, 2022.
LE MONDE, *Ouverture du procès contre Éric Zemmour pour ses propos sur les mineurs isolés,* 2021.
LE MONDE, *Qu'est-ce que la Neutralité du Net?,* 2017.
LEPRINCE-RINGUET D., *Evil AI: These Are the 20 Most Dangerous Crimes That Artificial Intelligence Will Create*, ZDNet, 2020.
LES ECHOS, *Nicolas Sarkozy face à la justice*. 2024.
LEWIS A., *Balancing Technological Advancements with Privacy Risks*, DMNews, blog, 2024.
LEWIS, K., *How Social Media Networks Facilitate Identity Theft and Fraud*. Octane Magazine.
LIVOLSI, G., DESTAL, M., LE FOLL, C., *La police nationale utilise illégalement un logiciel israélien de reconnaissance faciale*, Disclose, 2023.
MACASKIL, E., BOWCOTT, O., *Investigatory Powers Act: Snooper's Charter Bill Becomes Law,* The Guardian, 2016.
MACRON E., *Déclaration sur les Efforts en Faveur du Développement de l'Intelligence Artificielle*, discours, Paris, 21 mai 2024.
MANACH, J.M., *Plus d'un tiers des Français sont fichés dans le FNAEG*, Next Inpact, 2021.
MANIÈRE, P., *Les GAFA*, émission *Le Monde selon Philippe Manière*, France Culture, 2015.
MARR B., *The Top 10 Tech Trends In 2023 Everyone Must Be Ready For*, Forbes, 2022.
MAURICE, S., *Le cyberharcèlement, facile à repérer, difficile à contrer*, Libération, 2013.
MAY T., *Theresa May's Davos Address in Full*, discours, Davos, 2018.
MAYHEW, S., *Facial Recognition Software Tested During Carnival in Nice,* Biometric Update, 2019.
McLEAN HOSPITAL, *Here's How Social Media Affects Your Mental Health*.
MILANOVIC, M., *Blockbuster Strasbourg Judgment on Surveillance in Russia,* EJIL: Talk!, 2015.
Missions et pouvoirs de la Commission nationale de l'informatique et des libertés (CNIL), Dalloz, 2015.
MLFA, Muslim Legal Fund of America, *How Government Surveillance and Big Tech Erase Your Privacy Rights*, Criminal Defense Department Accessed, 2021.
MONITOIRE-PSYCHOLOGIE, *Minute d'inspiration: la magie des algorithmes et leur impact sur la psyché humaine*, Monitoire de la Psychologie, 2024.

MULLIN, S., GATTO, J., *The Game Goes On: Sheppard Mullin Obtains Dismissal With Prejudice of Class Action Alleging Social Gaming Micro-transactions Constitute Illegal Gambling*, Gambling, Virtual Currency, 2018.

NEW YORK TIMES, *Obama Calls Surveillance Programs Legal and Limited*, 2013.

NEW YORK TIMES, *One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority,* 2019.

NEW YORK TIMES, *The Dark Side of Encryption : Comment les cybercriminels exploitent les mesures de sécurité.*

NOD ACADEMY, *La cybersécurité dans les écoles. 5 modèles européens de bonnes pratiques*, 2024.

NSA/CSS, *President Biden Signs Memo to Combat Quantum Computing Threat*, communiqué de presse, 2022.

PAM, C., *Radiographie de la désinformation sur COVID-19 en Roumanie*." Cotidianul, 2020.

PARKIN, S., *Who Needs the Metaverse? Meet the People Still Living on Second Life*, The Guardian, 2023.

PELLEGRINI, F., VITALIS, A., *L'Ère du Fichage Généralisé.* Le Monde Diplomatique, 2018.

PERCEPTION SURVEY REPORT, *The Impact of Communication Surveillance on Human Rights Defenders in Kenya*, Defenders Coalition, 2021.

PERLROTH, N., *Yahoo Says Hackers Stole Data on 500 Million Users in 2014*, The New York Times, 2016.

PESTER R., *Patel v. Facebook: Facebook Settles Illinois Biometric Information Privacy Act ("BIPA") Violation Suit*, Harvard Journal of Law & Technology (JOLT) Digest, 2020.

POMERANTSEY, P., *Inside Putin's Information War*, Politico, 2015.

POPA, L., *Qu'est-ce que c'est l'identité numérique et pourquoi est-elle importante*, Capital, 2023.

PORTAIL DE L'INTELLIGENCE ÉCONOMIQUE, *France Quantum 2025 : le quantique comme enjeu de puissance pour la France*, 2025.

PRÉSIDENCE DE LA RÉPUBLIQUE, *Stratégie nationale sur les technologies quantiques*, communiqué de presse, 21 janvier 2021, France 2030.

REPORTER OHNE GRENZEN, *Worldwide mass surveillance by Germany's intelligence service declared unconstitutional in landmark ruling on press freedom in the digital age,* déclaration de presse, 2020.

REUTERS, *Yahoo Data Breach Settlement Gets Preliminary Approval from U.S. Judge*, 2019.

RILEY, M., ROBERSTSON, J*., Inside the Billion-Dollar Hack of Yahoo: The Internet Heist That Keeps On Hurting,* Bloomberg, 2017.

ROLLER, S., *The Stasi: The Most Terrifying Secret Police in History?,* Hystory Hit, 2021.
ROPARTZ, P., AFP agence, *États-Unis : qui est Ross Ulbricht, ce libertarien créateur du «eBay de la drogue», gracié par Donald Trump ?,* le Figaro, 2025.
ROSEN, P., *This Metaverse Casino Raked in $7.5 Million in Last 3 Months and Accounts for a Third of Decentraland's Daily Users*. Business Insider, 2022.
ROTH, E., *23andMe Admits Hackers Accessed 6.9 Million Users' DNA Relatives Data*, Verge Deals, 2023.
SARBU, M, TANNO, S., *Romania's Top Court Annuls Presidential Election Result*, CNN, 2024.
SÉNAT FRANÇAIS, *Séance du 28 janvier 2020. Compte rendu intégral de la séance*, Sénat, 2020.
SHANE, S., *How Unwitting Americans Encountered Russian Operatives Online*, New York Times, 2018.
SHIELDS, C., *Why Do Computers Crash?,* Scientific American, 2003.
SHODHGANGA, *International initiative to combat cybercrime and analysis of jurisdictional provisions in Convention on Cyber Crime*, 2019.
SOMERS, M., *Deepfakes, Explained*, MIT Management – Sloan School, 2020.
SPENCER, A., BALL, J., *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ,* The Guardian, 2014.
SPIEGEL, NSA überwacht 500 Millionen Verbindungen in Deutschland, en ligne, 2013.
STARGARDTER, G., *Behind the arrest of Telegram boss, a small Paris cybercrime unit with big ambitions*, Reuters, 2024.
STOICA, R., BALOG, I., *Mult Așteptata Modificare Aduse Codului Penal: Incriminarea Fenomenului de 'Revenge Porn*, Juridice.ro, 2023.
STUDENT CENTER, *L'importance de la cybersécurité à l'ère numérique* , studentcenter.ro, en ligne, 2024
SWAYNE, M., *Quantum Leaders Tell FT: Quantum Computing Race Enters Final Stretch, But Scaling Challenges Still Loom*, The Quantum Insider, 2025.
T POINT TECH, *History of Computers,* 2020.
TEAM S. E. O., *What Is Biometric Authentication and How Does It Work*?, LoginTC blog.
THE CYBERWIRE, *Proof-of-concept: BlackMamba AI-developed malware*, N2K, 2023.
THE DAILY STAR*, Merkel Says 'Germany Not a Surveillance State,* AFP, 2013.
THE GUARDIAN, *Telegram: the app of choice for ISIS*, 2017.
THE GUARDIAN, *The Cambridge Analytica Files*.

THOMPSON, N., *Emmanuel Macron Talks to WIRED About France's AI Strategy*, Wired, 2018.
TONNERRE-SEYCHELLES, S*., Après J'accuse...!, les procès de Zola*, Bibliothèque nationale de France, Gallica, 2018.
TOOR, A., *Germany Passes Controversial Law to Fine Facebook over Hate Speech*, The Verge, 2017.
TRUȚĂ, F., *German Authorities Take Down Darknet Marketplace 'Nemesis Market'*, Bitfender, 2024.
TRUȚĂ, F., *Patient Dies After Ransomware Attack on Düsseldorf Hospital, Security*, Boulevard, 2020.
TTO, *Conference for Truth and Trust Online*, 2021.
TULANE UNIVERSITY, *Everything You Should Know About the Dark Web*.
UPI, *Robot Kills Man,* UPI Archives, 1981.
VALLANCE, C., *Police Investigate Virtual Sex Assault on Girl's Avatar*, BBC News, 2024.
VERIZON, *Digital footprint: definition, examples and ways reduce*.
Vie privée, L'Influx, 2013.
VIȘNIEC, M., *Despre putinizare și tik-tokare*, Contributors.ro, 2024.
VITARD, A., *Pourquoi la nouvelle plateforme de déchiffrement d'Europol inquiète des députés européens?,* Usine Digitale, 2021.
VULCAN, D., *CNA Cere Comisiei Europene să Investigheze TikTok După Victoria lui Călin Georgescu în Primul Tur,* Europa Liberă, 2024.
WALSH, J., *Kevin Mitnick, founder of Mitnick Security*, EBSCO Knowledge Advantage, 2024.
WHITE, J.B., *Police Identify First Pedestrian Killed by Self-Driving Car,* Independent, 2018.
WIRED, *Comment les criminels utilisent WhatsApp pour coordonner le commerce mondial de la drogue.*
WISE, *Le passeport biométrique: qu'est-ce que c'est, documents nécessaires, prix et validité*, 2022.
WONG, C., *Use of a Ring Doorbell Found To Be In Breach of Data Protection Laws*, HJA, 2021.

IX. Jurisprudence

Jurisprudence France

Conseil constitutionnel,

- *décision n° 2003-467 DC du 13 mars 2003,* JO n° 66, 2003.
- *décision n° 2014-693 DC du 25 mars 2014, Loi relative à la géolocalisation*, JO, n° 0075, 2014.
- *décision n° 2015-713 DC du 23 juillet 2015*, JO, n° 0171, 2015.
- *décision n° 2018-773 DC du 20 décembre 2018*, JO, n° 0297, 2018.
- *décision n° 2019-778 DC du 21 mars 2019*, JO, n° 71, 2019.
- *décision n° 2020-801 DC du 18 juin 2020*, JO, n° 156, 2020.
- *décision n° 2021-821 du 29 juillet 2021*, JO, n° 178, 2021.
- *décision n° 2021-933 QPC du 30 septembre 2021*, JO n° 229, 2021.
- *décision n° 2022-1030 QPC du 19 janvier 2023*, JO n° 17, 2023.
- *décision n° 76-75 DC du 12 janvier 1977, Loi autorisant la visite des véhicules en vue de la recherche et de la prévention des infractions pénales*, JO, 1977.
- *décision n° 83-164 DC du 29 décembre 1983, Loi de finances pour 1984*, JO, p.3871, 1983.
- *décision n° 94-352 DC du 18 janvier 1995, Loi d'orientation et de programmation relative à la sécurité*, JO, p.1154, 1995.
- *décision n° 99-416 DC du 23 juillet 1999, Loi portant création d'une couverture maladie universelle*, JO n° 172, 1999.
- *décisions* du 1er Juillet 2010 au 30 Septembre 2010, Les Nouveaux Cahiers du Conseil Constitutionnel, 2011/1, no. 30, pp. 97–168.
- *décision n° 2010-25 QPC*, 16 sept 2010,Dalloz actu., 28 sept. 2010.
- *décision n° 2015-512 du 8 janvier 2016*, JO, n° 8, 2016.

Conseil d'État,

- *décision n° 136727 du 27 octobre 1995,* recueil Lebon.
- *décision n° 296845, du 10 avril 2008*, recueil Lebon.
- *décision n° 439360 du 13 avril 2021*, JO n°98, 2021.

Cour d'appel

- d'Amiens, chambre correctionnelle, *arrêt du 15 avril 2009, n° 08/01374*.
- de Caen, chambre correctionnelle, *arrêt du 15 novembre 2004*.
- de Chambéry, *arrêt du 22 mai 2008, n° 07/02077*.
- de Montpellier, chambre correctionnelle 3, *arrêt du 2 février 2006*.
- de Paris, *arrêt du 5 décembre 1997, publié au Recueil Dalloz 1998, p. 32*.
- de Paris*, Baptiste C. c. Ministère public du 24 avril 2007*.
- de Paris, pôle 2, chambre 7, *arrêt du 25 septembre 2019, n° 18/04688*.
- de Rennes, chambre correctionnelle 3, *arrêt du 14 novembre 2000*.

- de Rouen, chambre correctionnelle, *arrêt du 25 juin 2009, n° 08/00962*.

Cour de cassation :

- *Assemblée plénière, 7 mai 2004, n° 02-10.450*.
- *Assemblée plénière, 7 novembre 2022, n° 21-83.146*.
- *Chambre criminelle 29 mars 2017, pourvoi n° 15-28.813*.
- *Chambre criminelle, 10 mai 2005, n° 04-84.705*.
- *Chambre criminelle, 11 juin 2024, n° 23-85.632*.
- *Chambre criminelle, 12 avril 2005, n° 04-85.637*.
- *Chambre criminelle, 12 décembre 2000, n° 00-83.323*.
- *Chambre criminelle, 13 avril 2016, n° 15-82.400*.
- *Chambre criminelle, 15 février 2011, n° 10-82.808*.
- *Chambre criminelle, 16 janvier 1990, Bull. crim. n° 25*.
- *Chambre criminelle, 16 mars 2016, n° 15-82.676*.
- *Chambre criminelle, 16 novembre 1827, Sirey 1828*.
- *Chambre criminelle, 16 octobre 2012, n° 11-88.136*.
- *Chambre criminelle, 19 mai 1981, n° 80-94634*.
- *Chambre criminelle, 19 mai 1981, pourvoi n° 80-94634, Bull. crim. n° 161*.
- *Chambre criminelle, 2 avril 1997, n° 97-80.269 et n° 97-80.270*.
- *Chambre criminelle, 20 novembre 2007, n° 06-82.753*.
- *Chambre criminelle, 20 octobre 1998, Bull. crim. n° 264*.
- *Chambre criminelle, 20 octobre 1998, n° 97-84.621*.
- *Chambre criminelle, 20 septembre 2016, n° 16-80.820*.
- *Chambre criminelle, 20 septembre 2016, pourvoi n° 16-80.820*.
- *Chambre criminelle, 22 janvier 1997, n° 95-81.186*.
- *Chambre criminelle, 22 juin 1837, Sirey, 1837.*
- *Chambre criminelle, 22 octobre 2013, n° 13-81.945*.
- *Chambre criminelle, 23 juin 2021, n° 21-80.682*.
- *Chambre criminelle, 24 janvier 1995, n° 94-81.207*.
- *Chambre criminelle, 24 mai 2023, n° 21-87.509, JurisData n° 2023-008828*.
- *Chambre criminelle, 25 avril 1989, n° 86-93.632*.
- *Chambre criminelle, 26 mai 2009, n° 08-85.983*.
- *Chambre criminelle, 26 mai 2009, n° 08-85.983*.
- *Chambre criminelle, 26 mars 1991, Dr. pén. 1991, comm. 333, 4e arrêt*.
- *Chambre criminelle, 27 février 2018, n° 17-81.850*.
- *Chambre criminelle, 27 janvier 1981, JurisClasseur Périodique, II, n° 19742, 1982*.

- *Chambre criminelle, 28 mars 2023, no 22-83.069.*
- *Chambre criminelle, 28 novembre 2006, n° 06-81.200, inédit*.
- *Chambre criminelle, 3 mars 1982, n° 80-95.226*.
- *Chambre criminelle, 31 octobre 2017, n° 16-87.411*.
- *Chambre criminelle, 4 avril 2024, n° 23-84.520, publié au Bulletin*.
- *Chambre criminelle, 4 mars 1997, n° 96-84.773, publié au Bulletin*.
- *Chambre criminelle, 7 mars 2007, n° 06-88.651*.
- *Chambre criminelle, 7 octobre 1997, n° 96-81.485*.
- *Chambre criminelle, 9 décembre 1998, n° 97-80.578*.
- *Chambre criminelle, 9 février 2016, n° 15-85.070*.
- *Chambre criminelle, 9 mai 2018, n° 17-86.558, Dalloz actualité, 29 mai 2018*.
- *Chambre criminelle, 9 septembre 2003, n° 02-87.098, inédit*.
- Chambre criminelle, *Précisions sur la nécessité des collectes de données biométriques et génétiques* , AJ Pénal, 4 avr. 2024, p. 331.
- *Chambre sociale, 19 janvier 2022, n° 20-12.420 et n° 20-12.421, JurisData n° 2022-000598*.
- *Chambres réunies, 21 juillet 1849, Sirey 1849*.
- *Deuxième chambre civile, 29 janvier 1997, n° 95-15.255*.
- *Pourvoi n° 04-20.735*.
- *Pourvoi n° 16-15.792*.
- *Pourvoi n° 16-87.411*.
- *Pourvoi n° 20-84.201, décision 2021*.
- *Première chambre civile, 12 décembre 2000, n° 98-21.161, JurisData n° 2000-007308*.
- *Première chambre civile, 12 octobre 2016, n° 15-14.896, publié au Bulletin*.
- *Première chambre civile, 17 février 2021, n° 19-24.780, publié au Bulletin*.
- *Première chambre civile, 17 juin 2009, n° 07-21.796*.
- Première chambre civile, 3 avril 2002, *Protection de la vie privée: la Cour de cassation pose de nouvelles règles* , Dalloz, 2002.
- *Première chambre civile, 5 février 2014, n° 13-21.929*.
- *Première chambre civile, 6 avril 2004, n° 00-19.245, inédit*.
- *Troisième chambre civile, 17 janvier 2019, n° 18-40.040*.

CNIL:

- *Délibération n° 2015-078 du 5 mars 2015*.
- *Délibération n° 2021-009 du 7 janvier 2021: avis sur un projet de décret relatif au traitement de données à caractère personnel*.

- *Délibération n° 2021-045 du 15 avril 2021*, Paris, 2021.

Tribunaux administratifs:

- *Tribunal administratif de Nantes, décision du 19 août 2022, n° 2210578*.

Tribunaux de commerce:

- *Tribunal de commerce de Paris, décision, Conform n° 181, mars 1995, Expertises*.

Tribunaux correctionnels:

- *Tribunal correctionnel de Privas, décision, Science criminelle, 1998*.

Jurisprudence Roumanie

Cour constitutionnelle

- *Décision n° 2 du 5 octobre 2024*, Monitorul Oficial de Roumanie, n°1003, 2024.
- *Décision n° 244 du 6 avril 2017,* Monitorul Oficial de Roumanie, n° 529, 2017.
- *Décision n° 26 du 16 janvier 2019,* Monitorul Oficial de Roumanie, n° 193, 2019.
- *Décision n° 32 du 6 décembre 2024*, Monitorul Oficial de Roumanie, n°1231, 2024.
- *Décision n° 33 du 19 janvier 2017*, Monitorul Oficial de Roumanie, n° 320, 2017.
- *Décision n° 51 du 14 mars 2016*, Monitorul Oficial de Roumanie, n° 190, 2016.
- *Décision n° 55 du 4 février 2020*, Monitorul Oficial de Roumanie, n° 517, 2020.
- *Décision n° 630 du 19 décembre 2019,* Monitorul Oficial de Roumanie, n° 1024, 2019.
- *Décision n°55 du 16 février 2022,* Monitorul Oficial de Roumanie, n° 358, 2022.
- *Décision n°55 du 21 avril 2022,* Monitorul Oficial de Roumanie, n° 358, 2022.

Haute Cour de cassation et de justice:

- *Apel. Violarea vieții private în modalitatea prevăzută de art. 226 alin. (1), (5) din Codul penal. Tipicitate*, *décision n° 92/A du 1 mars 2023.*
- *Décision n° 18 du 22 avril 2024,* Monitorul Oficial de Roumanie, n° 446, 2024.
- *Décision n° 4 du 25 janvier 2021,* Monitorul Oficial de Roumanie, n° 171, 2021.
- *Décision n° 51 du 24 juin 2021,* Monitorul Oficial de Roumanie, n°1050, 2021.
- *Décision n° 64 du 2 octobre 2023,* Monitorul Oficial de Roumanie, n° 1047, 2023.
- *Décision RIL n° 18 du 18 novembre 2013.,* Monitorul Oficial de Roumanie, n° 43, 2014.

Tribunaux :

- *Tribunal de première instance de Brașov, jugement pénal n° 701 du 18 avril 2018 (définitif)*.
- *Tribunalul București, decizia nr. 15-06/2018 din 18 iunie 2018*.

Cour de justice de l'Union européenne (CJUE)

- *Affaire 155/79, AM & S Europe Limited c. Commission des Communautés européennes*, 18 mai 1982.
- *Affaire C-118/22, NG c. Direktor na Glavna direktsia « Natsionalna politsia », grande chambre*, 30 janvier 2024.
- **Affaire C-131/12, 13 mai 2014.**
- *Affaire C-28/08 P, Commission européenne c. The Bavarian Lager Co. Ltd., grande chambre*, 29 juin 2010.
- *Affaire C-434/16, Peter Nowak c. Data Protection Commissioner*, 20 décembre 2017.
- *Affaire C-470/21, arrêt*, 2024.
- *Affaire C-536/15, Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV c. Autoriteit Consument en Markt (ACM)*, 2017.
- *Affaire C-543/09, Deutsche Telekom AG c. Bundesrepublik Deutschland*, 2011.
- *Affaire C-61/22, Première chambre*, 19 mai 2020.
- *Affaire C-670/22, arrêt*, 2022.
- Affaire **C-670/22,** Conclusions présentées le 26 octobre 2023 pour **Ćapeta, T.(avocate générale).**
- Affaire C-673/17, *Planet49.*
- *Affaires jointes C-511/18, C-512/18 et C-520/18*, 6 octobre 2020.
- *Arrêt relatif à l'insertion obligatoire de deux empreintes digitales dans les cartes d'identité*, 2020.
- Arrêts relatifs à l'effacement des données génétiques.
- Données personnelles : interdiction des collectes générales des services de sécurité, 6 octobre 2020.
- Protection des données : la CJUE infléchit sa jurisprudence, AJDA, 6 octobre 2020.

Cour européenne des droits de l'homme (CEDH)

- 1re section, *Décision du 14 juin 2007, n° 71111/01*.
- 4e section, *Décision du 22 octobre 2009, n° 17599/05, affaire Norbert Sikorski c. Pologne*.
- 5e section, *Décision du 2 septembre 2010, n° 35623/05*.
- *Arrêt du 18 décembre 2012, requête n° 3111/10, commenté par L. Marino*.
- *Arrêt relatif à l'utilisation de la géolocalisation en temps réel dans les procédures pénales*, 2018.
- *Aycaguer c. France, 22 juin 2017, requête n° 8806/12 (Section V)*.
- *B.B. c. France, requête n° 5335/06*.

- *Bankovic et autres c. Belgique et 16 autres États*.
- *Ben Faiza c. France, 2018*.
- *Big Brother Watch et autres c. Royaume-Uni*, requêtes nos 58170/13, 62322/14 et 24960/15.
- *Canali c. France, 25 avril 2013, requête n° 40119/09*.
- *Conservation des empreintes digitales : atteinte au respect de la vie privée, Dalloz, 18 avr. 2013*
- *Couderc et Hachette Filipacchi Associes c. France*, grande chambre, arrêt du 10 novembre 2015, requête n° 40454/07.
- *Dupate c. Lettonie*, arrêt du 19 novembre 2020, requête n° 18068/11.
- *Egill Einarsson c. Islande (n° 2)*, arrêt du 17 octobre 2017.
- *Elberte c. Lettonie, 2015, requête n° 61243/08*.
- *Gardel c. France, 17 décembre 2009, requête n° 16428/05*.
- *Gaughran c. Royaume-Uni, 18 février 2020, requête n° 45245/15*.
- Grande Chambre, *Décision du 22 octobre 2018, n° 35553/12, 36678/12, 36711/12, affaire S., V. et A. c. Danemark*.
- *Hachette Filipacchi Associés (Ici Paris) c. France, requête. n° 12268/03*
- *Haldimann et autres c. Suisse, 24 février 2015*.
- *Huvig c. France*.
- *Jurisprudence de la Cour européenne des droits de l'Homme relative à la protection des données personnelles*, Strasbourg, 2018.
- *Jurisprudence sur la protection des données personnelles et les droits fondamentaux*, fiche thématique, 2018.
- *Klass et autres c. Allemagne*, requête n° 5029/71.
- *Kruslin c. France*, requête n° 11801/85.
- *Le fichier des empreintes génétiques condamné par la Cour européenne des droits de l'homme*, Dalloz, 22 juin 2017, n° 8806/12.
- *M. c. Allemagne, 1er juillet 2008, requête n° 19359/04*.
- *Malone c. Royaume-Uni*, requête n° 8691/79.
- *Michaud c. France*, 445(2012), 2012.
- *Niemietz c. Allemagne*, (1996) 16 ECHR 97.
- *Niemietz c. Allemagne*, requête n° 13710/88, arrêt du 16 décembre 1992.
- *Peck c. Royaume-Uni*, (2003) 36 ECHR 41.
- *Pihl c. Suède (décision)*, pt. 28.
- *Podchasov c. Russie, 13 février 2024, requête n° 33696/19*.

- *Pretty c. Royaume-Uni*.
- *Reichman c. France*, requête n° 50147/11.
- *Requêtes nos 44715/20 et 47930/21, A.L. c. France et E.J. c. France*.
- *Rodina c. Lettonie*, arrêt du 14 janvier 2020, pt. 131.
- *Roman Zakharov c. Russie*, requête n° 47143/06.
- *S. et Marper c. Royaume-Uni*, requêtes nos 30562/04 et 30566/04, arrêt du 4 décembre 2008.
- *Satakunnan Markkinapörssi Oy et Satamedia Oy c. Finlande*.
- *Tamiz c. Royaume-Uni (décision)*.
- *Von Hannover c. Allemagne (n° 1), 24 juin 2004, requête n° 59320/00*.
- *Von Hannover c. Allemagne (n° 2)*.
- *Weber et Saravia c. Allemagne, 2006*.
- *Zemmour c. France*, arrêt du 1er mars 2021, requête n° 63539/19.

Jurisprudence internationale / autre

Allemagne

- *Cour constitutionnelle fédérale (Bundesverfassungsgericht)*, 1 BvR 2835/17, 19 mai 2020.
- *Cour constitutionnelle fédérale (Bundesverfassungsgericht)*, *Order of the First Senate, 1 BvR 370/07, 27 février 2008.*

Afrique du Sud

- *Cour constitutionnelle de l'Afrique du Sud*, 4 avril 2007, *Butterworths Constitutional Law Reports*, vol. 7, 2007.

Canada

- *R. c. Jarvis*, Cour suprême du Canada.

États-Unis

- *Bragg v. Linden Research, Inc.*
- *Crichton v. United States*, 92 F.2d 224, 67 App. D.C. 300 (D.C. Cir. 1937).
- *Evans v. Linden Research, Inc.*, No. C-11-01078 DMR (N.D. Cal., 29 avril 2014).
- *Johnson v. State*, 142 Ala. 70, 38 So. 182 (1904).
- *Katz v. United States*, 389 U.S. 347 (1967).

- *Riley v. California*, 573 U.S. 373 (2014).
- *Schenck v. United States*, 249 U.S. 47 (1919).
- *Semayne's Case*, Michaelmas Term, 2 James I, 1604, *Reports*, vol. 5.
- *Soto v. Sky Union, LLC*, U.S. District Court, N.D. Illinois, Eastern Division, 29 janvier 2016.
- *Stanford v. Texas*, 379 U.S. 476, 483 (1965).
- *United States v. Powell*, 929 F.2d 724 (D.C. Cir. 1991).
- *United States v. Ulbricht*.
- *Wendt v. Host Intern., Inc.*, 197 F.3d 1284 (9th Cir. 1999).

Pays-Bas

- *Cour suprême des Pays-Bas*, J. 10/00101, chambre criminelle, 31 janvier 2012.

Royaume-Uni

- *Fairhurst v. Woodard*.

Italie

- *Cour de cassation penale, 31 janvier 1934, Giustizia Penale, 1934, II.*

X. Législation/Actes normatifs

Législation internationale et comparée

ALLEMAGNE,

Code de procédure pénale (Strafprozeßordnung – StPO), RGBl., S. 253, 1877. (version consolidée).

Code pénal allemand (Strafgesetzbuch – StGB), RGBl., S.127, 1871. (version consolidée en 1998).

Constitution allemande (Grundgesetz), Bundesrepublik Deutschland, BGBl, I, 1949.

Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG), Federal Law Gazette, BGBl, I, 2017.

Loi relative à l'introduction d'une carte d'identité électronique pour les citoyens de l'Union européenne et de l'Espace économique européen (eID-Karte-Gesetz), BGBl, I, 2019.

ESPAGNE,

Constitution espagnole, Boletín Oficial del Estado, no 311, 1978.
Code pénal espagnol (Ley Orgánica 10/1995, du 23 novembre 1995), Boletín Oficial del Estado, no 281, 1995.

ÉTATS-UNIS,
California Consumer Privacy Act of 2018 (CCPA), Assembly Bill 375, Sacramento, 2018.
California Privacy Rights Act of 2020 (CPRA), Proposition 24, 2020.
Computer Fraud and Abuse Act (CFAA), Public Law 99-474, 18 U.S. Code § 1030, 1986.
Quatrième amendement à la Constitution des États-Unis, 1791 (Bill of Rights).
USA PATRIOT Act, Public Law 107–56, 2001.

ITALIE,
Code pénal italien, article, Gazzetta Ufficiale, no 251, 1930 (version consolidée).

NORVÈGE,
Lov om gjennomføring av straff mv. (straffegjennomføringsloven) – Act no. 21 of 18 May 2001 relating to the execution of sentences etc., Norsk Lovtidend, 2001 (version consolidée).

ROYAUME-UNI,
Counter-Terrorism (Sentencing and Release) Bill et *Sentencing Bill*, présentés dans le Discours de la Reine, 14 octobre 2019, House of Commons Papers, 2019.
Criminal Justice and Immigration Act 2008, c. 4, UK Public General Acts, 2008.
Investigatory Powers Act 2016, c. 25, UK Public General Acts, 2016.
Legal Aid, Sentencing and Punishment of Offenders Act 2012, *(LASPO Act),* c. 10, UK Public General Acts, 2012.
Regulation of Investigatory Powers Act (RIPA), c. 23, UK Public General Acts, 2000.

NATIONS UNIES (ONU),

Convention sur certaines armes classiques (CCW), Assemblée générale, 1980.
Déclaration internationale sur le génome humain et les droits de l'homme, adoptée par la Conférence générale de l'UNESCO Paris, 1997.
Déclaration universelle des droits de l'homme, Assemblée générale, Paris, 1948.

ASSOCIATION MÉDICALE MONDIALE,

Déclaration d'Helsinki: recommandations guidant les médecins dans la recherche clinique, adoptée par la 18e Assemblée mondiale de la santé, Helsinki, 1964.

COMITÉ EUROPÉEN DE LA PROTECTION DES DONNÉES (EDPB),

Lignes directrices 07/2020 sur les notions de responsable du traitement et de sous-traitant dans le RGPD, version 2.0, 2020.

Réponse à la demande de la Commission européenne concernant l'application cohérente du RGPD, en particulier dans le domaine de la recherche en matière de santé, 2021.

COMMISSION EUROPÉENNE, (COM)

Communication : Intelligence artificielle pour l'Europe, 2018.

Communication : Une stratégie européenne relative aux données, 2020.

Communication relative à un plan d'action destiné à renforcer la lutte contre le financement du terrorisme, 2016.

Communication relative au deuxième rapport sur l'état d'avancement de la mise en œuvre de la stratégie de l'UE pour l'Union de la sécurité, 2021.

Communication stratégique et lutte contre la désinformation, 2018.

GROUPE DE TRAVAIL « ARTICLE 29 »,

- *Avis 15/2011 concernant la notion de consentement*, WP 187, Bruxelles, 2011.
- *Avis sur le traitement des données à caractère personnel médicales dans le dossier électronique de santé (DES),* WP 131, Bruxelles, 2008.
- *Avis 2/2017 concernant le traitement des données sur le lieu de travail*, WP 249, Bruxelles, 2017.
- *Avis 5/2009 sur les réseaux sociaux en ligne,* WP 163, 2009,

La surveillance électronique : Recommandation CM/Rec(2014)4 et exposé des motifs, Conseil de l'Europe, 2016.

Liability Rules for Artificial Intelligence, 2021.

Livre blanc – Intelligence artificielle : une approche européenne axée sur l'excellence et la confiance, 2020.

Plan d'action pour l'éducation numérique (2021–2027), 2020.

Recommandation (UE) 2024/1101 du 11 avril 2024 relative à une feuille de route pour la mise en œuvre coordonnée de la transition vers la cryptographie post-quantique 2024.
Staff Working Document, Développement de l'Internet des objets en Europe, SWD, 2016, 110 final, 2016.
Staff Working Document, Liability for Emerging Digital Technologies. Accompanying the document Artificial Intelligence for Europe, SWD, 2018, 137 final, 2018.

CONSEIL DE L'EUROPE,

Convention d'Istanbul sur la prévention et la lutte contre la violence à l'égard des femmes et la violence domestique, Istanbul, 2011.
Convention de sauvegarde des droits de l'Homme et des libertés fondamentales, Rome, 1950. (version consolidée en 2024*).*
Convention de sauvegarde des droits de l'Homme et des libertés fondamentales telle qu'amendée par le Protocole n° 15, Strasbourg, 2021.
Convention du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg 1981.
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No.108, Strasbourg, 1981.
Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, ETS No. 181, Additional Protocol, Strasbourg, 2001.
Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, (Convention 108), Strasbourg, 1981. *Protocoles additionnels en* 2001.
Convention sur la cybercriminalité (Convention de Budapest), Budapest, 2001.
Convention sur la protection des droits de l'Homme et de la dignité de l'être humain à l'égard des applications de la biologie et de la médecine : Convention sur les droits de l'Homme et la biomédecine, Oviedo, 1997.
Déclaration sur les capacités manipulatrices des processus algorithmiques, 2019.
Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif à la coopération renforcée et à la divulgation des preuves électroniques, Strasbourg, 2023.
État des signatures et ratifications du Traité n° 164 (Convention sur la cybercriminalité), Strasbourg, 2023, 2024.
Mid-term Horizontal Review of GREVIO Baseline Evaluation Reports, Strasbourg, 2022.
Recommandation CM/Rec(2010)1 sur les règles de probation du Conseil de l'Europe, Strasbourg, 2010.

Recommandation CM/Rec(2012)4 du Comité des ministres sur la protection des droits de l'homme dans les services de réseaux sociaux, Strasbourg, 2012.
Recommandation CM/Rec(2014)4 sur la surveillance électronique, Strasbourg, 2014.
Recommandation CM/Rec(2014)6 – Guide des droits de l'homme pour les utilisateurs d'Internet, Strasbourg, 2014.
Recommandation CM/Rec(2018)2 sur les rôles et responsabilités des intermédiaires de services Internet, Strasbourg, 2018.
Recommandation CM/Rec(2018)7 sur les lignes directrices pour respecter, protéger et réaliser les droits de l'enfant dans l'environnement numérique, Strasbourg, 2018.

UNION EUROPÉENNE,
Charte des droits fondamentaux de l'Union européenne (2012/C 326/02), JOUE C 326, 2012.
Déclaration d'Amsterdam sur la coopération dans le domaine de la conduite connectée et automatisée, 2016.
Directive (UE) 2016/1148 du 6 juillet 2016 concernant des mesures destinées à assurer un niveau commun élevé de sécurité des réseaux et des systèmes d'information dans l'Union, JOUE L 194, 2016.
Directive (UE) 2024/2853 du 23 octobre 2024 relative à la responsabilité du fait des produits défectueux et abrogeant la directive 85/374/CEE du Conseil.
Directive 2000/31/CE du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, JOCE L 178, 2000.
Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JOUE L 201, 2002.
Directive 2004/38/CE relative au droit des citoyens de l'Union et des membres de leur famille de circuler et de séjourner librement sur le territoire des États membres, JOUE L 158, 2004.
Directive 2005/60/CE relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, JOUE L 309, 2005.
Directive 2006/24/CE du 15 mars 2006 relative à la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, JOUE L 105, 2006.
Directive 2009/103/CE du 16 septembre 2009 relative à l'assurance de la responsabilité civile résultant de la circulation de véhicules automoteurs et à l'obligation d'assurer cette responsabilité, JOUE L 263, 2009.

Recommandation du Parlement européen du 26 mars 2009 au Conseil concernant le renforcement de la sécurité et des libertés fondamentales sur Internet, JOUE C 117, 2009.
Règlement (CE) n° 1223/2009 relatif aux produits cosmétiques, JOUE L 342, 2009.
Règlement (CE) n° 178/2002 établissant les principes généraux et les prescriptions générales de la législation alimentaire, JOUE, L 31, 2002.
Règlement (CE) n° 2252/2004 du 13 décembre 2004 concernant les normes relatives aux éléments de sécurité et aux éléments biométriques intégrés dans les passeports et documents de voyage délivrés par les États membres, JOUE L 385, 2004.
Règlement (CEE) n° 17/62, premier règlement d'application des articles 85 et 86 du Traité, JOCE 13, 1962.
Règlement (UE) 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement général sur la protection des données – RGPD), JOUE L 119, 2016.
Règlement (UE) 2017/745 du 5 avril 2017 relatif aux dispositifs médicaux, modifiant la directive 2001/83/CE, JOUE L 117, 2017.
Règlement (UE) 2017/746 du 5 avril 2017 relatif aux dispositifs médicaux de diagnostic in vitro, JOUE L 117, 2017.
Règlement (UE) 2018/858 du 30 mai 2018 relatif à l'homologation et à la surveillance du marché des véhicules à moteur, JOUE L 151, 2018.
Règlement (UE) 2019/1157 du 20 juin 2019 relatif au renforcement de la sécurité des cartes d'identité, JOUE L 188, 2019.
Règlement (UE) 2019/2144 du 27 novembre 2019 relatif à la sécurité des véhicules et à la protection des occupants, JOUE L 325, 2019.
Règlement (UE) 2021/695 du 28 avril 2021 établissant Horizon Europe, JOUE L 170, 2021.
Règlement (UE) 2022/2065 du 19 octobre 2022 relatif à un marché unique des services numériques (Digital Services Act), JOUE L 277, 2022.
Règlement (UE) 2024/1689 du 13 juin 2024 établissant des règles harmonisées concernant l'intelligence artificielle (Artificial Intelligence Act), JOUE L 202, 2024.
Règlement (UE) n° 1215/2012 du 12 décembre 2012 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale (refonte), JOUE L 351, 2012.
Règlement (UE) n° 603/2013 du Parlement européen et du Conseil du 26 juin 2013 relatif à l'établissement d'Eurodac, JOUE L 180, 2013.
Résolution du 12 février 2019 relative à une politique industrielle européenne globale en matière d'intelligence artificielle et de robotique, 2018/2088(INI), Strasbourg, 2019.

Résolution du 12 septembre 2018 sur les systèmes d'armes autonomes, 2018/2752(RSP), Strasbourg, 2018.
Résolution du 14 mars 2017 relative aux implications des mégadonnées sur les droits fondamentaux : vie privée, protection des données, non-discrimination, sécurité et application de la loi, 2016/2225(INI), Strasbourg, 2017.
Résolution du 16 février 2022 sur le renforcement de l'Europe dans la lutte contre le cancer – vers une stratégie globale et coordonnée, 2020/2267(INI), Strasbourg, 2022.
Résolution sur le chiffrement. Sécurité par le chiffrement et sécurité malgré le chiffrement, JOUE C 408, 2020.

Législation française

Code civil, Journal Officiel de la République française, Paris, 1804 (version consolidée).
Code de justice administrative, Journal Officiel de la République française, Paris, 2000 (version consolidée).
Code de la communication, Journal Officiel de la République française, Paris, 1982 (version consolidée).
Code de la construction et de l'habitation, Journal Officiel de la République française, Paris, 1978 (version consolidée).
Code de la protection des données personnelles, Journal Officiel de la République française, Paris, 2018.
Code de la santé publique, Journal Officiel de la République française, Paris, 1953 (version consolidée).
Code de la sécurité intérieure, Journal Officiel de la République française, Paris, 2012 (version consolidée).
Code de procédure pénale, Journal Officiel de la République française, Paris, 1958 (version consolidée).
Code du travail, Journal Officiel de la République française, Paris, 2006 (version consolidée).
Code pénal de 1810. Édition originale, publiée sous le titre « Code des délits et des peines », Imprimerie impériale, Paris, 1810.
Code pénal, Journal Officiel de la République française, Paris, 1992 (version actuelle).
Constitution du 4 octobre 1958 Journal Officiel de la République française, *1958*.

SÉNAT ET ASSEMBLÉE NATIONALE,

- *Bilan de la suppression de normes*, Question écrite n° 1584, 2022.

- *Déclaration des droits de l'Homme et du citoyen*, Journal officiel de la République française, 1789.
- *La surtransposition des directives européennes*, Note de législation comparée n° 277, février 2017.
- *Loi du 29 juillet 1881 sur la liberté de la presse*, JO, 1881.
- *Loi du 4 mars 2002 relative aux droits des malades et à la qualité du système de santé (« loi Kouchner »),* JO, 2002.
- *Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations,* JO, 2000.
- *Loi n° 2000-516 du 15 juin 2000 renforçant la protection de la présomption d'innocence et les droits des victimes*, JO, 2000.
- *Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne,* JO, 2001.
- *Loi n° 2002-1138 du 9 septembre 2002 d'orientation et de programmation pour la justice*, JO, 2002.
- *Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure*, JO, 2003.
- *Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité*, JO, 2004.
- *Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,* JO, 2004.
- *Loi n° 2009-1436 du 24 novembre 2009 pénitentiaire*, JO, 2009.
- *Loi n° 2010-242 du 10 mars 2010 tendant à amoindrir le risque de récidive criminelle et portant diverses dispositions de procédure pénale, 2010.*
- *Loi n° 2010-769 relative aux violences spécifiques faites aux femmes, aux violences au sein des couples et à l'incidence de ces dernières sur les enfants*, JO, 2010.
- *Loi n° 2011-814 du 7 juillet 2011 relative à la bioéthique,* JO, 2011.
- *Loi n° 2014-372 du 28 mars 2014 relative à la géolocalisation*, JO, 2014.
- *Loi n° 2014-896 du 15 août 2014 relative à l'individualisation des peines et renforçant l'efficacité des sanctions pénales*, JO, 2014.
- *Loi n° 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationales*, JO, 2015.
- *Loi n° 2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public*, JO, 2015.
- *Loi n° 2015-912 du 24 juillet 2015 relative au renseignement,* JO, 2015.
- *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique,* JO, 2016.

- *Loi n° 2016-1691 du 9 décembre 2016 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique,* JO, 2016.
- *Loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale,* JO, 2016.
- *Loi n° 2017-1510 du 30 octobre 2017 renforçant la sécurité intérieure et la lutte contre le terrorisme*, JO, 2017.
- *Loi n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information,* JO, 2018.
- *Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité*, JO, 2018.
- *Loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes,* JO, 2018.
- *Loi n° 2019-1428 du 24 décembre 2019 d'orientation des mobilités*, JO, 2019.
- *Loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice,* JO, 2019.
- *Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet*, JO, 2020.
- *Loi n° 2020-936 du 30 juillet 2020 visant à protéger les victimes de violences conjugales*, JO, 2020.
- *Loi n° 2021-1017 du 2 août 2021 relative à la bioéthique*, JO, 2021.
- *Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement*, JO, 2021.
- *Loi n° 2023-380 du 19 mai 2023 relative aux Jeux Olympiques et Paralympiques de 2024 et portant diverses autres dispositions,* JO, 2023.
- *Loi n° 2023-566 du 7 juillet 2023 visant à instaurer une majorité numérique et à lutter contre la haine en ligne, JO,* 2023.
- *Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense*, JO, 2023.
- *Loi n° 2024-120 du 19 février 2024 visant à garantir le respect du droit à l'image des enfants*, JO, 2024.
- *Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique*, JO, 2024.
- *Loi n° 70-643 du 17 juillet 1970 tendant à renforcer la garantie des droits individuels des citoyens*, JO, 1970.

- *Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés,* JO, 1978.
- *Loi n° 83-1179 du 29 décembre 1983 de finances pour 1984*, JO, 1983.
- *Loi n° 95-125 du 8 février 1995 relative à l'organisation des juridictions et à la procédure civile, pénale et administrative*, JO, 1995.
- *Loi no 2015-912 du 24 juillet 2015 relative au renseignement,* JO*,* 2015.
- *Loi no 78-17 du janvier 1978 relative a l'informatique, aux fichiers et aux libertés*, JO, 1978.
- *Lutte contre la manipulation de l'information. Loi relative à la lutte contre la manipulation de l'information*, JO, 2018.
- *Proposition de loi n° 367 (2013-2014) relative au fichage*, 2014.
- *Proposition de loi relative à la sécurité globale, n°3452*, Paris, 2020.
- Proposition de résolution n° 724 (2016-2017), *Simplification des normes entravant la vie économique*, 2017.
- *Rapport sur le projet de loi relatif à la bioéthique*, 2020.
- *Séance du 28 janvier 2020. Comptes rendus intégraux de janvier 2020*, 2020.

GOUVERNEMENT,

- *Décret n° 2006-736 du 26 juin 2006 relatif à la lutte contre le blanchiment de capitaux*, 2006.
- *Décret n° 2020-81 du 3 février 2020 relatif à la peine de détention à domicile sous surveillance électronique*, 2020.
- *Décret n° 2021-922 du 13 juillet 2021 portant création d'un service de vigilance et de protection contre les ingérences numériques étrangères*, 2021.
- *Décret n° 2023-552 du 30 juin 2023 portant Code de déontologie des avocats*, 2023.
- *Plan pénitentiaire. Présentation*, Ministère de la Justice, 2018.
- *Rapport de lutte contre la cybercriminalité*, Ministère des Finances, Notes Bleues de Bercy, n° 289, 2005.
- *Ordonnance n° 2011-1012 du 24 août 2011 relative aux communications électroniques*, JO, 2011.
- *Ordonnance n° 2019-964 du 18 septembre 2019 relative à la programmation 2018-2022 et à la réforme pour la justice*, JO, 2019.
- *Ordonnance n° 2020-324 du 25 mars 2020 relative à des mesures d'urgence en matière de revenus de remplacement mentionnés à l'article L. 5421-2 du code du travail*, JO, 2020.

- *Projet de loi relatif à la programmation militaire pour les années 2019 à 2025 et portant diverses dispositions intéressant la défense*, n° 659, 2018.
- *Décret n° 2016-146 du 11 février 2016 relatif aux modalités de publication et de transmission des actes des collectivités territoriales et des établissements publics de coopération intercommunale,* JO*, 2016*.
- *Décret n° 2020-797 du 29 juin 2020 relatif à la mise à la disposition du public des décisions des juridictions judiciaires et administratives,* JO, 2020.
- *Décret n° 2019-536 du 29 mai 2019 pris pour l'application de la loi n° 78-17 du 6 janvier 1978*, 2019.

L'ASSEMBLÉE GÉNÉRALE DU CONSEIL NATIONAL DES BARREAUX

- *Décision du 26 janvier 2017 portant réforme du Règlement Intérieur National (RIN) de la profession d'avocat,* JO, no 0088, 2017.

Législation roumaine

Codul civil al României, republicat, Monitorul Oficial al României, nr. 505, 2011.
Codul de deontologie medicală al Colegiului Medicilor din România, Monitorul Oficial al României, nr. 981 2016.
Codul de procedură penală al României, adoptat prin Legea nr. 135/2010, Monitorul Oficial al României, nr. 486, 2010 (versiune actualizată).
Codul Penal din 17 iulie 2009, adoptat prin Legea nr.286/2009, Monitorul Oficial al României nr. 510, 2009.
Constituția României, *adoptată în 1991, revizuită prin Legea de revizuire nr.429/2003*, Monitorul Oficial al României, nr. 758, 2003.

GOUVERNEMENT DE LA ROUMANIE,

- *Decretul nr. 59 din 2 martie 1978 pentru modificarea Legii nr. 5/1971 privind actele de identitate și regimul schimbării domiciliulu*, Monitorul Oficial al Republicii Socialiste România, n° 15 1978.
- *Exposé des motifs concernant l'élaboration et l'adoption d'un nouveau code pénal, Ministère de la Justice,2009.*
- *Hotărâre privind aprobarea Strategiei Naționale în domeniul Inteligenței Artificiale 2024-2027,* Monitorul Oficial al României, nr. 730, 2024.
- *Hotărâre nr. 755 din 4 iulie 2024 privind stabilirea datei alegerilor pentru Senat et Camera Deputaților din anul 2024*, Monitorul Oficial al României, nr. 755, 2024.

- *Hotărârea nr. 1.194 din 27 noiembrie 2001 privind organizarea şi funcţionarea Consiliului Naţional pentru Combaterea Discriminării*, Monitorul Oficial al României, nr. 792, 2001.
- *Ordinul nr. 904/2006 privind aprobarea Normelor de aplicare a Legii nr. 95/2006,* Monitorul Oficial al României, nr. 628, 2006.
- *Ordonanţa de urgenţă a Guvernului nr. 6 din 14 martie 2016 privind unele măsuri pentru punerea în executare a mandatelor de supraveghere tehnică dispuse în procesul penal,* Monitorul Oficial al României, nr. 190, 2016.
- *Ordonanța nr. 137/2000 privind prevenirea și sancționarea tuturor formelor de discriminare,* Monitorul Oficial al României, nr. 537, 2008.
- *Ordonanță de urgență nr. 14/2022 pentru modificarea Legii nr. 146/2021 privind monitorizarea electronică,* Monitorul Oficial al României, nr.182, 2022.
- *Ordonanță de urgență nr. 60/2006 pentru modificarea și completarea Codului de procedură penală,* Monitorul Oficial al României, nr. 764, 2006.
- *Ordonanță de urgență nr. 61/2024 pentru modificarea Legii nr. 146/2021 privind monitorizarea electronică,* Monitorul Oficial al României, 2024.
- *Strategia militara a României din 11 august 2021,* Monitorul Oficial al României, nr. 781, 2021.

PARLEMENT DE LA ROUMANIE,

- *Codul audiovizualului*, republicată și consolidată, Monitorul Oficial al României, nr. 641, 2025.
- *Legea audiovizualului nr.504/2002, republicată,* Monitorul Oficial al României nr. 261, 2025.
- *Legea nr. 11/1991 privind combaterea concurenței neloiale*, Monitorul Oficial al României nr. 24, 1991.
- *Legea nr. 146 din 17 mai 2021 privind monitorizarea electronică în cadrul unor proceduri judiciare și execuțional penale*, Monitorul Oficial al României, nr. 515, 2021.
- *Legea nr. 151 din 13 iulie 2016 privind ordinul european de protecție, precum și pentru modificarea și completarea unor acte normative*, Monitorul Oficial al României, nr. 545, 2016.
- *Legea nr. 171 din 14 iunie 2023 pentru modificarea și completarea art. 226 din Legea nr. 286/2009 privind Codul penal*, Monitorul Oficial nr. 532, 2023.
- *Legea nr. 217 din 22 mai 2003* (republicată) pentru prevenirea și combaterea violenței domestice, Monitorul Oficial nr. 948, 2003.

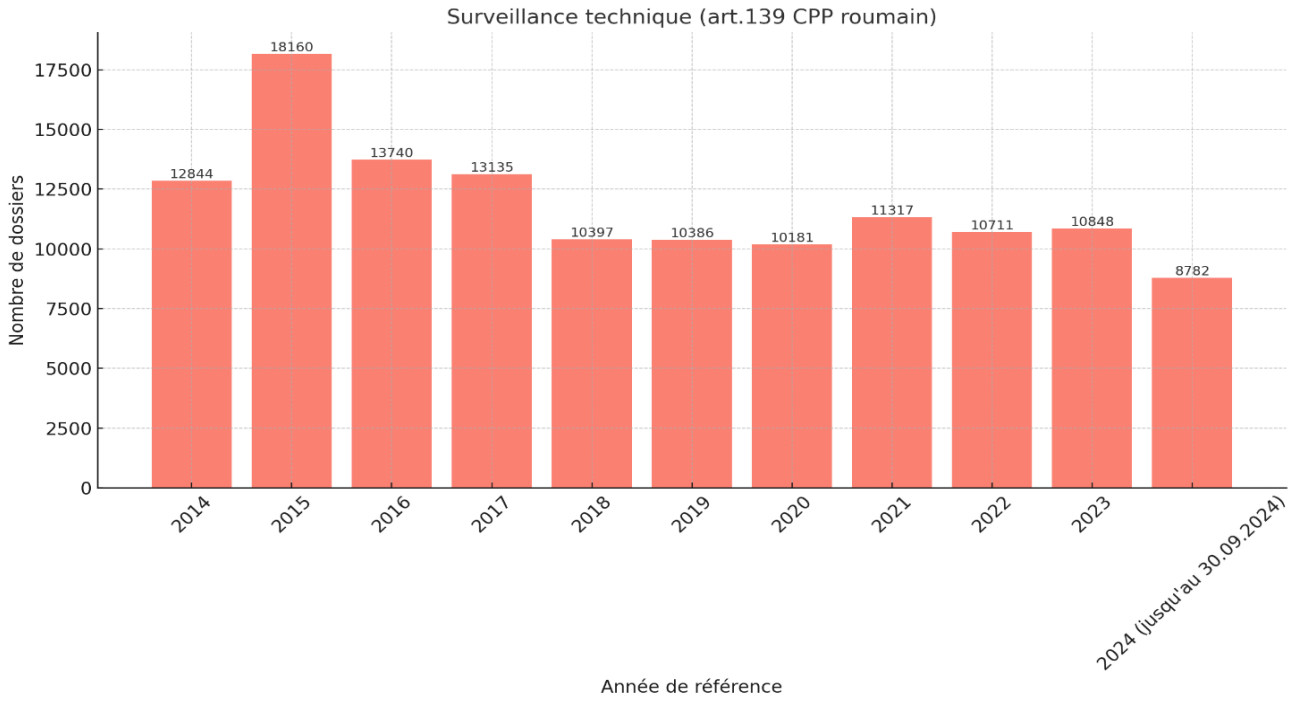
- *Legea nr. 254 din 19 iulie 2013 privind executarea pedepselor și a măsurilor privative de libertate dispuse de organele judiciare în cursul procesului penal*, Monitorul Oficial al României, nr. 514, 2013.
- *Legea nr. 290 din 24 iunie 2004 (republicată, actualizată până la data de 10 decembrie 2016) privind cazierul judiciar*, Monitorul Oficial al României nr. 586, 2004.
- *Legea nr. 30/2016 pentru ratificare Convenției Consiliului Europei privind prevenirea și combaterea violenței împotriva femeilor și a violenței domestice,* Monitorul Oficial al României, nr. 224, 2016.
- *Legea nr. 46 din 21 ianuarie 2003 privind drepturile pacientului*, Monitorul Oficial al României, nr.51, 2003.
- *Legea nr. 51 din 29 iulie 1991* privind siguranța națională a României *(republicată),*Monitorul Oficial al României nr. 190, 2014.
- *Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date*, Monitorul Oficial al României, nr. 790, 2001. (Abrogată)
- *Legea nr. 76 din 8 aprilie 2008 privind organizarea și funcționarea Sistemului Național de Date Genetice Judiciare*, Monitorul Oficial al României, nr. 289, 2008.
- *Legea nr. 95 din 14 aprilie 2006 (republicată) privind reforma în domeniul sănătății,* Monitorul Oficial al României, nr. 652, 2015.
- *Proiect de Lege privind utilizarea responsabilă a tehnologiei în contextul fenomenului deepfake*, PL-x nr. 471/2023.

Annexes

Annexe 1 – Données statistiques concernant la situation en Roumanie

Annexe 2 – Données statistiques concernant la situation en France

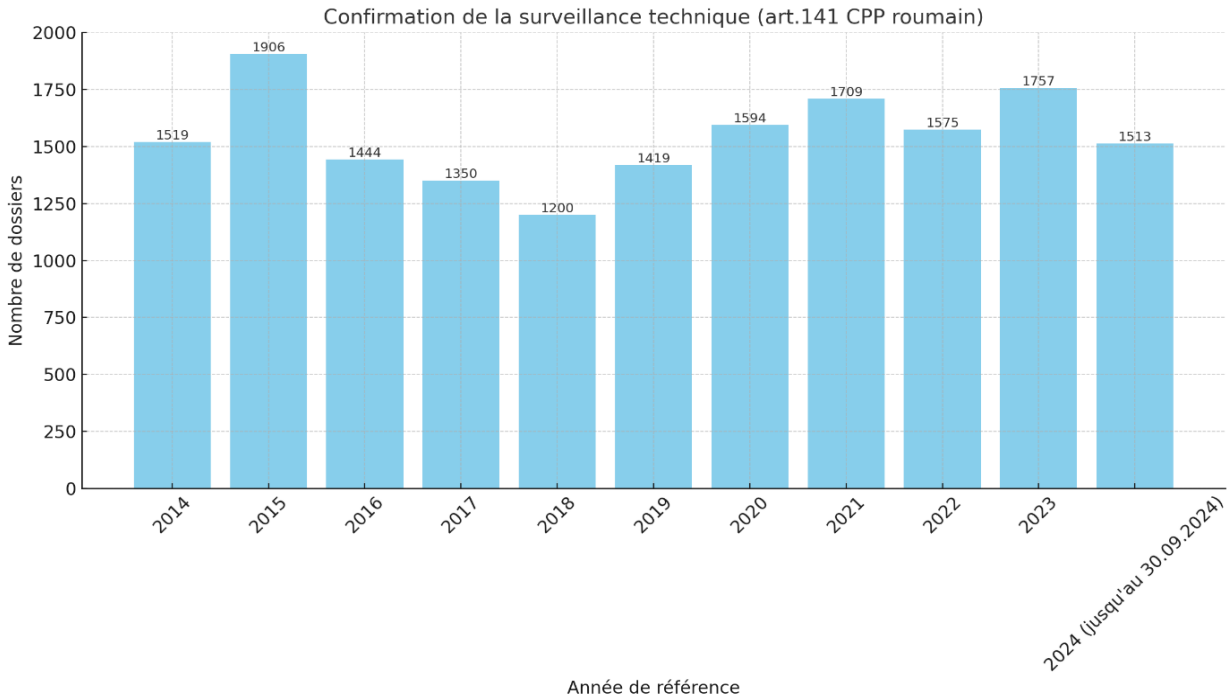
Annexe 1 – *Données statistiques concernant la situation en Roumanie*



Analyse visant le nombre de dossiers de toutes les juridictions de Roumanie, à l'exception de la Haute Cour et des mandats exécutés directement par le SRI.

Les données ont été mises à disposition par le Ministère de la Justice de Roumanie aux fins de la documentation de la présente étude.

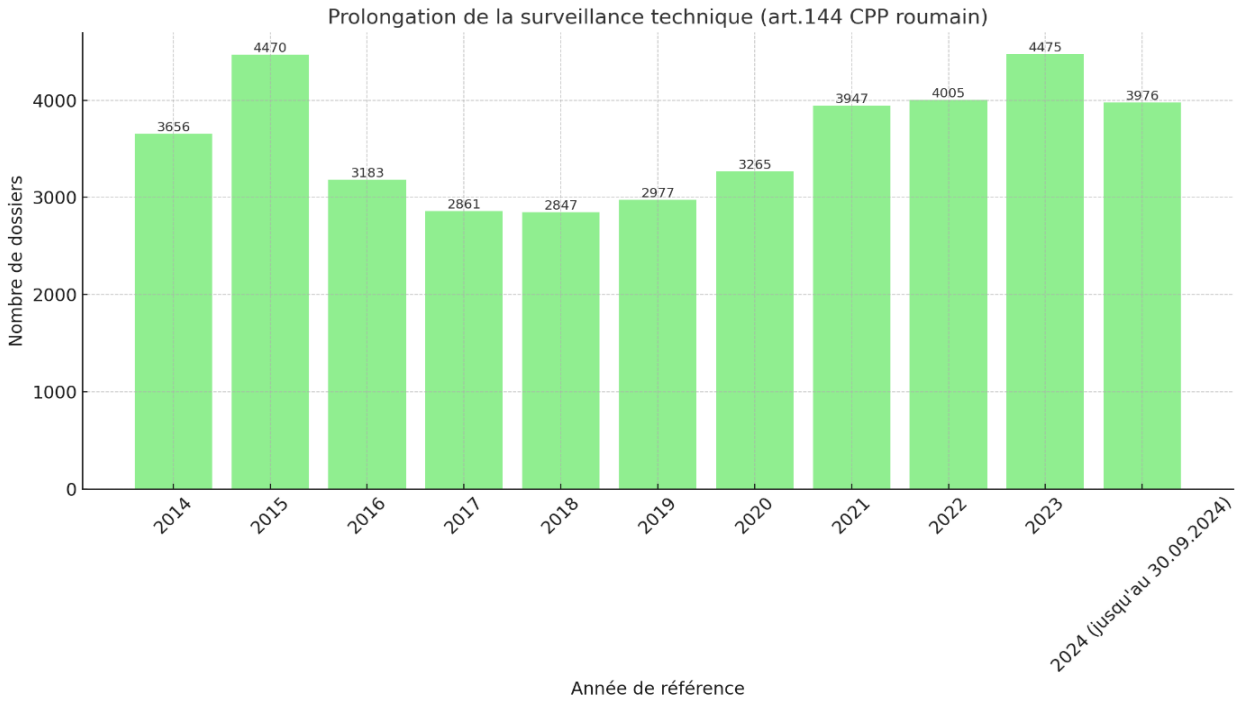
Figure 1 – Surveillance technique (art.139 CPP roumain)



Analyse visant le nombre de dossiers de toutes les juridictions de Roumanie, à l'exception de la Haute Cour et des mandats exécutés directement par le SRI.

Les données ont été mises à disposition par le Ministère de la Justice de Roumanie aux fins de la documentation de la présente étude.

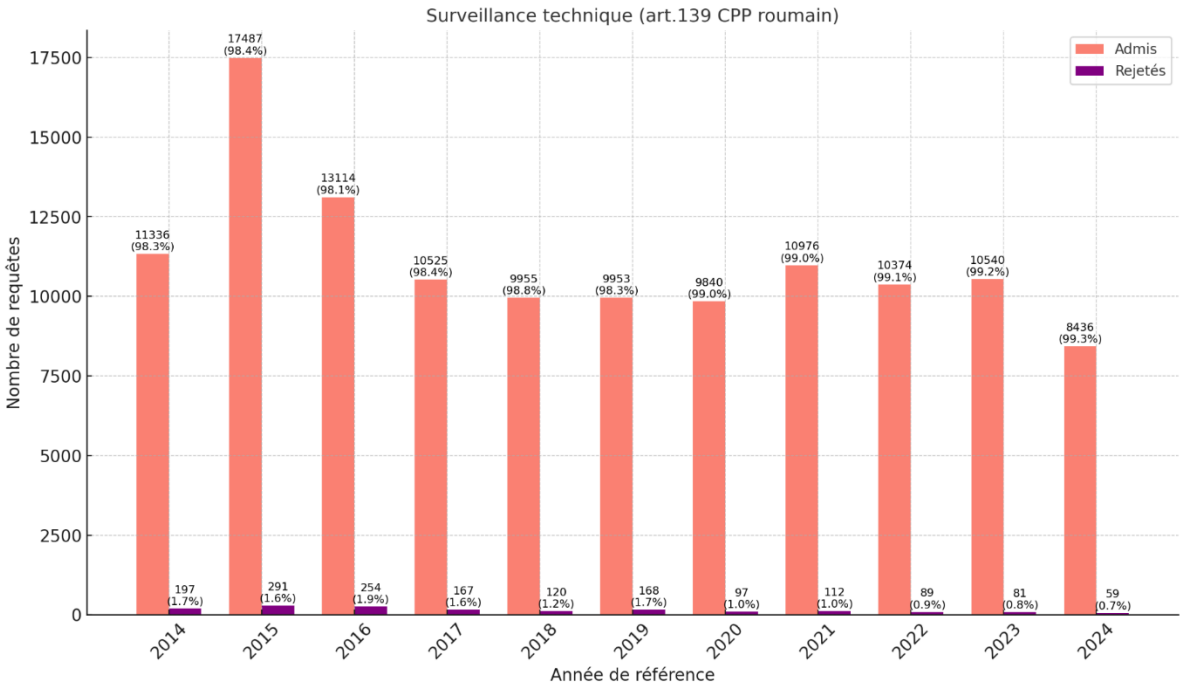
Figure 2 – Confirmation de la surveillance technique (art.141 CPP roumain)



Analyse visant le nombre de dossiers de toutes les juridictions de Roumanie, à l'exception de la Haute Cour et des mandats exécutés directement par le SRI.

Les données ont été mises à disposition par le Ministère de la Justice de Roumanie aux fins de la documentation de la présente étude.

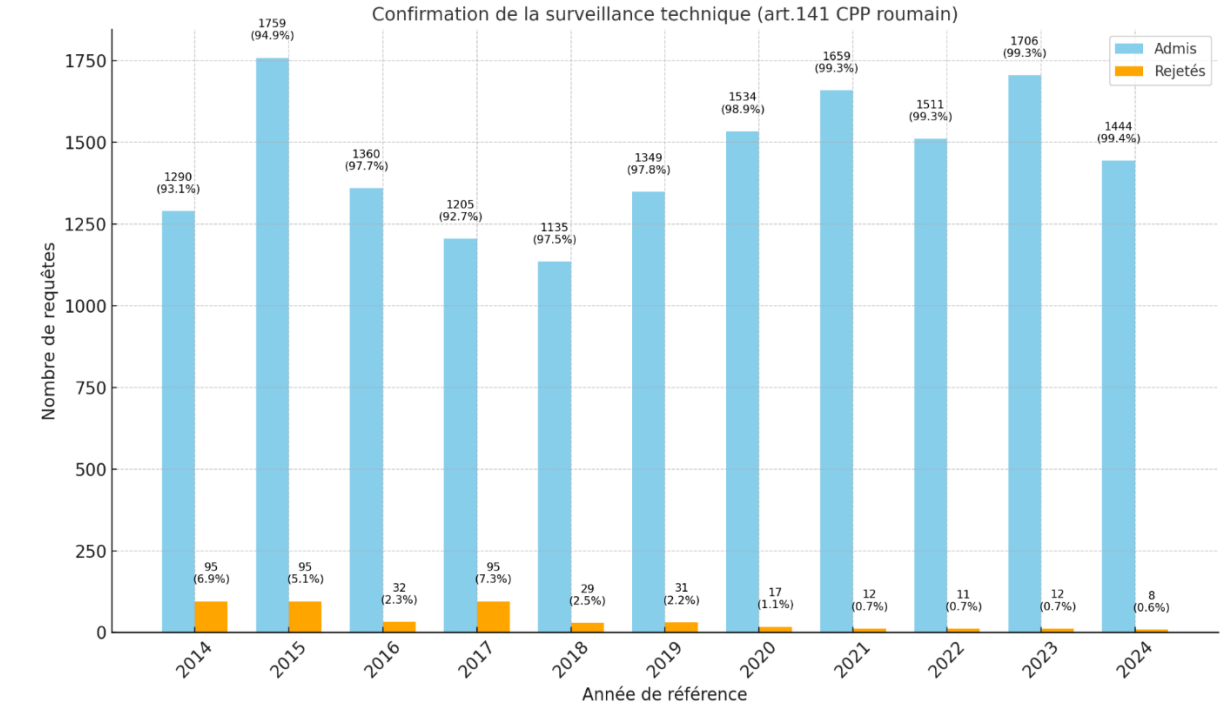
Figure 3 – prolongation de la surveillance technique (art.144 CPP roumain)



Les données ont été mises à disposition par le Ministère de la Justice et centralisées spécialement pour la présente thèse de doctorat.

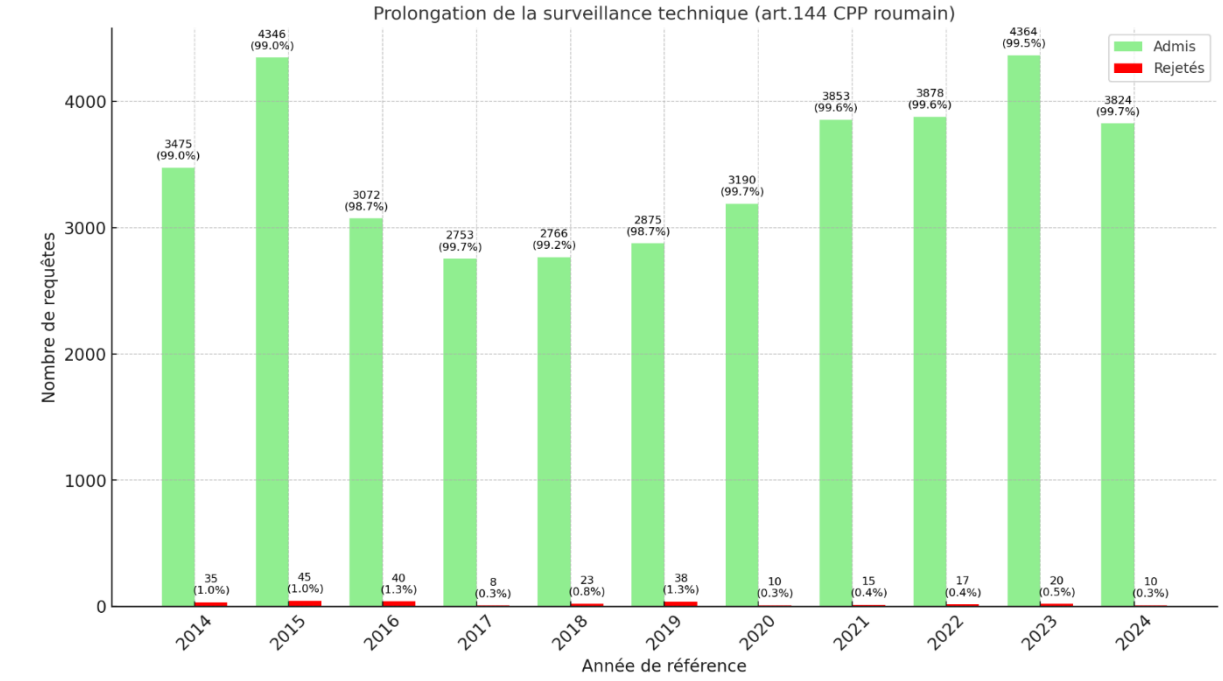
L'analyse vise tous les dossiers enregistrés auprès des juridictions, à l'exception des mandats relatifs à la sécurité nationale exécutés par le SRI ou émis par la Haute Cour de cassation et de justice. Pour l'année 2024, elles sont valables jusqu'au 30.09.2024.

Figure 4 – Surveillance technique (art.139 CPP roumain)



Les données ont été mises à disposition par le Ministère de la Justice et centralisées spécialement pour la présente thèse de doctorat.
L'analyse vise tous les dossiers enregistrés auprès des juridictions, à l'exception des mandats relatifs à la sécurité nationale exécutés par le SRI ou émis par la Haute Cour de cassation et de justice. Pour l'année 2024, elles sont valables jusqu'au 30.09.2024.

Figure 5 – Confirmation de la surveillance technique (art.141 CPP roumain)



Les données ont été mises à disposition par le Ministère de la Justice et centralisées spécialement pour la présente thèse de doctorat.
L'analyse vise tous les dossiers enregistrés auprès des juridictions, à l'exception des mandats relatifs à la sécurité nationale exécutés par le SRI ou émis par la Haute Cour de cassation et de justice. Pour l'année 2024, elles sont valables jusqu'au 30.09.2024.

Figure 6 – prolongation de la surveillance technique (art.144 CPP roumain)

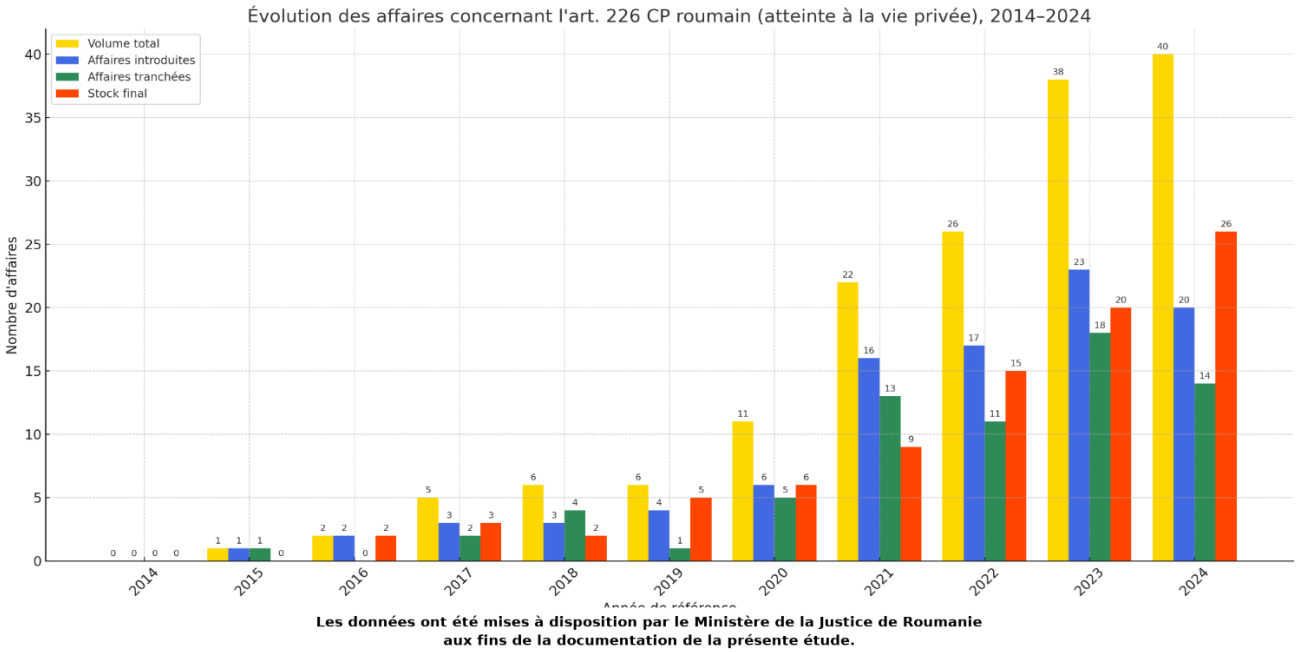


Figure 7 – Évolution des affaires cocernant l'art. 226 CPP roumain (atteinte à la vie privée), 2014-2024

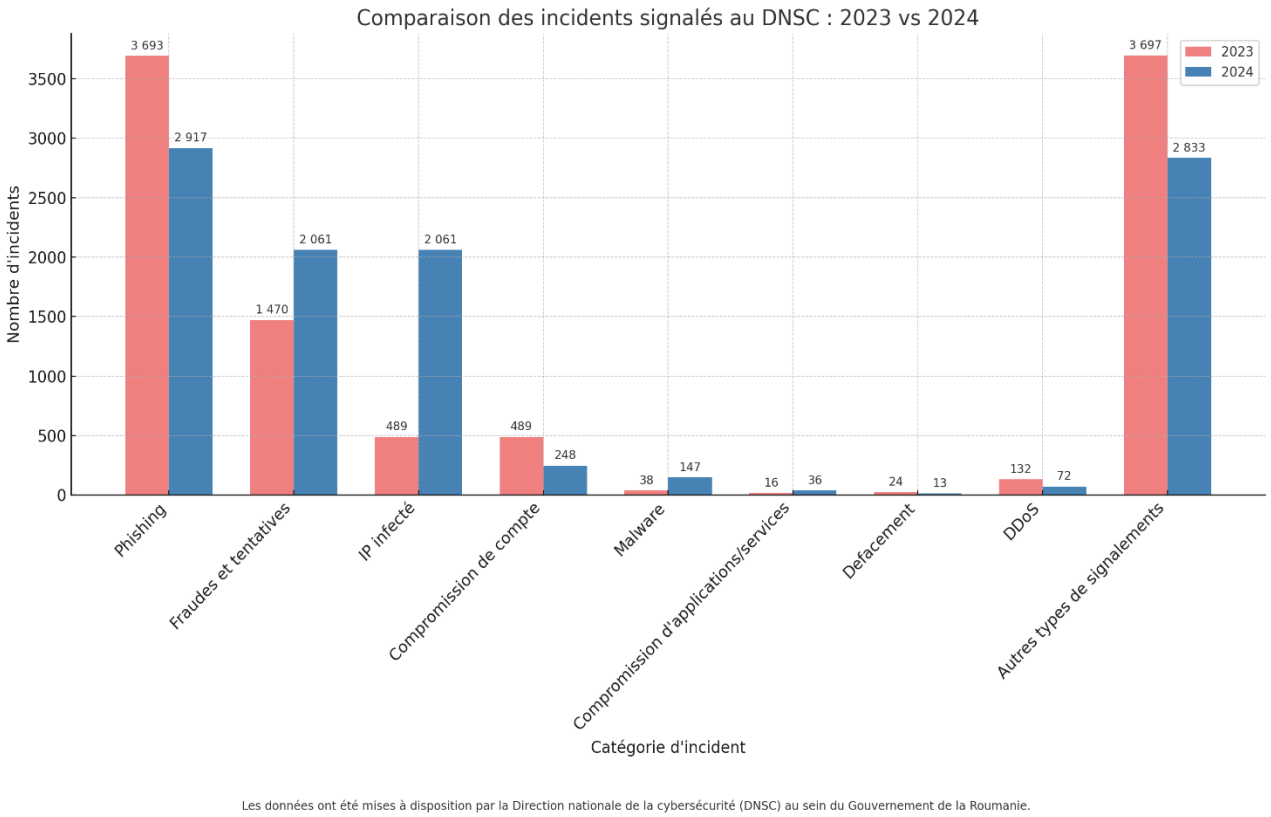
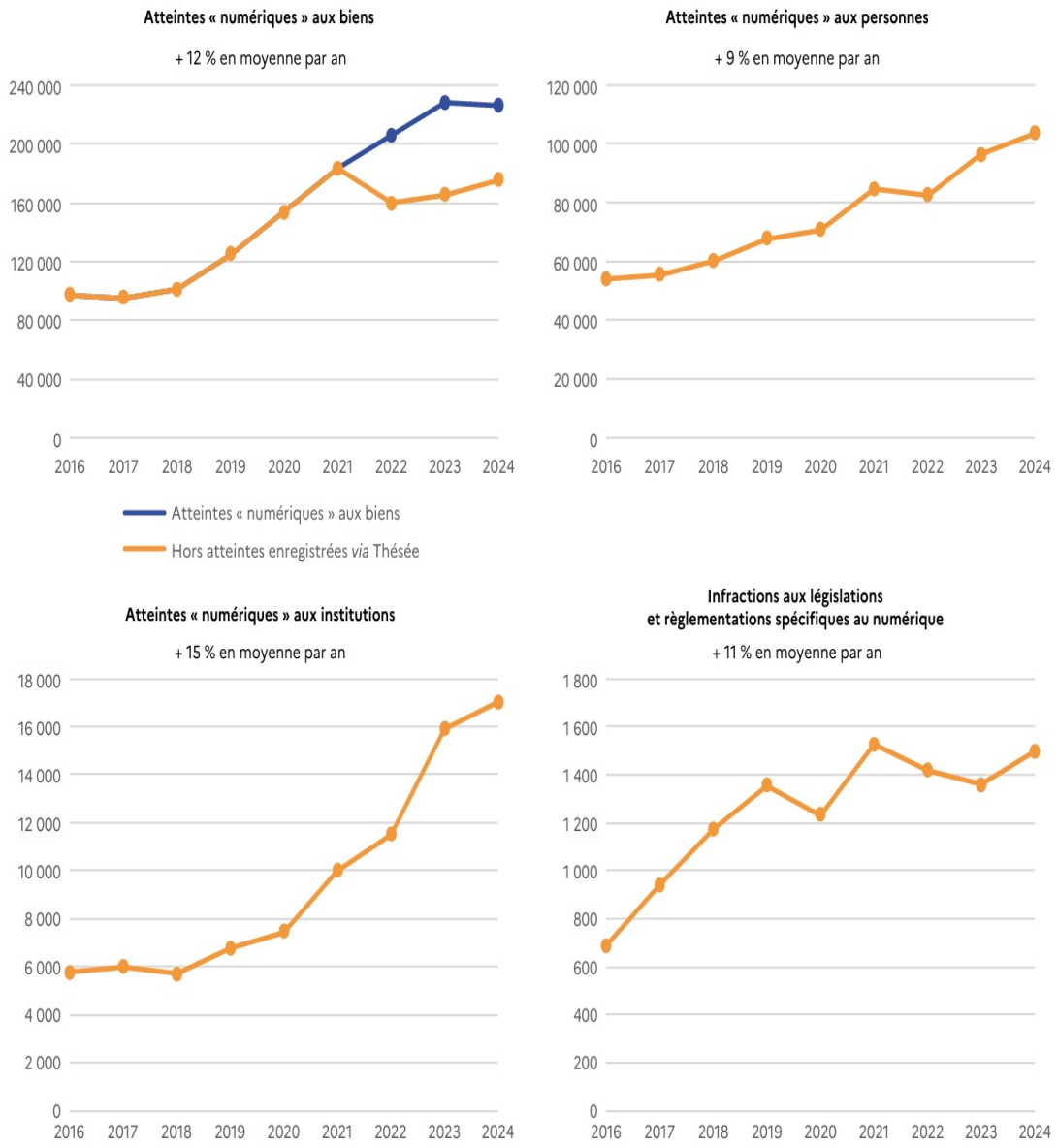


Figure 8 – Comparaison des incidents signalés au DNSC: 2023 vs 2024.)

Annexe 2 – *Données statistiques concernant la situation en France*



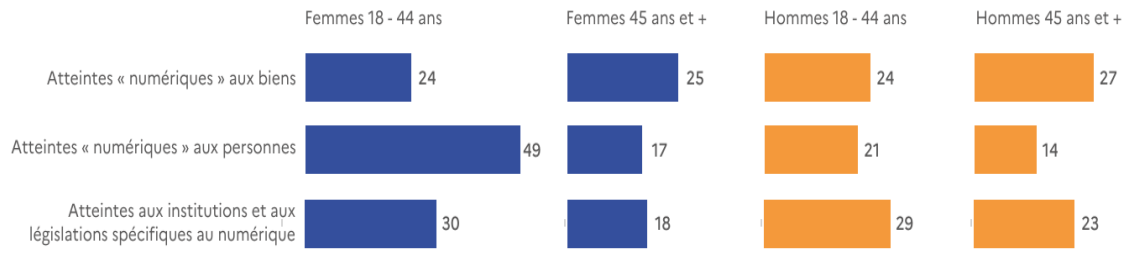
Lecture : En 2024, 226 300 infractions désignant des atteintes « numériques » aux biens ont été enregistrées par les services de sécurité. Entre 2016 et 2024, les infractions « numériques » relevant des atteintes aux biens ont augmenté de 12 % par an en moyenne.
Champ : Crimes et délits enregistrés en France.
Source : *SSMSI, bases statistiques des infractions enregistrées ou élucidées par la police et la gendarmerie entre 2016 et 2024. Base 2024 provisoire.*

Figure 9 – Évolution du nombre d'infractions « numériques » et évolution annuelle moyenne par catégorie entre 2016 et 2024 (Source SSMSI - Service statistique ministériel de la sécurité intérieure)

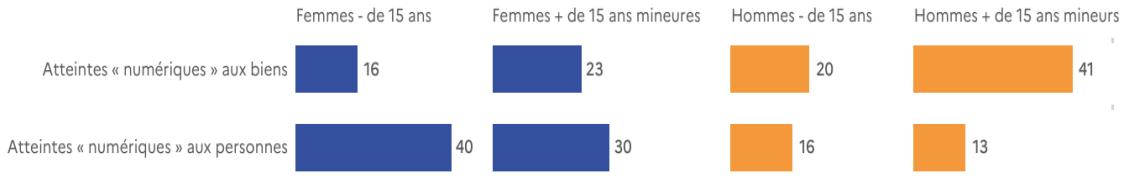
	2016	2017	2018	2019	2020	2021	2022	2023	2024
Atteintes aux biens	10 100	9 800	9 300	10 600	13 000	15 100	15 400	17 500	16 600
dont atteintes enregistrées via Thésée	*0*	*0*	*0*	*0*	*0*	*0*	*96*	*74*	*32*
hors atteintes enregistrées via Thésée	*10 100*	*9 800*	*9 300*	*10 600*	*13 000*	*15 100*	*15 300*	*17 400*	*16 600*
Atteintes aux personnes	230	250	240	270	270	290	240	280	330
Autres	34	35	54	59	63	66	90	118	163
Total	**10 400**	**10 100**	**9 600**	**10 900**	**13 300**	**15 400**	**15 700**	**17 800**	**17 100**

Note : Regroupement des catégories atteintes aux institutions et législation spécifique au numérique en raison d'effectifs trop faibles.
Lecture : En 2016, 10 100 atteintes aux systèmes de traitement automatisé de données et relevant d'une atteinte aux biens ont été enregistrées par les forces de sécurité.
Champ : Crimes et délits enregistrés en France.
Source : *SSMSI, bases statistiques des infractions enregistrées ou élucidées par la police et la gendarmerie entre 2016 et 2024. Base 2024 provisoire.*

Figure 10 – Évolution du nombre d'atteintes aux systèmes de traitement automatisé de données entre 2016 et 2024 par catégorie d'infractions numériques. (source: SSMSI - Bases statistiques des infractions enregistrées ou élucidées par la police et la gendarmerie entre 2016 et 2024).



Note : Regroupement des catégories comptabilisant les atteintes « numériques » aux institutions et celles aux législations spécifiques au numérique en raison d'effectifs trop faibles.
Lecture : En 2024, 49 % des victimes majeures d'une atteinte à la personne « numériques » sont des femmes âgées de 18 à 44 ans.
Champ : Crimes et délits enregistrés en France. Victimes âgées de 18 ans et plus au moment des faits.
Source : *SSMSI, base statistique provisoire des victimes enregistrées par la police et la gendarmerie en 2024.*



Lecture : En 2024, 16 % des victimes mineures d'une atteinte à la personne « numériques » sont des femmes âgées de moins de 15 ans.
Champ : Crimes et délits enregistrés en France. Victimes âgées de 18 ans et plus au moment des faits.
Source : *SSMSI, base statistique provisoire des victimes enregistrées par la police et la gendarmerie en 2024.*

Figure 11 –profil des victimes majeures par sexe, âge et catégorie d'infraction numérique en 2024. (source: SSMSI, bases statistiques des infractions enregistrées ou élucidées par la police et la gendarmerie entre 2016 et 2024).

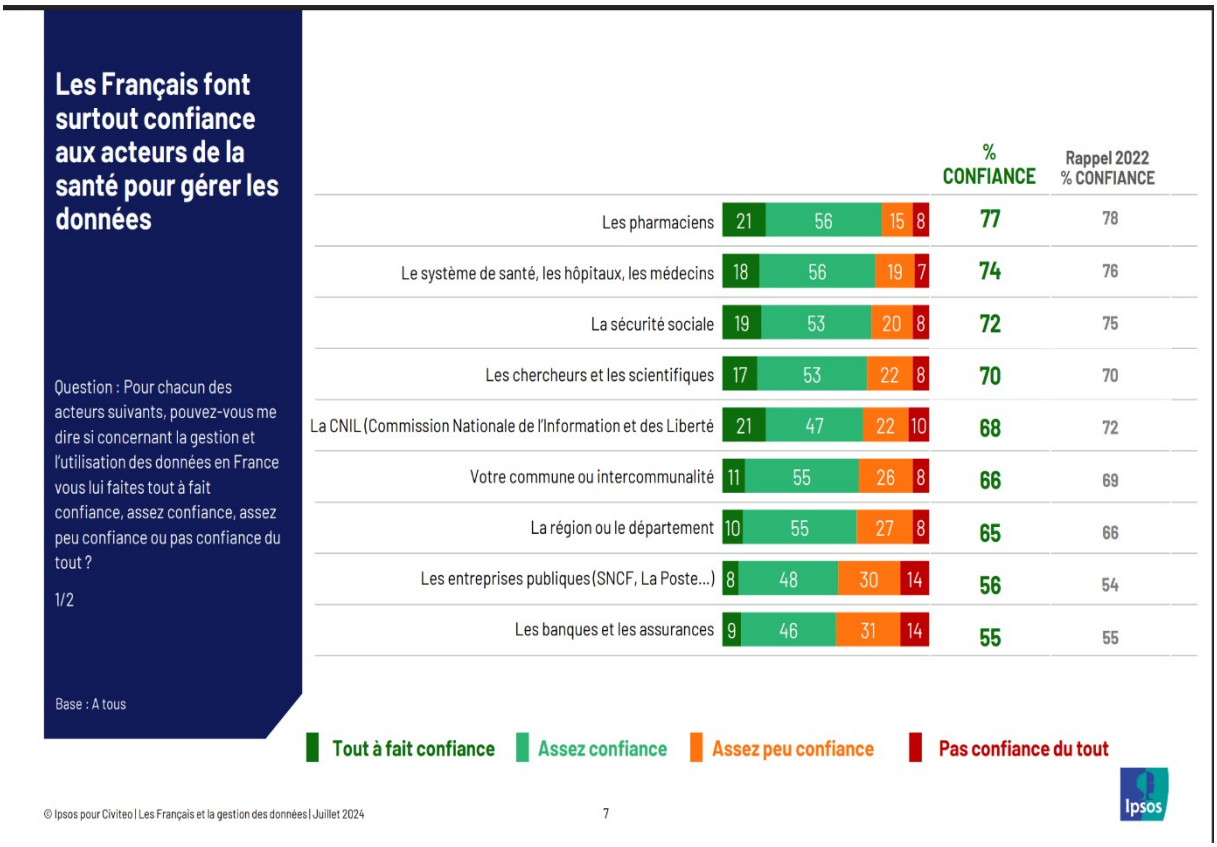


Figure 12 — Les Français font surtout confiance aux acteurs de la santé pour gérer les données (source: Ipsos -Global Market Research and Public Opinion Specialist).

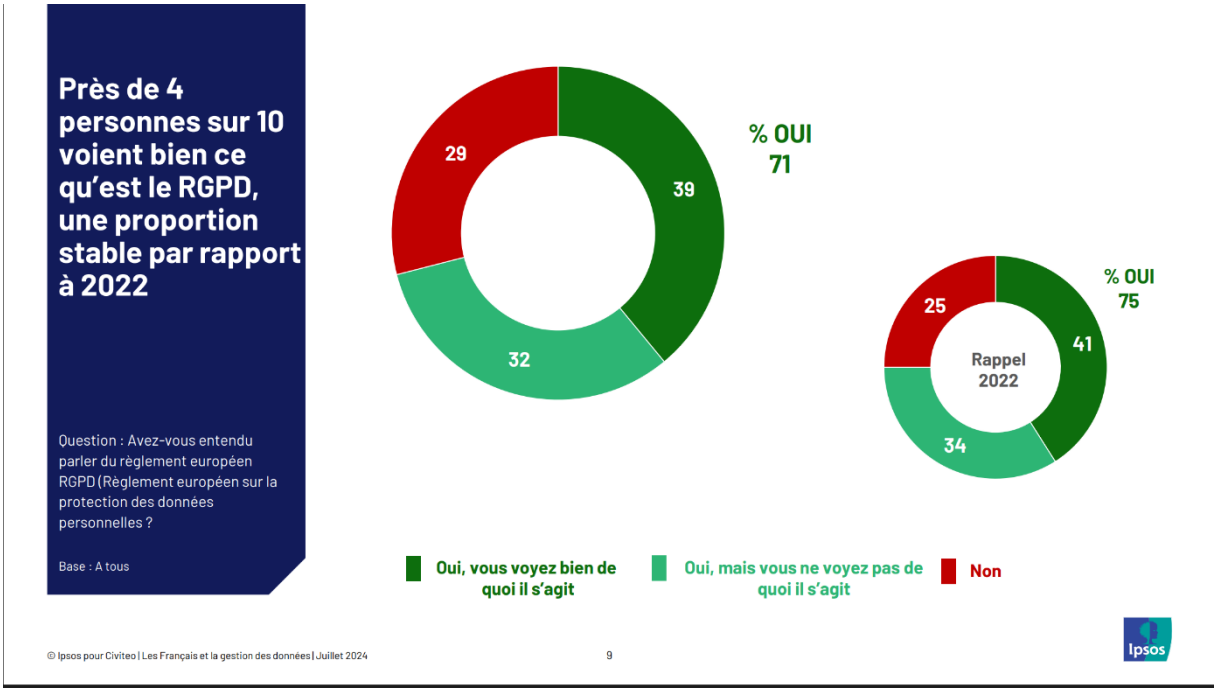


Figure 13 – Près de 4 personnes sur 10 voient bien ce qu'est le RGPD, une proportion stable par rapport à 2022 (source: Ipsos -Global Market Research and Public Opinion Specialist).

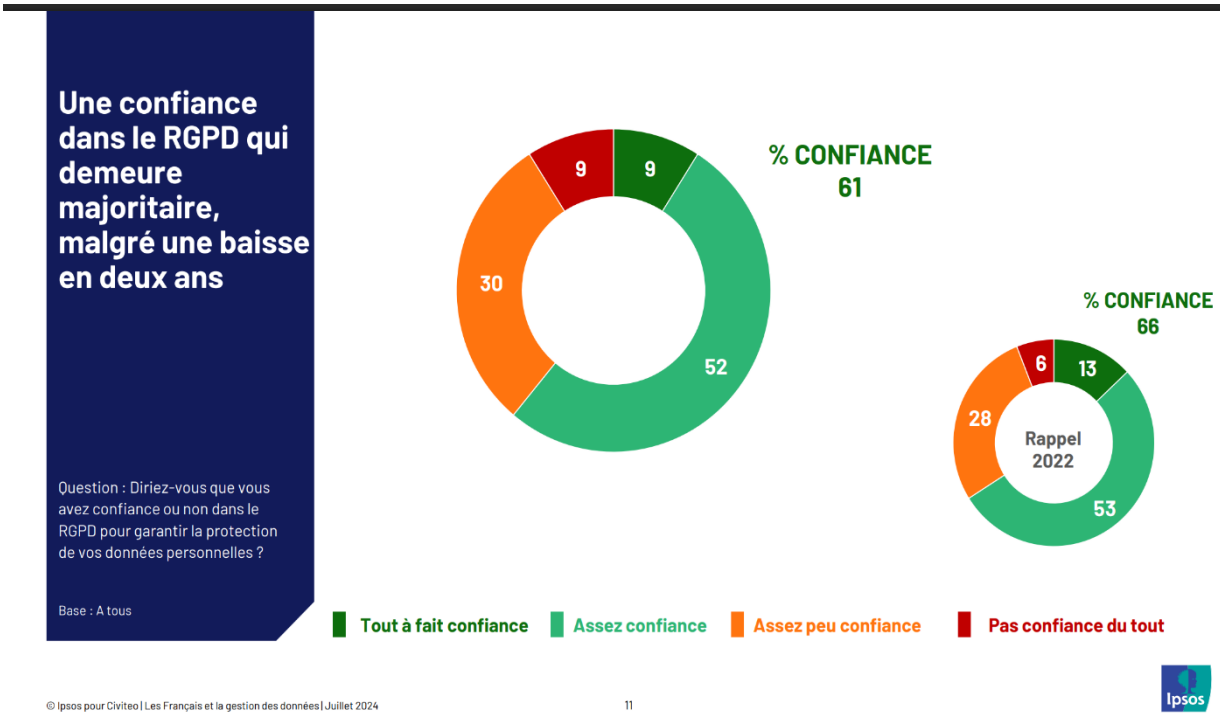


Figure 14 – Une confiance dans le RGPD qui demeure majoritaire, malgré une baisse en deux ans (source: Ipsos -Global Market Research and Public Opinion Specialist).

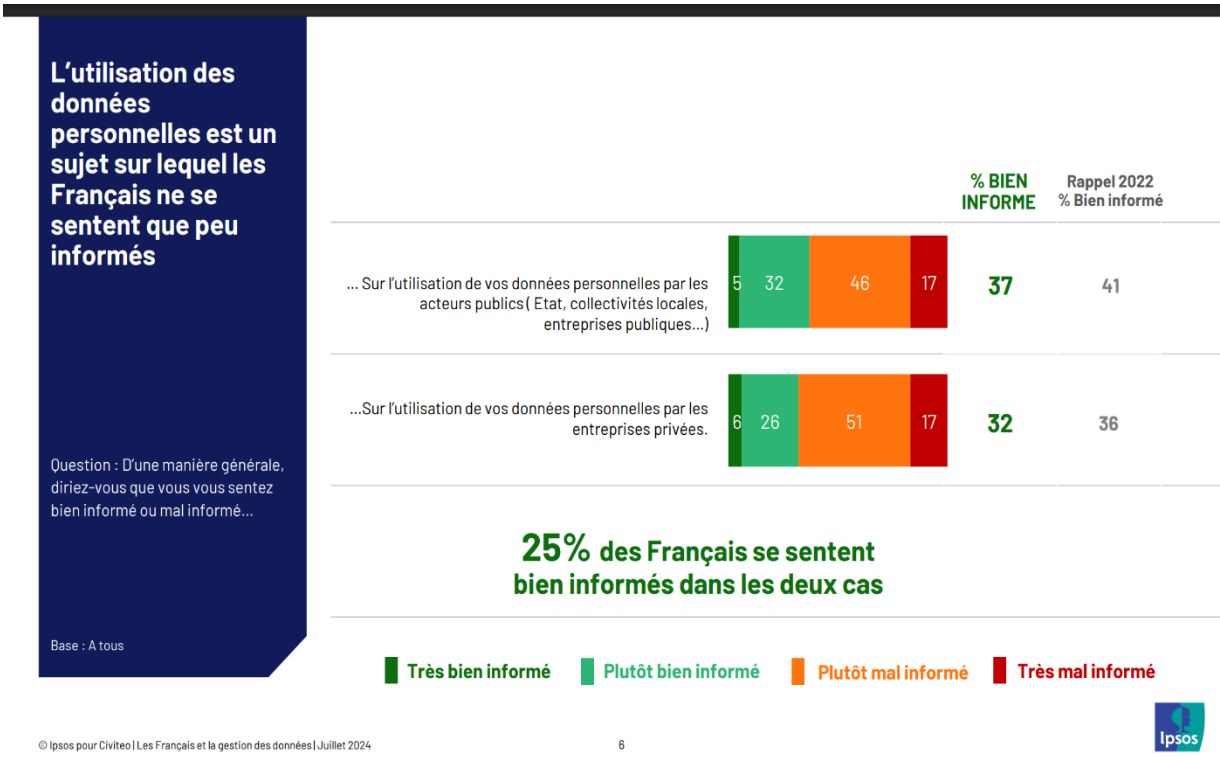


Figure 15 - L'utilisation des données personnelles est un sujet sur lequel les Français ne se sentent que peu informés (source: Ipsos -Global Market Research and Public Opinion Specialist).

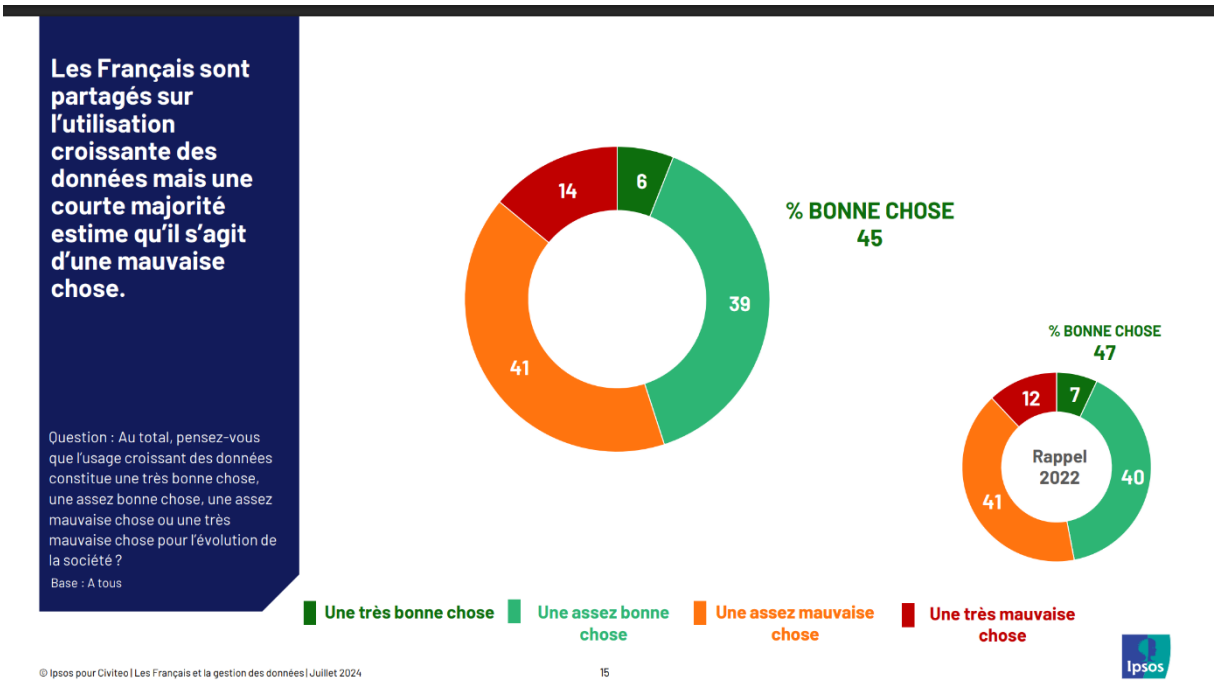


Figure 16 – Les Français sont partagés sur l'utilisation croissante des données mais une courte majorité estime qu'il s'agit d'une mauvaise chose. (source: Ipsos -Global Market Research and Public Opinion Specialist).

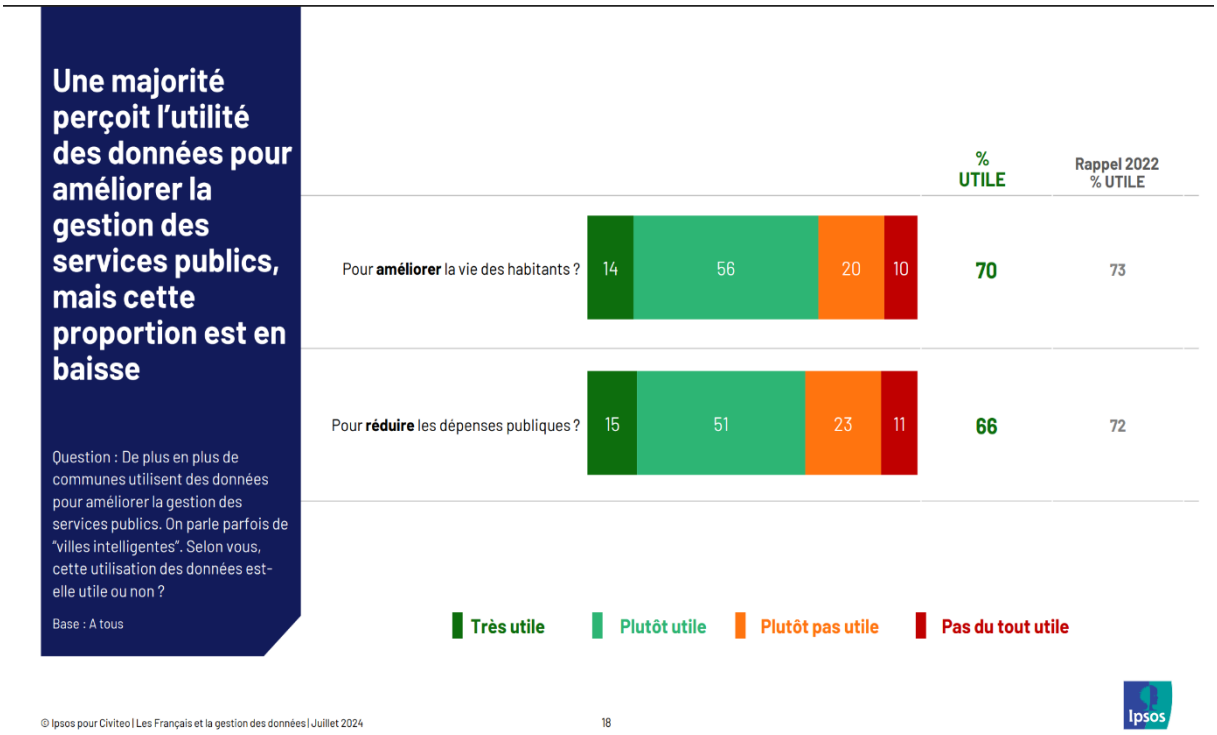


Figure 17 – Une majorité perçoit l'utilité des données pour améliorer la gestion des services publics, mais cette proportion est en baisse. (source: Ipsos -Global Market Research and Public Opinion Specialist).

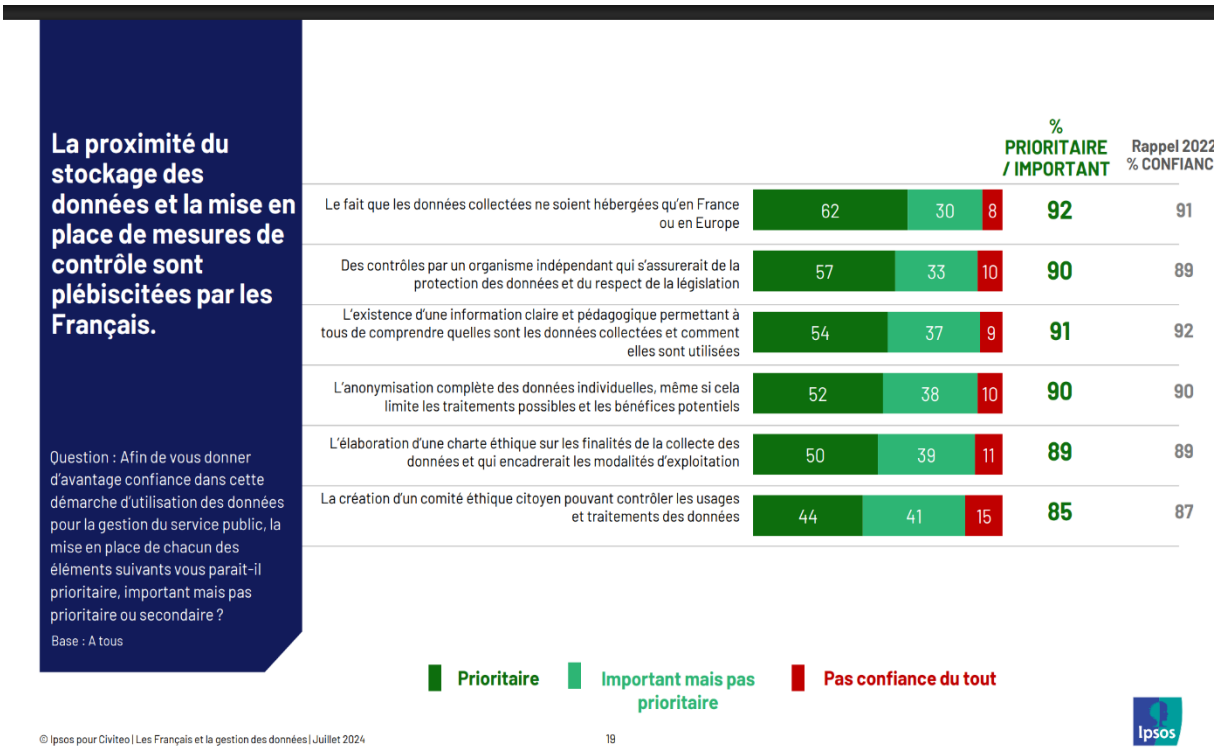


Figure 18 – La proximité du stockage des données et la mise en place de mesures de contrôle sont plébiscitées par les Français. (source: Ipsos -Global Market Research and Public Opinion Specialist).

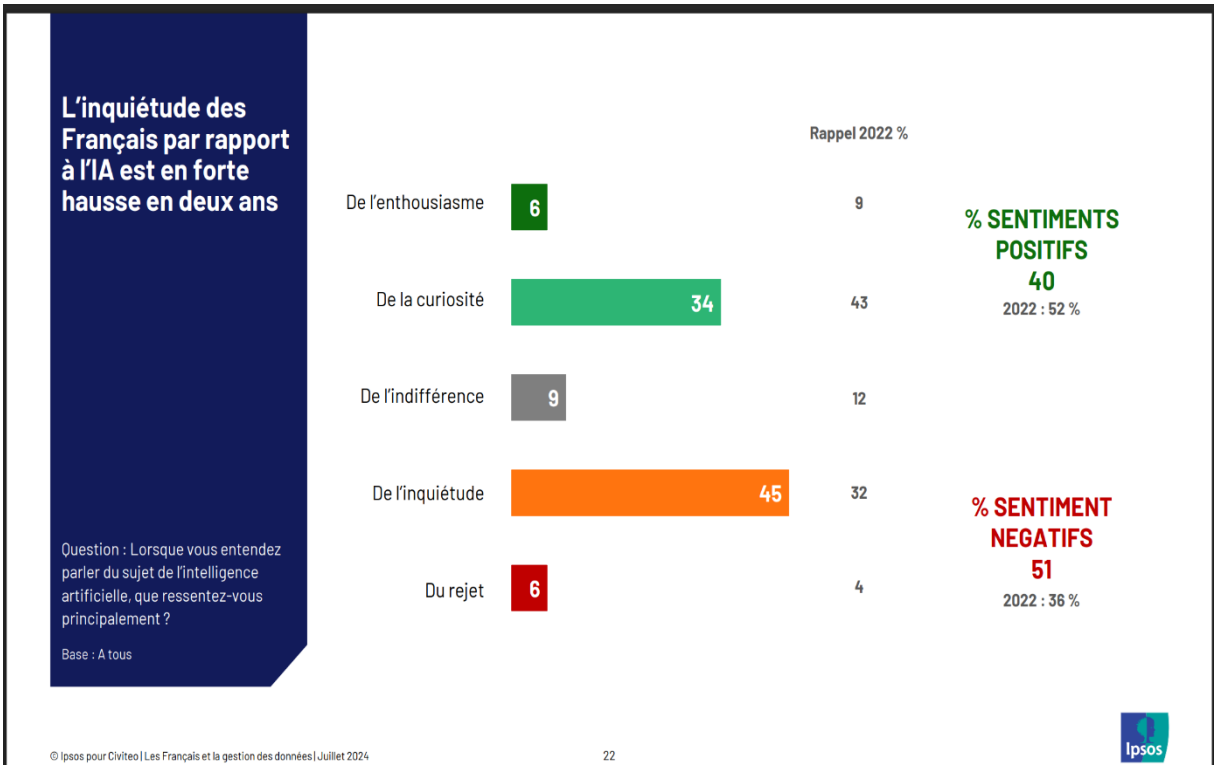


Figure 19 – L'inquiétude des Français par rapport à l'IA est en forte hausse en deux ans(source: Ipsos -Global Market Research and Public Opinion Specialist).

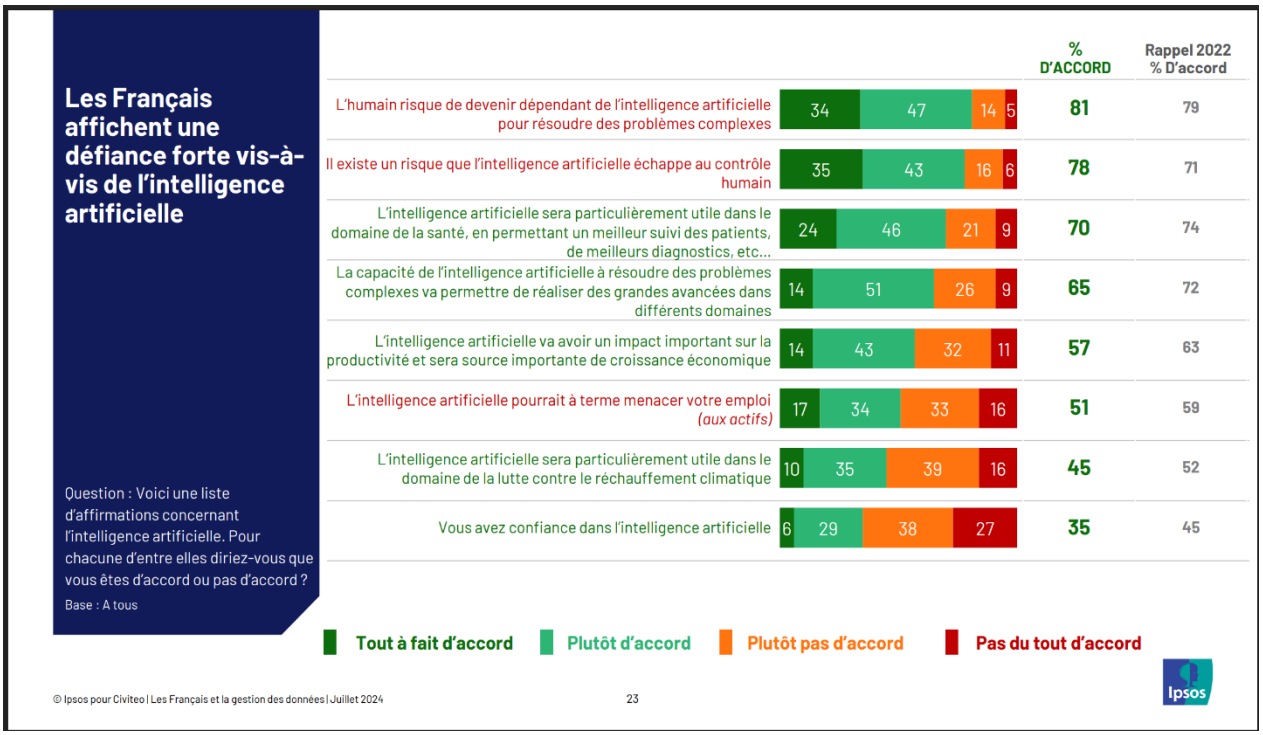


Figure 20 – Les Français affichent une défiance forte vis-à-vis de l'intelligence artificielle (source: Ipsos -Global Market Research and Public Opinion Specialist).

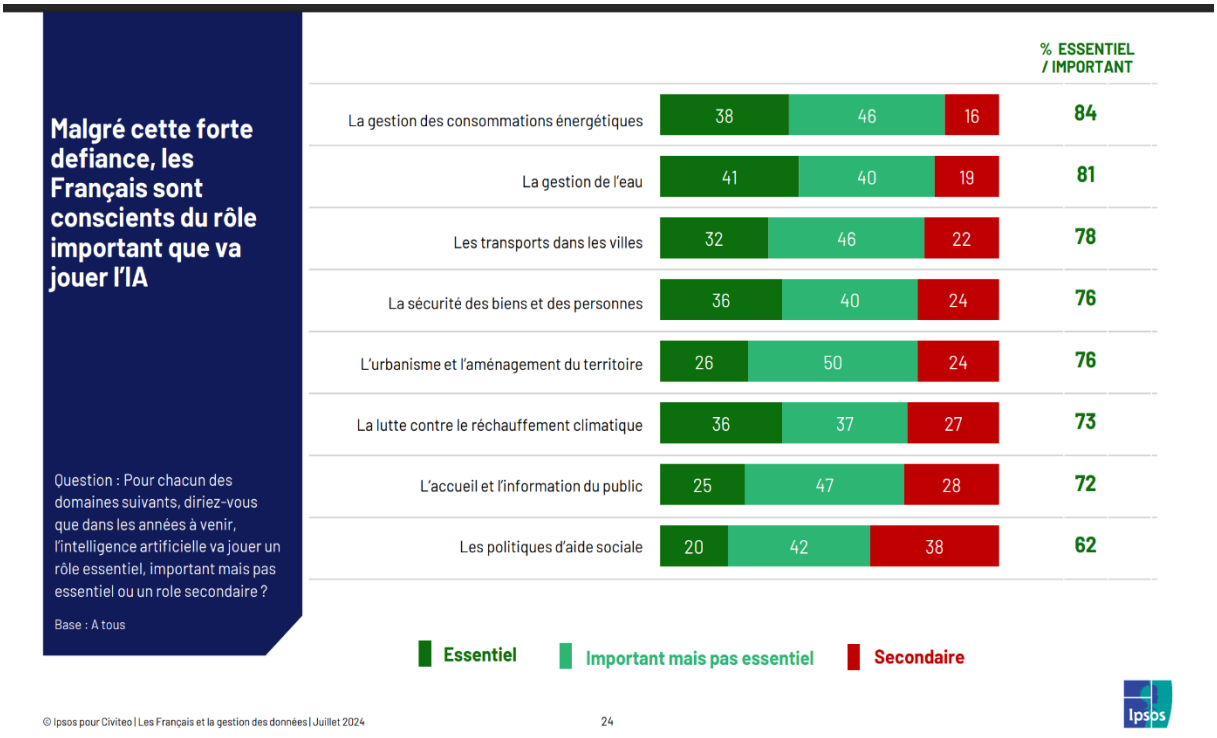


Figure 21 – Malgré cette forte défiance, les Français sont conscients du rôle important que va jouer l'IA (source: Ipsos -Global Market Research and Public Opinion Specialist).

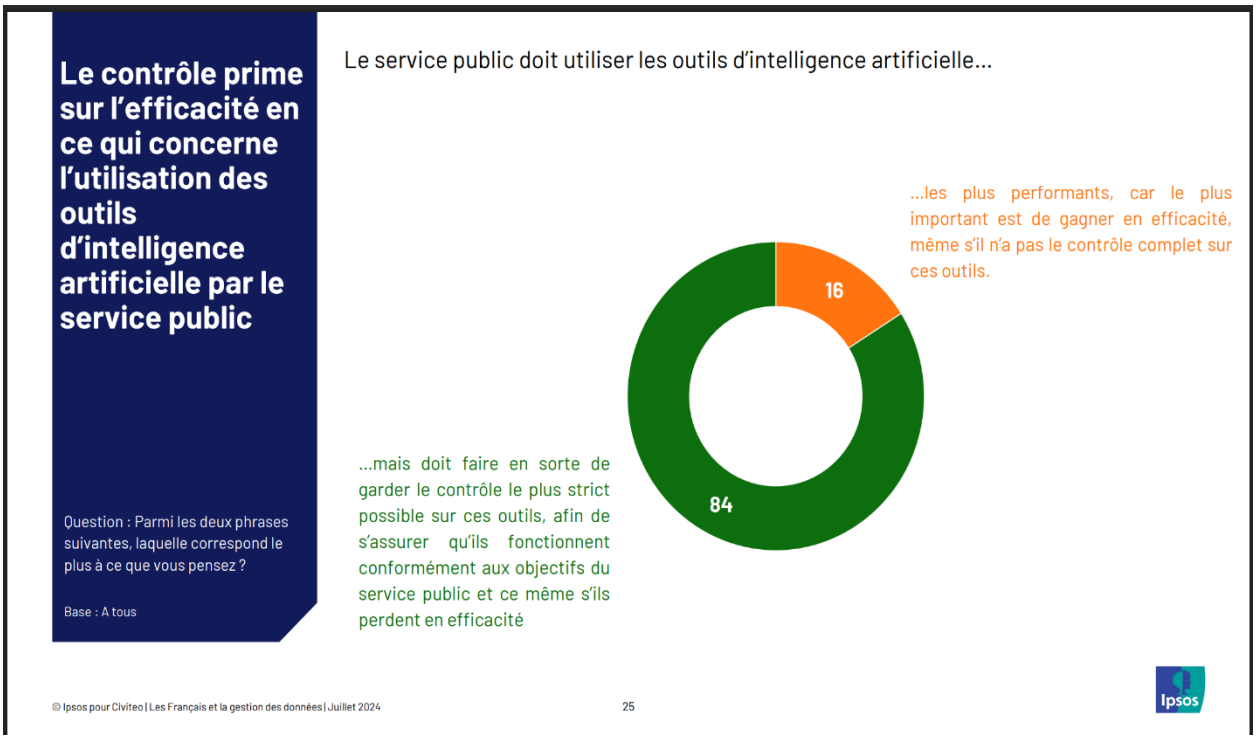


Figure 22 – Le contrôle prime sur l'efficacité en ce qui concerne l'utilisation des outils d'intelligence artificielle par le service public. (source: Ipsos -Global Market Research and Public Opinion Specialist).

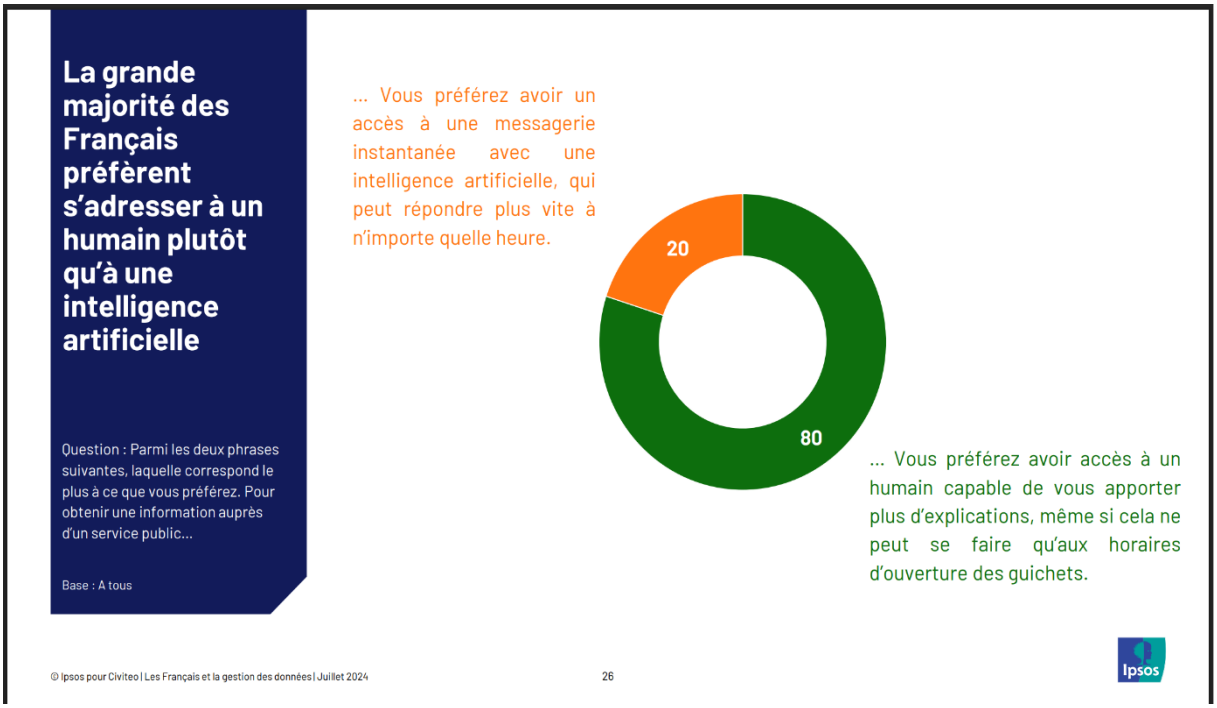


Figure 23 – La grande majorité des Français préfèrent s'adresser à un humain plutôt qu'à une intelligence artificielle. (source: Ipsos -Global Market Research and Public Opinion Specialist).

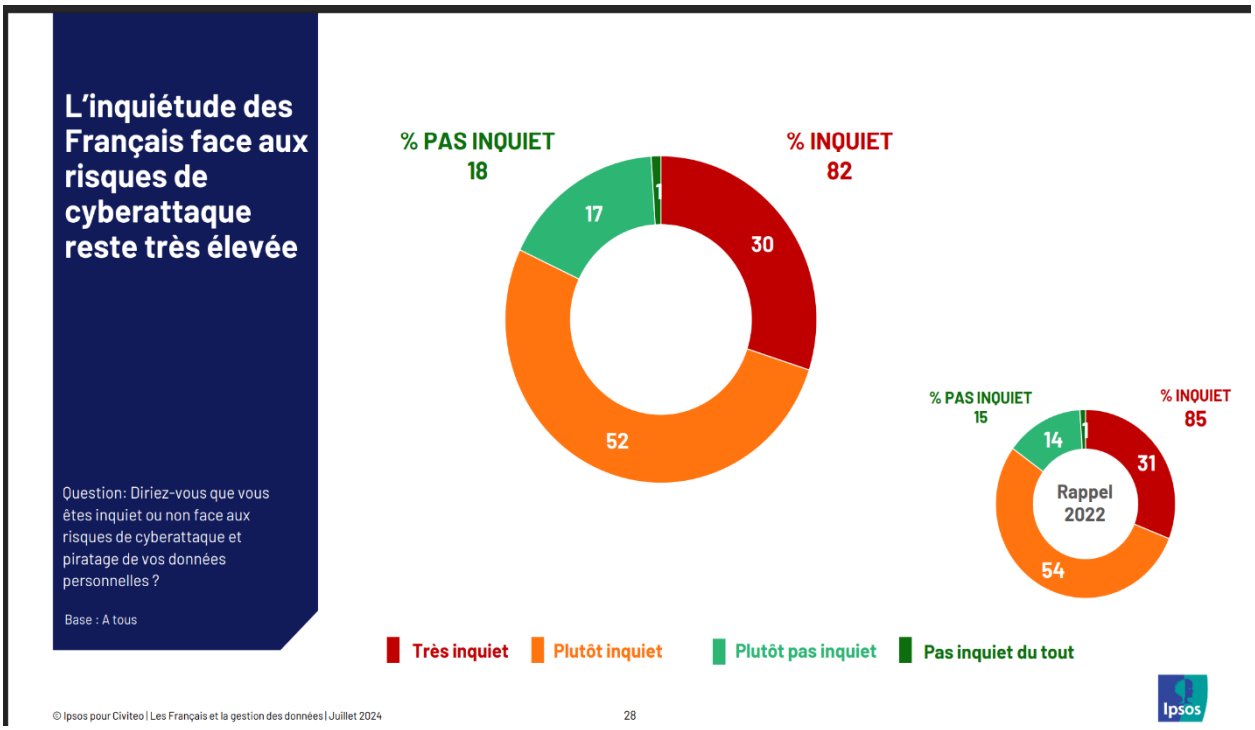


Figure 24 – L'inquiétude des Français face aux risques de cyberattaque reste très élevée. (source: Ipsos -Global Market Research and Public Opinion Specialist).

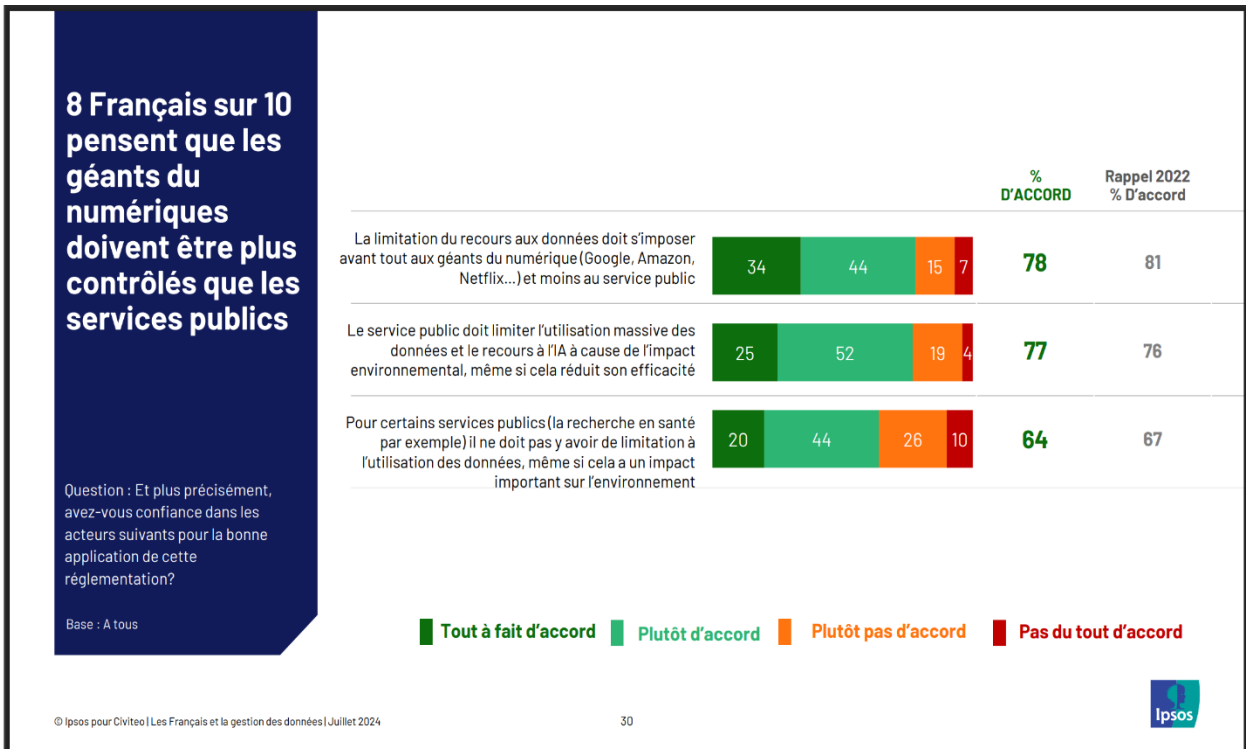


Figure 25 – 8 Français sur 10 pensent que les géants du numériques doivent être plus contrôlés que les services publics. (source: Ipsos -Global Market Research and Public Opinion Specialist).

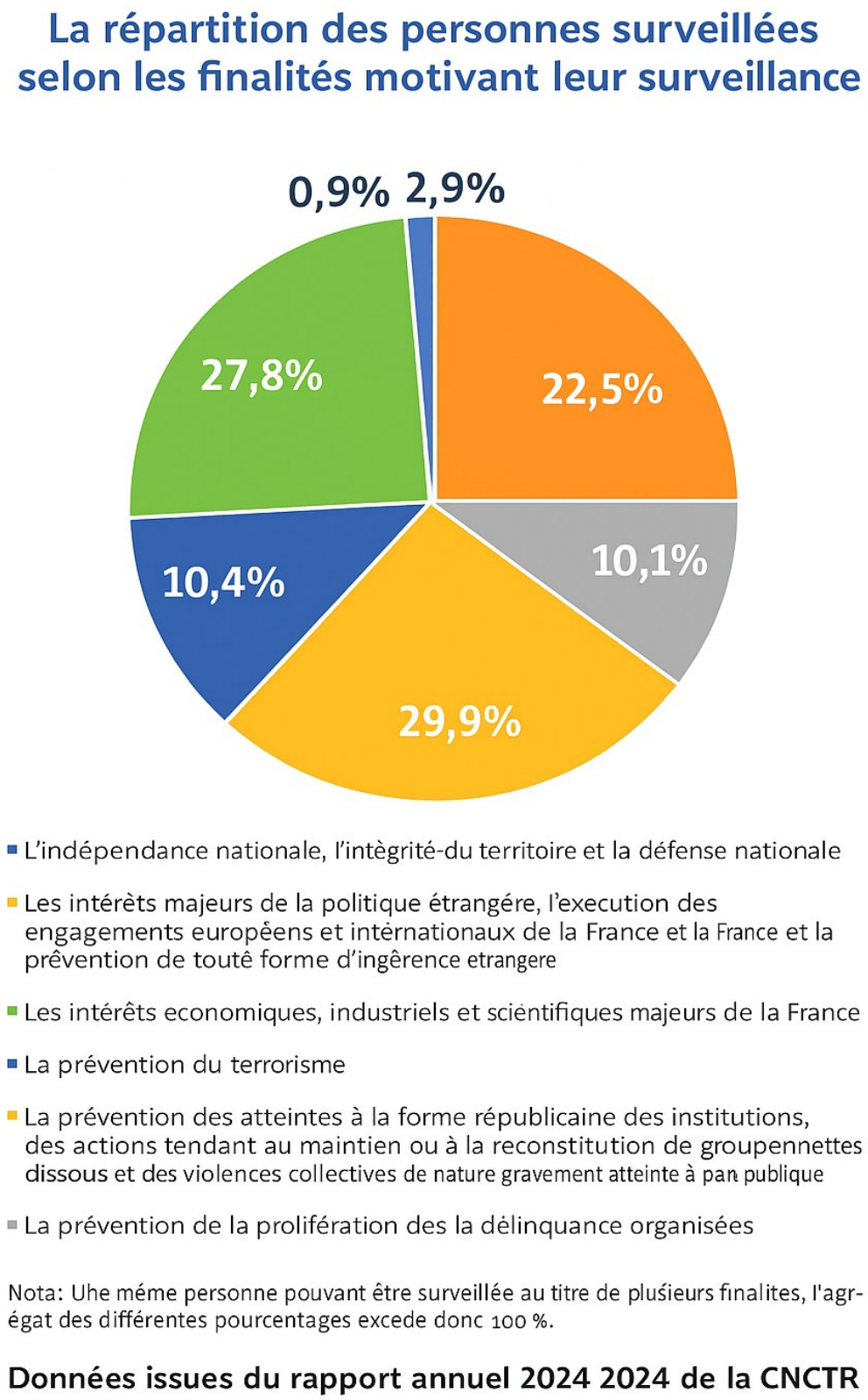
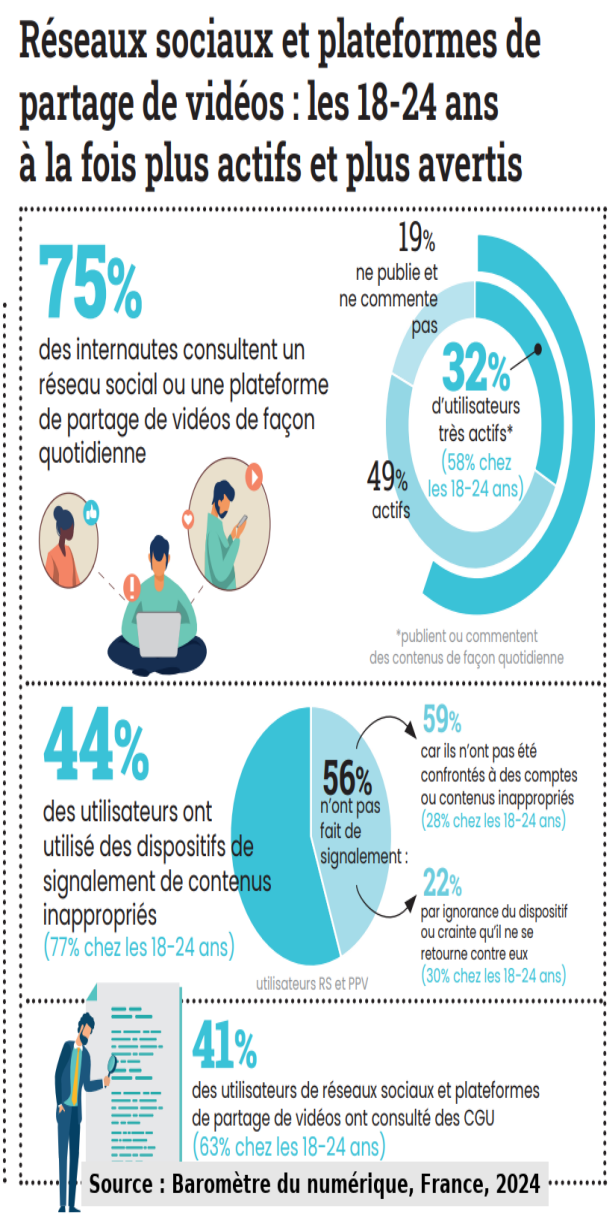
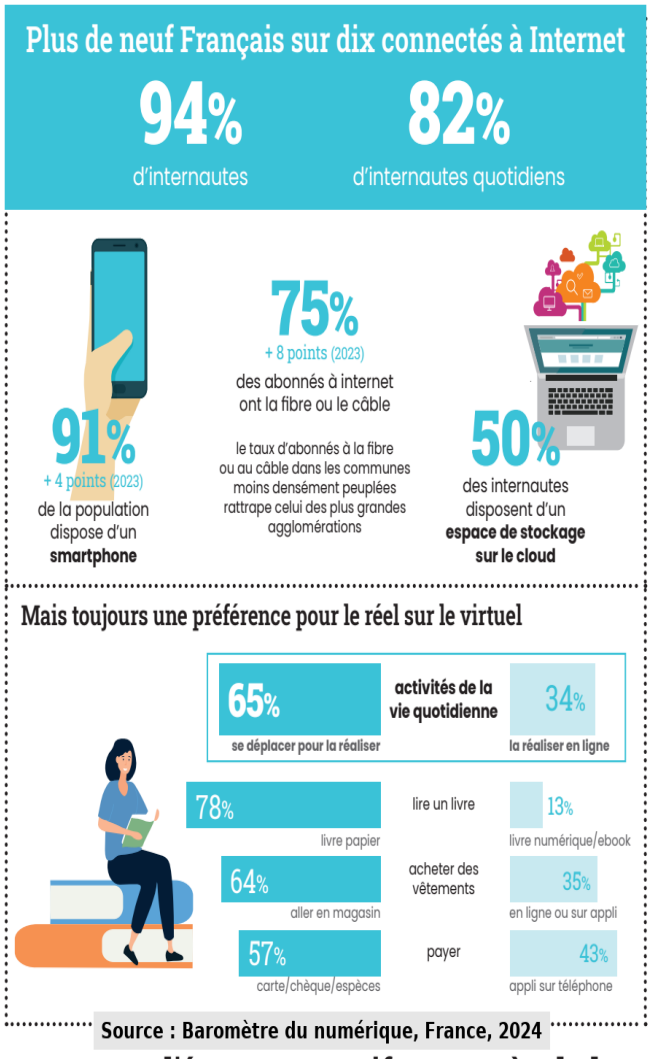


Figure 26 – La répartition des personnes surveillées selon les finalités motivant leur surveillance (source: CNCTR – rapport annuel, 2024)



Figure 27 – Les chiffres clés (CNCTR, 2024)





Figures 28 et 29 – Connexion numérique et comportements sur les réseaux sociaux (source: Baromètre du numérique, France, 2024).

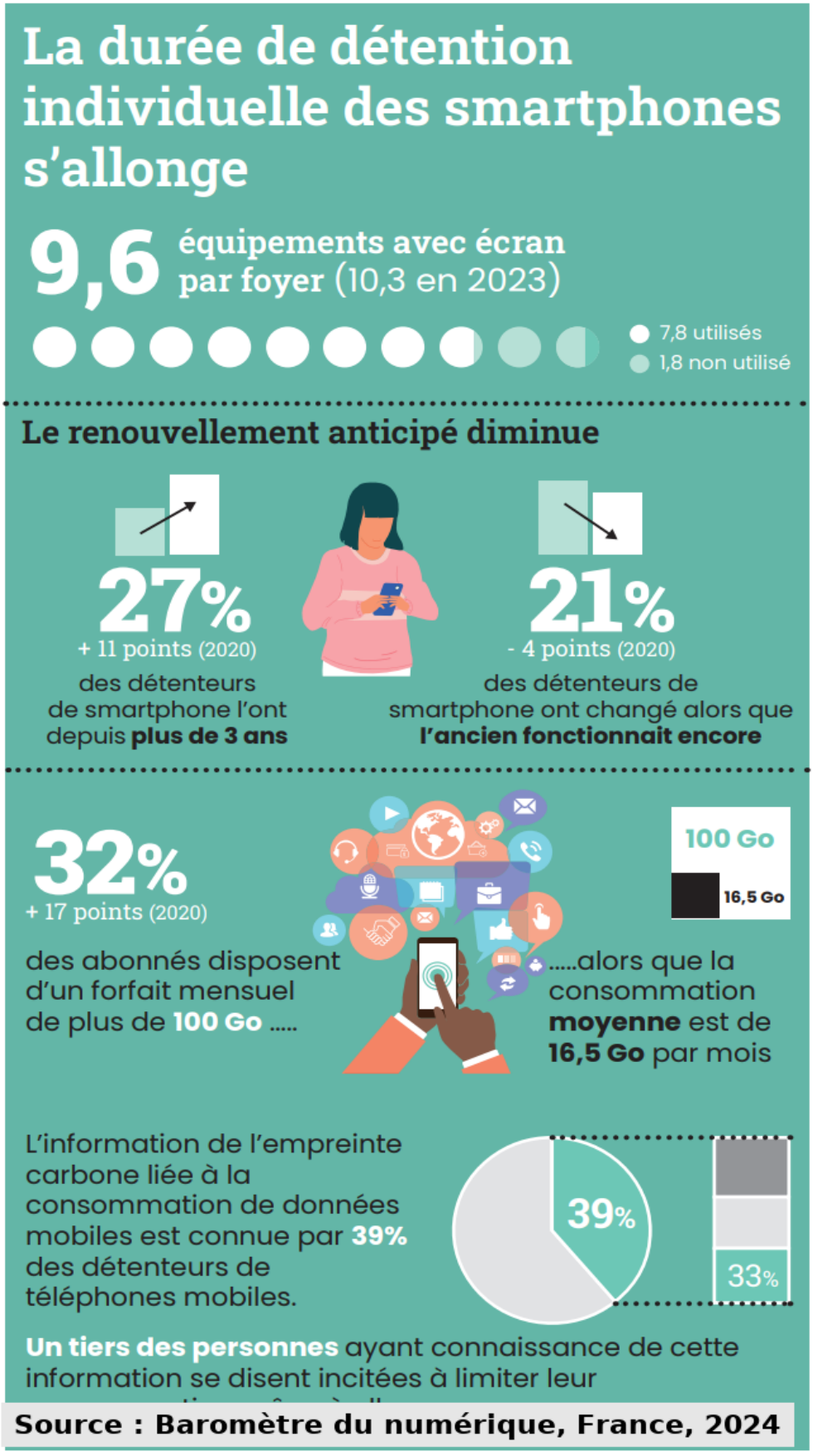


Figure 30 – La durée de détention individuelle des smartphones s'allonge. (source: Baromètre du numérique, France, 2024).

	2020	2021	2022	2023	2024	Évolution 2023 / 2024	Évolution 2020 / 2024
Accès aux données de connexion en temps différé (Identification d'abonnés ou recensement de numéros d'abonnement) (article L. 851-1 du code de la sécurité intérieure)	30 758	32 254	31 427	33 657	34 612	+ 2,8 %	+ 12,5 %
Accès aux données de connexion en temps différé (Autres demandes, dont celles de « factures détaillées ») (article L. 851-1 du code de la sécurité intérieure)	18 006	19 974	19 263	21 430	22 493	+ 5 %	+ 24,9 %
Accès aux données de connexion en temps réel (article L. 851-2 du code de la sécurité intérieure)	1 644	1 534	1 175	763	731	- 4,2 %	- 55,5 %

Données issues du rapport annuel 2024 de la CNCTR

Figura 31 – Accès aux données de connexion, 2020-2024 (source: CNCTR, rapport annuel, 2024).

	2023	2024	Évolution 2023 / 2024
Techniques de renseignement (hors données techniques de connexion)			
Avis rendus	39 815	41 778	4,9 %
Demandes de renseignements complémentaires	1 373 (soit 3,4 % du total)	1 609 (soit 3,9 % du total)	+ 17,2 % (0,5 pt)
Avis défavorables	496 (soit 1,2 % du total)	542 (soit 1,3 % du total)	+ 9,3 % (0,1 pt)
Données techniques de connexion			
Avis rendus	55 087	57 105	3,7 %
Demandes de renseignements complémentaires	1 424 (soit 2,6 % du total)	1 698 (soit 3 % du total)	+ 19,2 % (0,4 pt)
Avis défavorables	279 (soit 0,5 % du total)	261 (soit 0,5 % du total)	- 6,5 % (0 pt)
Toutes techniques de renseignements confondues			
Avis rendus	94 902	98 883	4,2 %
Demandes de renseignements complémentaires	2 797 (soit 2,9 % du total)	3 307 (soit 3,3 % du total)	+ 18,2 % (0,4 pt)
Avis défavorables	775	803	

Données issues du rapport annuel 2024 de la CNCTR

Figura 32 – Techniques de renseignement, 2023-2024. (source: CNCTR, rapport annuel, 2024).

	2020	2021	2022	2023	2024	Évolution 2023 / 2024	Évolution 2020 / 2024
Géolocalisations en temps réel (article L. 851-4 du code de la sécurité intérieure)	8 394	9 920	10 901	10 982	9 909	- 9,8 %	+ 18 %
Interceptions de sécurité via le GIC (I de l'article L. 852-1 du code de la sécurité intérieure)	12 891	12 736	12 798	13 021	14 316	+ 9,9 %	+ 11,1 %
Interceptions des communications par *IMSI catcher* (II de l'article L. 852-1 du code de la sécurité intérieure)	0	0	0	0	0	-	-
Interceptions de sécurité sur les réseaux exclusivement hertziens (article L. 852-2 du code de la sécurité intérieure)	0	3	5	10	5	- 50 %	-
Interceptions de correspondances émises ou reçues par la voie satellitaire (article L. 852-3 du code de la sécurité intérieure)	0	0	0	0	1	-	-
Localisations des personnes ou des objets (« Balisages ») (article L. 851-5 du code de la sécurité intérieure)	1 598	2 006	1 951	2 084	2 065	- 0,9 %	+ 29,2 %
Recueils de données de connexion par *IMSI catcher* (article L. 851-6 du code de la sécurité intérieure)	311	583	641	607	616	+ 1,5 %	+ 98,1 %
Captations de paroles prononcées à titre privé et captations d'images dans un lieu privé (article L. 853-1 du code de la sécurité intérieure)	1 564	2 138	3 314	3 802	3 912	+ 2,9 %	+ 150,1 %
Recueils et captations de données informatiques (article L. 853-2 du code de la sécurité intérieure)	2 418	3 758	4 260	4 493	5 715	+ 27,2 %	+ 136,4 %
Introductions dans des lieux privés (article L. 853-3 du code de la sécurité intérieure)	2 021	2 682	3 767	4 053	4 508	+ 11,2 %	+ 123,1 %
Ensemble des techniques de renseignement	79 605	87 588	89 502	94 902	98 883	+ 4,2 %	+ 24,3 %

Données issues du rapport annuel 2024 de la CNCTR

Figura 33 – Ensemble des techniques de renseignement, 2020-2024. (source: CNCTR, rapport annuel, 2024).

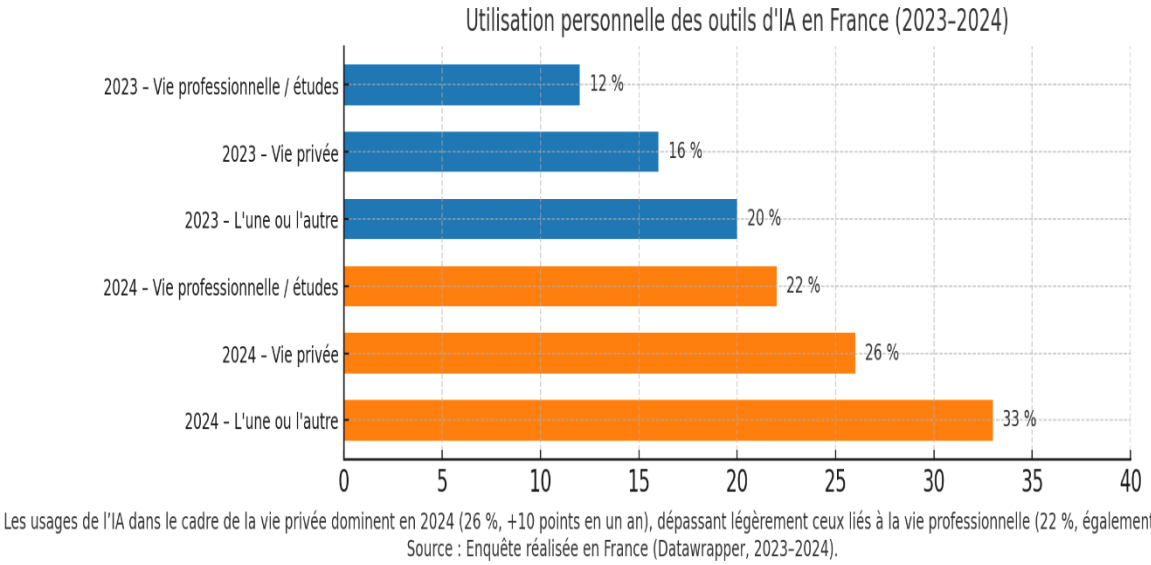


Figure 34 – Utilisation personnelle des outils d'IA en France (2023-2024) (source: Datawrapper, 2023-2024).

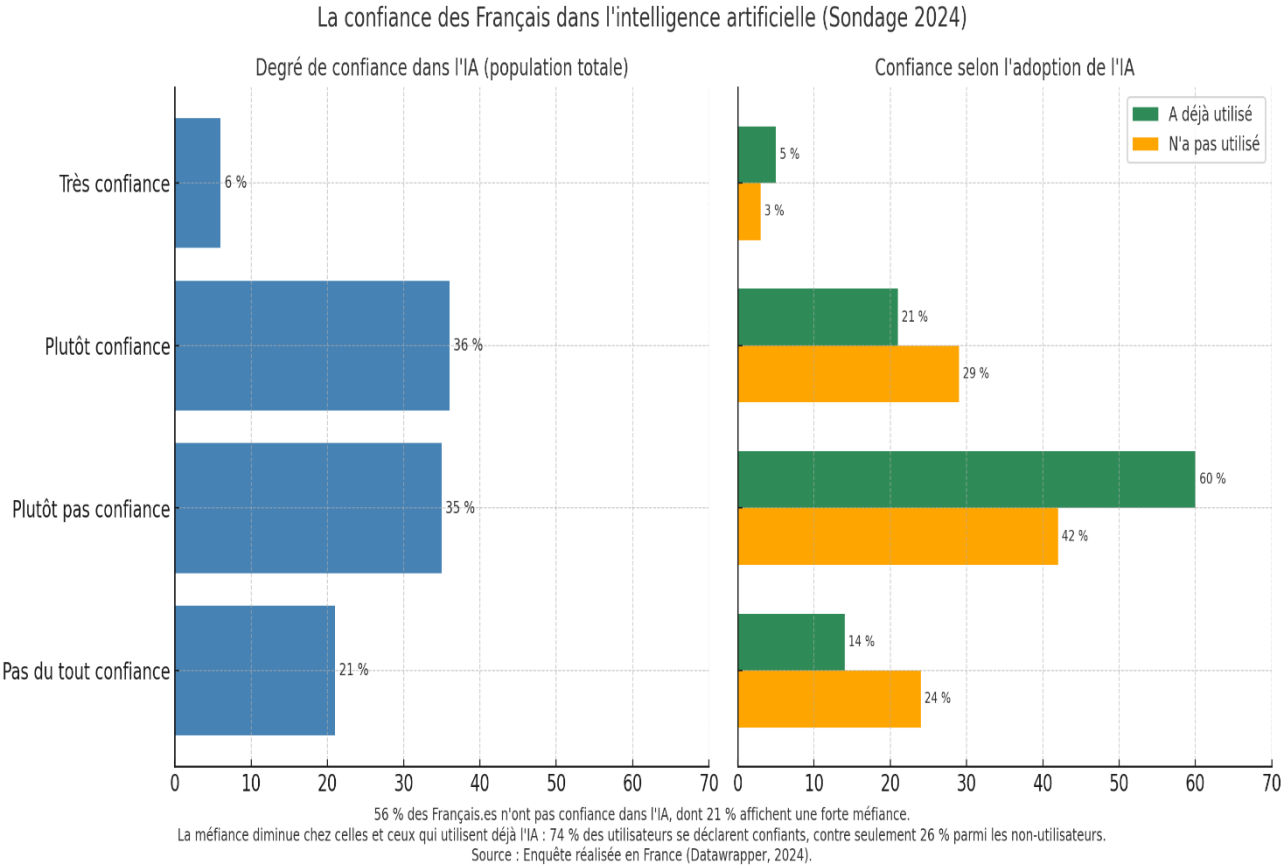


Figure 35 – La confiance des Français dans l'intelligence artificielle (Sondage 2024). (source: Datawrapper, 2023-2024).

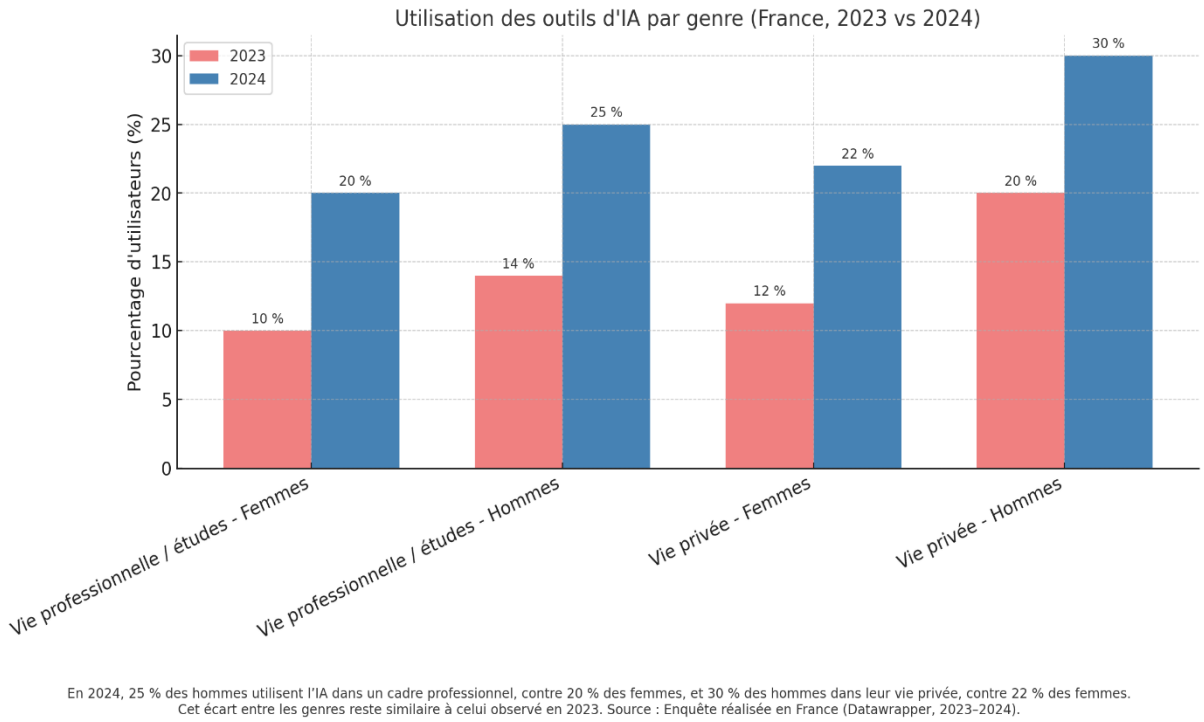


Figure 36 – Utilisation des outils d'IA par genre (France, 2023 vs 2024). (source: Datawrapper, 2023-2024).

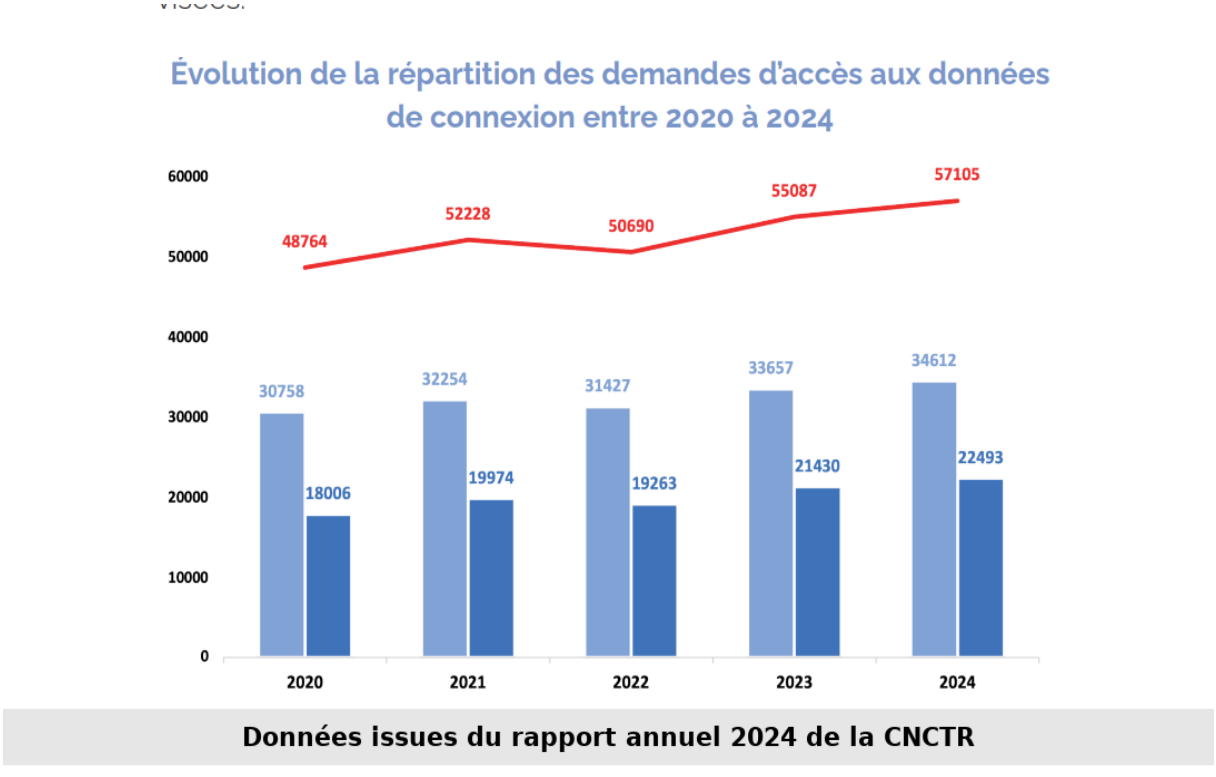


Figure 37 – Évolution de la répartition des demandes d'accès aux données de connexion (2020-2024) (source: CNCTR, rapport annuel, 2024).

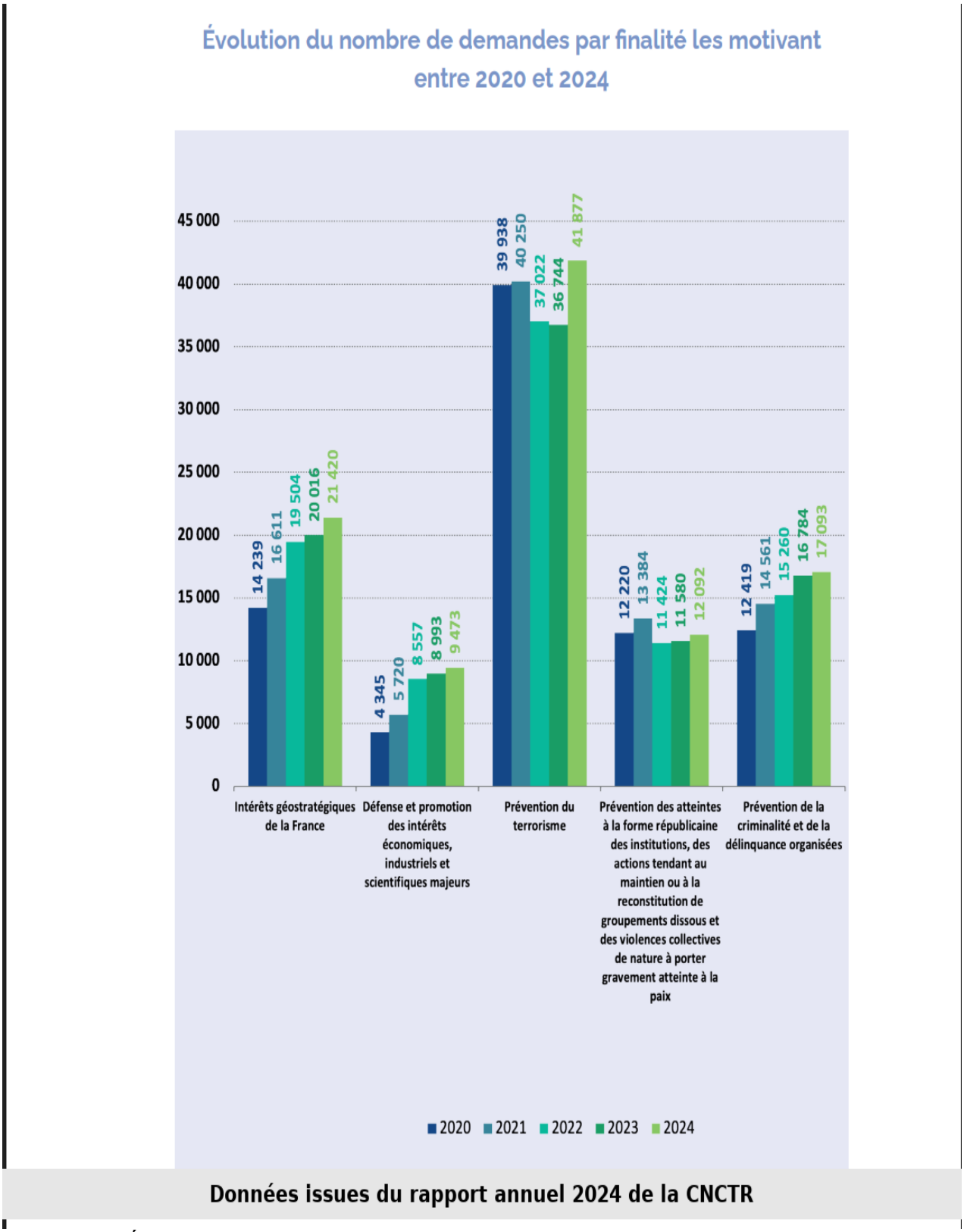


Figure 38 – Évolution du nombre de demandes par finalité les motivant (2020-2024). (source: CNCTR, rapport annuel, 2024).

Index alphabétiques

« cercle intime »,, 105
« Droit - liberté », 305
« Droit d'être laissé seul »,, 490
« écart de responsabilité », 414
« Noyau dur de la vie privée », 309
« siège professionnel », 263
Algorithmes
adaptant le droit, 655
aide pour justice pénale, 298
automatisés, 188, 298
deepfakes, 424
données collectées, 115, 116
influence, 145, 158
intelligence artificielle, 294, 411, 449, 501
méthode OCEAN, 146
reconnaissance faciale, 232
surveillance, 123, 653
Biens
de valeur économique, 488
historique, 97
personnels, 236, 282
Biométrie, 161
cadre juridique, 165
défis éthiques, 165, 233
évolution, 162
reconnaissance faciale, 231
risques, 164
utilisation, 163, 226, 228
Consentement, 149
du juge des droits et libertés, 528
éclairé, 140, 612
librement exprimé, 140
manquant d'ambiguïté, 141
numérique, 129
pour les enfants, 142
pour surveillance, 587, 605
présumé, 383
spécifique, 141
théoriquement illicite, 340
Cryptage, 131, 492
contre terrorisme, 501
controverse, 500, 511
données personnelles, 130, 186, 467
effets juridiques, 489
nécessité, 493, 499
pour protection, 168
pseudonymisation, 132
résolution européenne, 495
Cyber-harcèlement, 191
jurisprudence française, 308
Décryptage
adaptant le droit, 631
Backdoors, 510
Investigatory Powers Act, 506
jurisprudence française, 509
Deepfakes, 424
classification, 432
fins positives, 427
implication, 431
législation spécifique, 431, 432
Délit d'atteinte à la vie privée
Code pénal français, 272, 371
Code pénal roumain, 369, 371, 374, 491
contexte européen, 385
elements typiques, 337
éléments typiques, 337
enregistrement de conversations privées, 353
étude comparative France - Roumanie, 91, 369, 372
formes, 338, 339
hameçonnage, 169, 178
images intimes, 331
jurisprudence roumaine, 345
personne décédée, 372
personne morale, 373
tendances en France, 314
tendances en Roumanie, 349, 357
vengeance pornographique, 286
Délit de contrefaçon informatique, 264
Haute Cour, 268
Désinformation
développements juridiques, 443
en ligne, 444, 446
fausses nouvelles, 429
influence actuelle, 406, 429, 430, 450
première loi en France, 443
swarming et astroturfing, 449
Développement technologique
Big Data, 433
conséquences sociales et juridiques, 118, 120, 123
double numérique, 118
identification faciale, 313
nouvelles formes de surveillance, 158

réseaux sociaux, 117, 119, 155, 167, 171
sécurité des données, 129, 133, 155
technologies émergentes, 156
Développment technologique
identification faciale, 228
Diffamation
cas d'Emile Zola, 250
définition, 249
législation, 238
Distinction
anonymat en ligne - identité numérique, 460
conversation profesionnelle - conversation confidentielle, 280
diffamation - injurie, 249
internet de surface - internet deep, 466
lieu public -lieu privé, 282
protection des données - protection de la vie privée, 128
public - privé, 99, 326, 385, 520, 654
vie professionnelle - vie personnelle, 354
vraies - fausses informations, 426, 440
Données biométriques
clasification européene, 162
débat législatif, 645
en ligne, 234
FNAEG, 634
introduction dans les bulletins, 649
Loi de Bioéthique, 609
nécessité de réglementer, 232
RGPD, 226
système PARAFE, 162
zones grises, 227
Données génétiques
abus, 625
actes normatifs, 617, 626
caractère personnel, 227
directement au consommateur, 624
discrimination génétique en France, 613
discrimination génétique en Roumanie, 616
enquêtes pénales., 616
jurisprudence, 639
législation française, 629
législation roumaine, 627, 642
personne condamnée définitivement, 644
RGPD, 609
stockage, 637, 645
stockage en France, 636
stockage en Roumanie, 643
suppression, 638
utilisation, 620, 631
Droit
à l'image, 134, 285
à l'information, 283, 341
à l'inviolabilité du domicile,, 254
à l'oubli, 302
à l'oubli génétique, 610
à l'oubli numérique, 304
à la confidentialité, 302
à la confidentialité de la relation avocat-client, 248
à la liberté, 403, 588
à la liberté d'expression, 135, 250, 276
à la propriété, 243
à la protection de la réputation, 135
à l'anonymat, 452, 455
à l'oubli, 612
à sa propre image, 267
au privacy, 301
au respect de son corps, 623
au secret des données, 198
d'auteur, 209, 213
de l'agresseur, 582
du patient, 628
hybride, 128
international, 142, 149, 201, 373, 402, 577, 649
sur les données génétiques, 634
Droit à la vie privée, 111, 127, 207, 237, 306
biais de la technologie, 147
définition, 98
droit fondamental, 95
les défis du XXème siècle, 101
principes, 110
situations d'exclusion, 283
échange de données
entre pays, 543
génétiques, 640
équilibre
avantages technologiques - données personnelles, 157
biométrie - vie privée, 650
droit - humanité - technologie, 125
droit - technologie, 529
droit à la propriété - droit au respect du domicile, 244
droit à la protection des données - droit à la vie, 303
droit à la vie privée - le libre accès à internet, 305

droit de propriété - droit au respect du domicile, 243
droit européen - droit français, 494, 597
innovation - droits fondamentaux, 313
intention - conséquences, 316
interception - vie privée, 537
l'intérêt de la collectivité - vie privée, 385
métavers - vie réelle, 483
protection de la vie privée - progrès technologique, 400
protection des droits - lutter contre les délits, 349
sécurité - vie privée, 196, 202, 545
sécurité publique - les droits fondamentaux, 313
surveillance - vie privée, 582, 603
utilisation de la technologie - respect des règles de conduite légales, 296
vie privée - collecte des données génétiques, 638, 639, 642
vie privée - intérêt public, 315
vie privée - liberté d'expression, 291, 314
vie privée - protection de l'ordre public, 636
vie privée - sécurité - transparence, 124
vie privée - vie numérique, 143
vie privée - vie publique, 454
vie privée - violation du domicile, 323
vie privée de la victime - le but de la peine, 368
violation du domicile - definition du logement, 323, 324

Espionnage
auditif, 277, 287, 327
Code civil roumain, 103
Code pénal français - Code pénal roumain, 379, 383
controverse, 330, 331
de masse, 544
divulgation, 328
en réseau, 200
informatique, 386
moyens techniques, 321
peines, 292, 374
visuel, 281, 287, 321

Géolocalisation
consentement, 287
définition, 205
données statistiques, 554
législation, 289
mesure exceptionnelle, 284
réglementation juridique, 655

Initiatives législatives, 419
empreintes digitales et faciales dans les documents d'indentité, 649

Intelligence artificielle
« fossé de responsabilité », 415
définition, 145
impact sur la vie privée, 398
peines, 412
plan d'action de la CNIL, 422
réglementation, 420
responsabilité pénale, 408
types, 393
utilisation dans des activités criminelles, 401

Interceptions
administratives, 552
Allemagne, 535
applications WhatsApp, Telegram, Signal, 504
données statistiques, 554
historique, 534
illégale, 197
Livre blanc, 532
téléphoniques, 529, 533

Limitations
à la protection de la vie privée, 285, 304
du Code pénal roumain, 323
images de nature sexuelle, 284
interprétation et application, 350
personnalisation des espaces, 654

Loi ferenda
concernant la violation du domicile, 257

Mandat de perquisition
abusif, 525, 545
domiciliaire, 523
droit français, 525
droit roumain, 526

Menaces
à la sécurité nationale, 417, 536
cybercriminalité, 208
dark web/deep web, 464, 466
deepfakes, 426, 428
évolution de la technologie, 107, 297
manipulation de l'information, 442, 448
piratage moderne, 215
ransomware, 223
scamming, 181
surveillance non autorisée, 205
usurpation d'identité, 184, 186

Métavers, 478

bureau virtuel Interpol, 481
délits, 480, 487
données personnelles, 482, 487
perspectives juridiques, 485, 488
plateforme Second Life, 479
tendance actuelle, 479
Prison électronique, 583, 585
Sanctions
algorithmes d'intelligence artificielle, 295
chantage et menace, 307
dark web, 474, 475
désinformation, 444
discrimination, 615, 617
interception, 197
personnes morales, 252, 310
sphère sexuelle, 309, 332
Sans droit, 330
Secret professionnel
de l'avocat, 247
Surveillance, 538
bracelet électronique, 599, 604
cachée, 200
chinois, 230
considérations éthiques, 591
de la vie privée, 103
détention à domicile, 601
étatique, 158
gouvernementale, 515, 519
législation française, 596
législation roumaine, 592
loi G10, 536
Rapport GREVIO, 587
réglementation, 238
utilisation en Europe, 588
Vide juridique
deepfake, 433
délits générés par l'IA, 403, 410
interception des communications électroniques, 508
le vol en métavers, 487
les casinos du métavers, 481
pornographie de vengeance, 380
Vie privée
biais de réglementations, 123
CEDH, 105, 238
CNIL, 238
Code civil français, 102, 237
Code civil roumain, 103, 104
Code pénal français, 103, 112, 238, 276
Code pénal roumain, 104, 111, 256, 344
Constitution française, 112, 273
Constitution roumaine, 111
contexte de la technologie, 109, 111, 112, 119
Convention européenne, 344
datafication, 115
de la personne surveillée, 340
de la société, 263
définition, 98, 236, 271, 306, 319
dès la conception, 594
DUDH, 127
histoire, 97, 101
notion, 100, 108, 291, 376
perquisitions fiscales, 273
personne morale, 263
protection juridique, 114
réglementations, 294, 299, 305
sécurité des données, 130
Violation de domicile
CEDH, 240, 263
divorce, en France, 241
entrée autorisée, 242
notion de logement, 326, 359
par un agent public, en France, 241
par un agent public, en Roumanie, 256
par un particulier, en France, 243
protection en France, 239
protection en Roumanie, 254, 262
Violation du secret de correspondance, 244
autorité publique, 245
avocat - client, 246
divorce, 245
Violation du siège professionnel, 262
personne morale, 264

TABLES DES MATIÈRES

Sommaire **2**

Remerciements **2**

Abréviations **8**

Introduction générale **14**

Section 1. Objet d'étude: la vie privée dans le contexte de l'évolution numérique ***15***
§1. Notions essentielles 16
§2. Transformation de l'identité en un code numérique 19
§3. Le droit pénal face à l'*homo numericus* 22

Section 2. Conceptualisation: le nouveau rapport entre ordre public et vie privée ***25***
§1. L'ordre public, une notion ambiguë et imprévisible 25
§2. Controverses. Une notion élastique et déroutante 28

Section 3. Définition et évolution des algorithmes. Détermination du rôle par rapport à la vie privée ***30***
§1. La première expérience européenne 30
A. Problème d'actualité: l'identification biométrique de la population 32
B. La réponse de la société à la surveillance de l'État 33
C. Les algorithmes, à droite du juge 35
§2. La naissance de la société numérique, de « zéro » à « un » 36
A. Les racines des concepts courants d'aujourd'hui 37
B. Identification et protection binaire 39

Section 4. Identification des thèmes d'intérêt pour la recherche ***40***
§1. Obstacles à l'obtention et au maintien de l'anonymat 41
§2. Le droit à l'oubli: entre mémoire collective et protection individuelle 43
A. Mémoire hybride: humaine, numérique, algorithmique 44
B. Mémoire algorithmique et réécriture du passé 46
§3. La transformation conceptuelle du public et du privé 50

Section 5. Les limites des transformations contemporaines du droit pénal à l'ère numérique ***53***
§1. Interrogations du présent en droit pénal 53
§2. L'obésité du droit et le contrôle de la production législative 55
A. Prédisposition à une réglementation excessive 56
B. La transposition des directives européennes, un problème typiquement français? 58
C. Vers une nouvelle ère de codification, dans un contexte instable 59

Section 6. Repères conceptuels dans la reconfiguration de l'atteinte à la vie privée : éléments clés de la recherche ***61***
§1. Consentement de la victime 62
A. Interventions critiquables des tribunaux 64
B. Vision différente quant à la définition des termes 66
C. Interdiction de la commercialisation juridique du consentement 67
D. Le code pénal roumain, en matière de consentement. Vision comparative 71

E. Consentement dans le cas d'un acte médical 74
F. Situation particulière : consentement vs circonstance aggravante 75
G. La valeur du consentement dans l'espace numérique. Protection renforcée pour les mineurs 76
§2.« Lieu privé » dans l'architecture du droit à la vie privée. Ambiguïtés dans la définition 78
A. Termes clés du Code pénal français : à titre privé ou confidentiel et « lieu privé ». 79
B. Analyse conceptuelle : le véhicule est un « lieu privé ou public ». Vision différente 81

Section 7. Entre la reconnaissance de la personnalité juridique et la rédaction du droit. Les limites de la recherche 82
§1. Les algorithmes donnent l'impression d'avoir leur propre identité 82
A. La voie est-elle ouverte à la reconnaissance de la personnalité juridique pour l'intelligence artificielle ? 83
§2. L'intelligence artificielle, législateur potentiel ? Les limites des débats doctrinaux 85
A. L'intelligence artificielle risque-t-elle d'écrire elle-même le droit ? 86
B. « Un Carbonnier non publié sur internet ne vaut plus grand-chose » 89
a). Justice prédictive, les algorithmes collectent-ils des données pour écrire le droit ?91

Conclusion : homo algoritmus, construit exclusivement à partir de données fournies volontairement 92

Section 8. Plan de thèse 94
§1. Plan d'études 94
§2. Motif de la réalisation d'une étude comparative France - Roumanie 95
§3. Méthodes de recherche utilisées pour l'élaboration de la thèse 96

Première partie

La protection de la vie privée à l'ère numérique

Titre I. Le fondement juridique de la protection de la vie privée 98

Chapitre 1 L'effet des évolutions technologiques sur la vie privée 99

Section 1. D'un concept philosophique à un droit fondamental 99
§1. Premières approches philosophiques du concept 99
A. La vie privée n'est pas une invention de la modernité 100
B. Évolution du concept de vie privée. Définition 102
§2. Panoptique et coercition psychique 107

Section 2. Attributs de l'exercice du droit à la vie privée au moyen de la technologie 112
§1. Signes de l'émergence du droit à la vie privée dans le contexte de la technologie 114
A. Naissance du droit à la vie privée dans un contexte numérique 116
a). Impact de l'évolution de la technologie sur la vie privée 118
b). Protection juridique de la vie privée versus évolution de l'ordinateur 121
c). Convention pour la protection des données personnelles 122
d). Datafication, les algorithmes influencent de manière décisive la liberté de choix 123
e). La collecte de données personnelles influence le comportement humain 125
f). Les réseaux sociaux ont créé une extension virtuelle du soi 126
g). « Double numérique » – la vie privée devient une ressource exploitable 127

§2. Effet des changements technologiques sur la vie privée 128
A. Conséquences sociales et juridiques du développement technologique 130
a). Surveillance omniprésente - concurrence entre l'État et les entreprises 130
b). « Société d'exposition » - les utilisateurs acceptent volontairement le contrôle 132
c). Nécessité d'un équilibre entre la protection de la vie privée, la sécurité et la transparence 134
d). Redéfinir la relation entre le droit, l'humanité et la technologie 136
e). Collecte de données sur les réseaux sociaux, réglementation inégale 137
B. Principes de l'exercice du droit à la vie privée grâce à la technologie 139
a). Sécurité des données 142
b). Confidentialité 144
c). Le cryptage, une mesure essentielle pour la protection des données 146
d). Pseudonymisation 147
e). Disponibilité et intégrité des données 149
f). Le contrôle, l'information et l'autonomie relatifs aux données 151
g). Droit à l'image et la protection des photos 152
h). Droit à la protection de la réputation d'une personne 153
i). Confidentialité des communications électroniques 154
C. Les traits essentiels du consentement à l'ère numérique 157
a). Consentement librement exprimé 158
b). Consentement éclairé 158
c). Consentement spécifique 159
d). Consentement manquant d'ambiguïté 159
e). Consentement donné pour le compte des enfants 160
Conclusions du Chapitre 1 161

Chapitre 2 Les ingérences dans le droit à la vie privée dans le contexte de l'évolution numérique 162

Section 1. La surveillance continue mène-t-elle à l'autocontrôle et à la discipline? 163
§1. A.I. - Intelligence artificielle 163
A. Web 2.0 et web 3.0. 166
a). L'internet des gens 166
b). Internet des objets 167
c). Influence sur la vie privée 167
B. Homo numericus – mutation identitaire de la personne physique ou sujet de droit? 168
a). Homo numericus – sujet juridique hybride 170
§2. Sécurité des données et sensibilisation à la protection de la vie privée 174
A. Technologies émergentes et défis pour la protection de la vie privée 175
a). Big Brother contre le besoin de likes et de partages 177
b). Nouvelles formes de surveillance, collaboration entre les géants de l'informatique et le gouvernement 178
c). Foucault - Surveiller et punir 180
d). Biométrie et protection de l'identité 181
e). Blockchain et identité numérique 185
f). Réseaux sociaux et protection de l'identité 186
B. Protection de l'identité numérique 191
a). Usurpation d'identité numérique en France 192
b). Protection des informations personnelles contenues dans les fichiers ou stockées sur l'ordinateur 193
C. Techniques de tromperie en ligne 197

a). Délits d'hameçonnage 197
b). Le scamming 200
c). Le spoofing 202
d). Ad stacking (la fraude au clic) 206
e). Cyber-harcèlement et harcèlement en ligne 211

Section 2. Atteintes contemporaines à la vie privée : interception, surveillance et biométrie 214

§1. Interception illégale des communications 214
A. Analyse du délit d'« interception illégale d'une transmission de données informatiques » 217
a). Éléments constitutifs du délit 218
b). Interventions de la CEDH en lien avec l'interception de conversations. 221
B. Surveillance non autorisée et géolocalisation 224
C. Violation de la cybersécurité et piratage 228
a). Définition et classification des atteintes à la cybersécurité 228
b). Le piratage devient une méthode invisible d'exercice du pouvoir 234
§2. Approche juridique des atteintes à la cybersécurité : analyse des affaires et réglementations internationales 238
A. Vulnérabilités des systèmes d'information mondiaux 240
a). Kevin Mitnick, le hacker le plus recherché au monde 241
b). Convention de Budapest sur la cybercriminalité 242
c).Ransomware : taxonomie et impact 243
B. Technologies de reconnaissance et d'authentification biométriques 245
a). Données biométriques, zone grise aux États-Unis 247
b). La reconnaissance faciale augmente la sécurité dans l'espace public 247
c). Les aéroports annoncent l'exclusion de l'identification des passagers sur la base de documents 248
d). Critiques de l'utilisation par le gouvernement chinois de la reconnaissance faciale 249
e). Technologies de reconnaissance faciale et acceptation de la surveillance 251
f). Nécessité de réglementer les technologies biométriques 252
g). Éthique et avenir de la biométrie 252
C.Dispositifs IoT (Internet of Things) et collecte de données personnelles 253
Conclusions du Chapitre 2 255
Conclusions du Titre 1 257

Titre II. Les infractions classiques destinées à assurer la protection de la vie privée en roumanie et en france 258

Chapitre 1. Les réglementations traditionnelles relatives au domicile et à la correspondance 258

Section 1. Les bases juridiques propres au droit français 259

§1. Les infractions connexes et complémentaires à la protection de la vie privée 260
A. Violation de domicile 260
a). Violation de domicile lors du divorce 262
b). Violation de domicile par un agent public 263
c). Violation de domicile par un particulier (personne physique ou morale) 264
d). Droit de propriété versus droit au respect du domicile 265
B. Violation du secret de la correspondance 265

a). Violation du secret de la correspondance par une autorité publique 266
b). Violation du secret de correspondance lors d'un divorce 266
c). Violation du secret de la correspondance avocat - client 267
d). Attaque contre le secret professionnel 268
C. Diffamation et insultes 270
D. Article 226-19 du Code pénal français (conservation illicite de données) 272

Section 2. Les bases juridiques propres au droit roumain 274
§1. Les infractions connexes et complémentaires à la protection de la vie privée 275
A. Violation de domicile 275
a). Nouvelles méthodes de violation de domicile dans le contexte du développement technologique. 280
B. Violation du siège professionnel 283
§2. Contrefaçon informatique dans le contexte du délit d'atteinte à la vie privée 285
A. Saisie non autorisée de données pour créer un compte sur les réseaux sociaux 289
B. Falsification de la manifestation de la volonté du véritable détenteur 289
Conclusion du Chapitre 1 290

Chapitre 2 L'analyse de l'infraction d'atteinte à la vie privée 292

Section 1. Cadre juridique d'incrimination de l'atteinte à la vie privée en droit pénal français 293
§1. Modalité de commission du délit d'atteinte à la vie privée dans le domaine du droit français 297
A. Espionnage auditif 299
a). Caractère privé ou confidentiel 299
b). Capture, enregistrement et transmission 300
c). Cause justificative 302
B. Espionnage visuel 303
a). Caractère privé et confidentiel 303
b). Capture, enregistrement et transmission 304
c). Situations dans lesquelles le droit à la vie privée n'est pas violé 305
d). Droit à l'image 307
e). Limites de la loi. Forme aggravée 307
f). Nécessité du consentement 309
C. Géolocalisation 310
D. Droit à la vie privée versus droit à la liberté d'expression 313
§2. Autres réglementations juridiques étroitement liées à la vie privée 314
A. Fabrication, installation et promotion de dispositifs d'espionnage 314
B. Réglementation du délit d'atteinte à la vie privée par deepfake 316
C. Le régime juridique du délit d'atteinte à la vie privée envisagé sous l'angle de la privacy 321
a). Droit à la protection de la confidentialité de la correspondance par courriel 322
b). Droit à la protection des données personnelles et droit à l'oubli 324
c). Réglementation du délit d'atteinte à la vie privée par le biais du cyber-harcèlement 326
§3. SANCTIONS PÉNALES 329
A. Peines aggravantes dans le Code pénal français 330
B. Peines complémentaires dans le Code pénal français 331
C. Criminalisation de la tentative 332
§4. Jurisprudence sur la protection de la vie privée en France 334

Section 2. Cadre juridique d'incrimination de l'atteinte à la vie privée en droit pénal roumain 340

A. Éléments de typicité de l'infraction d'atteinte à la vie privée 340
Objet juridique 340
Objet matériel 341
Sujets du délit 341
Côté objectif 342
a). Espionnage visuel 343
b). Haute Cour de cassation et de justice : difficultés à définir *le logement* 345
c). Protection pénale de la vie privée dans les espaces publics 348
d). Espionnage auditif 349
e). Divulgation de sons, de conversations et d'images 350
f). Controverse : est-il important que les images soient obtenues avec ou sans droit ? 351
B. Réglementation récente dans le Code pénal : divulgation d'images intimes 353
a). Définition pénale de *l'image intime* 354
b). Conséquences immédiates : souffrance mentale 357
C. Installation de moyens techniques d'enregistrement audio-vidéo 357
a). Éléments typiques des variantes du délit d`atteinte à la vie privée 358
D. Causes particulières atypiques de délits 360
§2. Analyse de la jurisprudence roumaine: 2014 – 2024 364
A.Nombre d'affaires d'atteinte à la vie privée, en augmentation 366
a). Adaptation de la jurisprudence aux défis de l'évolution technologique 367
b). Clémence dans la punition du délit d'atteinte à la vie privée 367
B. Les controverses jurisprudentielles relatives au délit d'atteinte à la vie privée 370
a). Conditions objectives de réalisation du délit - pratique de la Haute Cour de Cassation 371
b). Peines en régime de détention uniquement pour les récidivistes et les délits concurrents 376
c). En général, la jurisprudence établit un régime de sanction clément 378
d). Motivation des jugements d'acquittement prononcés au cours des dix dernières années 379
e). Sept jugements reportant l'application de la peine en dix ans 385
f). Retrait de la plainte enlève la nature pénale de l'acte 388
g). Équilibre entre les intérêts de la victime et le but de la peine 388
Section 3. Vue comparative de la réglementation du délit d'atteinte à la vie privée dans le droit pénal français et roumain 389
§1. Réglementation du délit d'atteinte à la vie privée en contexte européen 406
Conclusions du Chapitre 2 408
Conclusions Titre II 408
Conclusions Première partie 410

Seconde partie

Le droit pénal face à l'évolution technologique : intrusion, défis, adaptation 412

Titre I

Le droit pénal face aux algorithmes: une nouvelle réalité juridique 412

Chapitre 1 Le droit pénal face à l'intelligence artificielle, l'apprentissage automatique et le profilage de masse 412

Section 1. L'intelligence artificielle et le machine learning: enjeux et régulation juridiques 414
§1. L'adaptation dynamique des technologies numériques face aux exigences du droit 416
A. Machine Learning et Deep Learning 416
a). Contexte de la vie privée et confidentialité (privacy) 419
b). ONU : La gouvernance de l'IA et son impact sur l'humanité 420
B. Intelligence artificielle, apprentissage automatique et responsabilité pénale 422
a). Les délits générés par l'IA , créativité supérieure au délit classique 425
b). Europol: ChatGPT, aide pour commettre des délits (fraude, tromperie, manipulation) 428
c). Modèles de responsabilité pénale de l'IA 428
d). L'IA en tant que personne morale 432
C. Initiatives de régulation et régime punitif de l'intelligence artificielle 434
a). Peines pour l'intelligence artificielle 435
b). Réglementation de l'IA et de l'Apprentissage automatique en droit pénal 439
c). Initiatives législatives et nécessité d'adaptation 441
d). Rapport de la CNIL : la technologie IA respecte le droit à la vie privée 443
e). Juridiction des délits causés par l'IA 444
§2. Deepfake, profilage comportemental et manipulation de l'information 446
A. Deepfake et les médias synthétiques : une menace mondiale 448
a). Utilisations bénéfiques de la technologie DeepFake 450
b). Pourquoi les deepfakes sont-ils un problème? 451
c). Lutte contre les deepfakes 454
B. Big Data et profilage comportemental 455
a). Big Data, IA et la vie privée 456
b). Le profilage comportemental compromet-il le libre arbitre ? 460
c) L'attentat terroriste contre *Charlie Hebdo* – un nouveau paradigme juridique pour le profilage comportemental 462
C. Manipulation de l'information, un danger réel pour le droit à la vie privée 469
a). Réseaux sociaux, forme de gouvernance hybride 470
b). Attaque contre la liberté de volonté. Réaction du droit pénal contre la manipulation 471
c). De la première fausse nouvelle (1815) à la première loi de lutte contre la désinformation (1881) 472
d). Développements juridiques récents dans la lutte contre la manipulation et la désinformation 473
f). Astroturfing, swarming et « l'armée des 50 cents » 478
g). Arme stratégique pour déstabiliser les gouvernements et les sociétés 479
Conclusion §2. 481

Section 2. Défis imminents pour le droit pénal : le droit à l'anonymat et la vie privée dans le métavers 482
§1. EFFETS JURIDIQUES DE L'ANONYMAT EN LIGNE 483
A. Anonymat en ligne versus identité numérique 489
a). Dark web/deep web 494
b). Développement de marchés noirs virtuels 497
c). Silk Road, « supermarché » en ligne pour les délits 500
d). Groupes organisés démantelés par la justice française 502
e). Séquestration de données (ransomware) 503
B. Atteintes à la sécurité des données privées 504
a). La conception du Code pénal français. 504
b). La conception du Code pénal roumain 507
§2. La vie privée dans le métavers 507

A. Délits possibles en métavers 509
a). Interpol a ouvert son bureau en métavers pour enquêter sur les délits 510
b). Vide législatif pour les casinos du métavers 511
c). Impact du métavers dans la vie réelle 512
d). Mécanismes permettant d'identifier le délinquant 513
B. Perspectives juridiques actuelles 514
a). Juridiction dans le métaverse. 515
b). Vol d'objets virtuels. 516
c). Héritage de l'identité numérique après le décès du titulaire 517
d). Droit européen et français, intérêt pour les métavers. 517
Conclusions du Chapitre 1 518

Chapitre 2 Effets juridiques de la cryptographie dans les conversations numériques 520

Section 1. La vie privée à l'ère de la mondialisation numérique – limiter les intrusions 520

§1. Cryptographie encouragée par les législations 521
A. Reconnaissance de la cryptographie dans le cadre réglementaire 523
a). Règlement ePrivacy 523
b). Résolution du Conseil de l'Europe « Sécurité par cryptage et sécurité malgré le cryptage » 525
c). La France a déjà introduit dans sa législation la notion de cryptographie post-quantique 528
B. Cryptage : protection de la vie privée ou protection contre la criminalité 528
a). Conflit entre Apple et FBI au sujet de l'accès aux informations privées 529
b). Telegram bloquée sur le territoire de la Russie 530
c). Propriétaire de Telegram arrêté en France 530
d). Les effets négatifs du chiffrement : une source d'inquiétude pour le droit 531
e). CEDH : les informations peuvent également être obtenues sans saboter le cryptage 533
§2. Réglementation légale concernant l'interception des applications whatsapp, telegram, signal 534
A. France : le refus de remettre la clé de décryptage est pénalement sanctionné 539
a). Backdoors, une solution de décryptage controversée 540
B. Allemagne, les conversations peuvent être décryptées en cas de délits très graves 541
Conclusions du Chapitre 2 542
Conclusions Titre 1 543

Titre II Intrusion de l'état dans la vie privée. Synchronisation du droit pénal avec l'évolution technologique 545

Chapitre 1 Intrusion gouvernementale: du mandat de perquisition à l'interception des conversations 547

Section 1. Origine de l'état total, de la vision thomiste à la surveillance gouvernementale 547

§1. La nécessité d'intrusion: de la philosophie au droit 547
A. Théorie de Jürgen Habermas 549
a). Les réseaux sociaux facilitent la surveillance gouvernementale 551

b). Autonomie individuelle 552
B. De la philosophie thomiste à la surveillance des masses 553
a). Premier jugement limitant l'intrusion de l'État, le procès de Semayne (1604) 554
C. Méthodes de surveillance et d'intrusion 555
a). Origine juridique du mandat de perquisition 555
b). Première réglementation du mandat de perquisition en France (1808) 557
c). Mandat de perquisition en droit roumain 558
d). Manque de synchronisation entre le droit et la technologie ? 561
§2. Interception des communications téléphoniques, dans le contexte européen 561
A. Conditions d'émission du mandat d'interception 562
a). Malone versus Royaume-Uni (1984). 562
b). Le rapport Birkett de 1957 563
c). Loi sur l'interception des communications de 1985 566
B. Allemagne – première réglementation juridique explicite sur l'interception 567
a). La loi G10 (1968) permettait une surveillance totale de la population 568
b). L'interception des appels à distance doit être nécessaire 569
c). Surveillance technique des étrangers versus surveillance des propres citoyens 570
d). Iniquités liées à l'intrusion de l'État dans la vie privée 570
e). Les services secrets sont tenus de respecter le droit à la vie privée au-delà des frontières 574
C. Partenariats d'échange de données entre la France, l'Allemagne, les États-Unis et le Royaume-Uni 575
a). Obama : « Vous ne pouvez pas avoir 100 % de sécurité et 100 % de respect de la vie privée en même temps » 576
D. Surveillance de type Big Brother : ciblée et massive. Le point de vue de la CEDH 577
a. La surveillance ciblée dans la vision de la CEDH 578
b. La surveillance de masse selon la CEDH. Big Brother Watch 578

Section 2. La surveillance technique : mécanismes gouvernementaux de lutte contre la criminalité (france/roumanie) 583
§1. La surveillance technique en droit français 583
A. Passivité difficile à comprendre en France : aucune réglementation avant 1991 583
a). Pratique judiciaire, principale source de droit 584
B. Interceptions judiciaires 584
a). Affaire ordonnant l'interception, mais sans que des poursuites pénales soient engagées 586
b). Utilisation de IMSI catcher – les données du téléphone sont accessibles à distance 586
c). Les agents pénitentiaires pouvaient effectuer une surveillance technique 587
d). Principes régissant les interceptions judiciaires 588
e). Durée du mandat et motivation des décisions 589
C. Interceptions administratives 590
a). Première attestation légale : le 28 mars 1968 590
b). Les interceptions traditionnelles ne remplissent plus leur objectif 591
c). Données statistiques sur les interceptions administratives en 2023 591
d). CNCTR : les conversations des personnes sont collectées sans autorisation préalable 593
§2. La surveillance technique en droit roumain. Une menace pour la vie privée ? 594
A. Méthodes spéciales de surveillance 594
a). Mandats de surveillance obtenus avant le changement de cadre juridique 597
b). Procédure de délivrance du mandat de surveillance technique 600

B. Aspects controversés générés par l'expression « autres organes spécialisés de l'État » 604
a). Protocoles inconstitutionnels entre le SRI et le Ministère Public concernant les interceptions 606
b). Le médiateur: les interceptions réalisées par le SRI violent le droit à la vie privée 607
C. Information de la personne surveillée et de l'interlocuteur occasionnel 611
Conclusions du Chapitre 1 614

Chapitre 2 Surveillance électronique 616

Section 1. La surveillance électronique: une mesure substitutive à l'incarcération et ses arguments justificatifs 617
§1. Méthode alternative à l'incarcération. Arguments en faveur de la surveillance électronique 617
A. Les fondements théoriques et pratiques 618
a). Surveillance électronique dans la lutte contre la violence domestique 620
b). Inconvénients de la surveillance électronique – « prison électronique » 622
B. Utilisation de la surveillance électronique dans les États européens 624
a). Conseil de l'Europe : méthode alternative aux peines privatives de liberté 625
b). Rapport GREVIO sur la mise en œuvre de la surveillance électronique 626
c). L'Allemagne, réticente à utiliser la surveillance électronique 627
d). La Norvège n'utilise la SE que dans les cas de violence conjugale 628
e). En Suède, la SE réduit la récidive et facilite la réinsertion sociale 628
f). Belgique : Réduction la surpopulation carcérale 628
g). Différence de vision entre l'Europe et les États-Unis sur l'utilisation de la surveillance 629
§2. La surveillance électronique dans les systèmes juridiques français et roumain 630
A. Roumanie - Loi no. 146/2021 sur la surveillance électronique 631
a). De la violence domestique aux procédures pénales 633
B. Utilisation des bracelets électroniques en France 634
a). Historique de la réglementation juridique de 2000 à 2024 634
b). Tensions entre le droit européen et le droit français au sujet des bracelets électroniques 636
c). Moindres coûts pour la surveillance à l'aide du bracelet électronique 638
d). De l'expérience à l'usage généralisé 639
e). Détention à domicile sous surveillance électronique 640
f). Utilisation de la SE, une punition évolutive qui protège le droit à la vie privée 641
g). Moyens de surveillance à l'aide du bracelet électronique 643
h). Le caractère obligatoire du consentement a été exclu 644
Conclusions Chapitre 2 - sur l'utilisation de la surveillance électronique 644

Chapitre 3 Vie privée versus médecine moderne 646

Section 1. Protection des caractéristiques génétiques 646
§1. Le cadre juridique de la protection des caractéristiques génétiques 647
A. Loi de la bioéthique en France 648
a). Droit à l'oubli génétique 649
b). Médecine personnalisée et tests génétiques 651
B. Discrimination génétique 652
a). Discrimination génétique en France 652

b). Discrimination génétique en Roumanie 655
c). Convention d'Oviedo et autres actes normatifs 655
d). Utilisation abusive des données génétiques – Tribu Havasupai 656
d). Discrimination sociale 657
§2. Demande d'examiner les propres caractéristiques génétiques 658
A. Transparence pour l'utilisation des données génétiques 658
a). Utilisation du corps humain à des fins médicales et scientifiques 659
b). Vision sur le corps humain, à partir de la philosophie au droit 661
B. Tests génétiques sans intervention d'un médecin, directement au consommateur 662
a). Réglementation des tests génétiques 664
b). Respect des données privées du patient 667
c). La France et la Suisse, les seuls pays de l'UE à interdire le test ADN de type DTC 670

Section 2. Identification d'une personne sur la base des empreintes génétiques 672
§1. Fichier national des empreintes génétiques 672
A. Du stockage des données ADN pour les crimes les plus graves jusqu'aux délits mineurs 674
a). Suppression de données génétiques 676
B. Durée de conservation des données génétiques, selon la nature de l'infraction 677
a). Adaptation législative 679
b). Stockage des données génétiques en Roumanie 680
c). Durée de conservation des données génétiques en Roumanie 681
§2. Les controverses juridiques autour de la gestion des caractéristiques génétiques en europe 682
A. Décision de la CJUE (le 30 janvier 2024) : conservation des données biométriques et génétiques, de « nécessité absolue » 683
B. Intervention de la CJUE en cas de refus d'utilisation des données biométriques 686
a). Empreintes digitales et faciales dans les documents d'identité 687
b). La Grande-Bretagne, un cas particulier 689
c). Eurodac, la base de données d'empreintes digitales de l'UE 690
d). Identification basée sur les empreintes génétiques, interdite par l'Ordre des médecins 691
Conclusions du Chapitre 3 691
Conclusions pour le Titre 2 692

Conclusions générales et propositions de lege ferenda 693

Bibliographie 698

Annexes 817

Index alphabétiques 840

Tables des matières 844