THÈSE POUR OBTENIR LE GRADE DE DOCTEUR DE L'UNIVERSITÉ DE MONTPELLIER

En droit privé

École doctorale Droit et Science politique ED 461

Unité de recherche LICeM

L'encadrement juridique des données dans l'environnement numérique agricole

Présentée par Laura TOMASSO
Le 7 décembre 2022

Sous la direction de Mme Agnès ROBIN

Devant le jury composé de

Mme Nathalie Mallet-Poujol, Directrice de recherche CNRS, Université de Montpellier (CEPEL)	Présidente du jury
M. Thibault Douville, Professeur, Université de Caen	Rapporteur
M. Sylvain Chatry, Maître de conférences HDR, Université de Perpignan	Rapporteur
Mme Mélanie Clément-Fontaine, Professeure, Université Paris-Saclay	Examinatrice
Mme Véronique Bellon-Maurel, Ingénieure, INRAe	Examinatrice
Mme Agnès Robin, Maître de conférences HDR, Université de Montpellier	Directrice

UNIVERSITÉ DE MONTPELLIER

« Ce travail a bénéficié d'une aide de l'État gérée par l'Agence Nationale de la Recherche au titre du programme d'Investissements d'avenir portant la référence ANR-16-CONV-0004 ») » / "This work was supported by the French National Research Agency under the Investments for the Future Program, referred as ANR-16-CONV-0004."







Remerciements

Comme le disait si justement Antoine de Saint-Exupéry, « *la pierre n'a point d'espoir d'être autre chose qu'une pierre. Mais, de collaborer, elle s'assemble et devient temple* ». Aussi, sans la vigilance et la bienveillance du personnel enseignant, l'enthousiasme et la cohésion des membres de DigitAg, l'intérêt et les questionnements des acteurs du secteur agricole, ainsi que les encouragements et l'appui de ma famille et de mes amis ce travail n'aurait jamais pu voir le jour. Par conséquent, je remercie avec force ma directrice de thèse Mme Agnès Robin pour son écoute, ses conseils bienfondés, sa bienveillance et son appui tout au long de ces années de thèse. Je remercie également Mme Nathalie Mallet-Poujol pour ses conseils avisés, ainsi que l'ensemble des personnels enseignants qui ont pu me conseiller chaque fois que j'en ai eu besoin. Je remercie Mme Véronique Bellon-Maurel et l'ensemble des membres de DigitAg, parmi lesquels je cite M. François Brun qui m'ont offert l'opportunité de cette recherche et m'ont permis de mieux comprendre les enjeux entourant les données dans le secteur agricole. De même, les rencontres et les échanges avec l'ensemble des acteurs du secteur agricole m'ont été précieux pour la réalisation de cette thèse. Je remercie également M. Bruno Lauga grâce à qui j'ai pu participer à de multiples projets de recherche me permettant d'enrichir mon travail. Je n'oublie pas non plus de remercier mes parents, mon compagnon et mes amis qui m'ont toujours encouragé et soutenu du premier au dernier jour sans jamais sourciller.

Sommaire

Remerciements *2*

Sommaire *3*

Liste des principales abréviations *4*

Introduction *9*

Partie I. L'accessibilité des données agricoles *37*

Titre I. L'accès aux données agricoles : l'émergence d'un droit d'accès pour l'agriculteur **38**

Chapitre 1. L'accessibilité des données agricoles publiques 39

Chapitre 2. L'accessibilité des données agricoles privées 97

Titre II. La réservation privative des données agricoles : l'organisation de l'exclusivité par les entreprises **152**

Chapitre 1. La réservation de l'accès aux données agricoles protégées 153

Chapitre 2. La réservation de l'accès aux données agricoles non protégées 204

Partie II. La maîtrise de l'usage des données agricoles *257*

Titre I. L'absence regrettée de contrôle de l'usage des données d'exploitation **259**

Chapitre 1. L'absence de contrôle par l'agriculteur de l'usage des données d'exploitation non personnelles 260

Chapitre 2. Le développement du contrôle de l'usage des données non personnelles d'exploitation par l'agriculteur 314

Titre II. La maîtrise envisagée de l'usage des données d'exploitation par l'exploitant agricole **361**

Chapitre 1. La consécration souhaitée du droit de contrôle de l'usage des données d'exploitation à caractère non personnel 363

Chapitre 2. La consécration actée du droit de contrôle de l'usage des données d'exploitation à caractère personnel 408

Conclusion *463*

Bibliographie *470*

Table de jurisprudence *494*

Index *509*

Liste des principales abréviations

Revues et ouvrages

AJCA	*Actualité juridique. Contrats d'affaires. Concurrence. Distribution*
AJCT	*Actualité juridique. Collectivités territoriales.*
AJDA	*Actualité juridique. Droit administratif*
AJP	*Actualité juridique pénal*
ALD	*Actualité Législative Dalloz*
Bull. civ.	*Bulletin des arrêts de la Cour de cassation (Chambres civiles)*
Bull. crim.	*Bulletin des arrêts de la Cour de cassation (Chambres criminelles)*
Cah. dr. aut.	*Cahier du Droit d'auteur*
Cah. dr. ent.	*Cahier du Droit de l'entreprise*
CCC	*Revue contrats, concurrence, consommation*
CCÉ	*Communication commerce électronique*
CDST	*Cahiers Droit, Sciences & Technologies*
D.	*Recueil Dalloz*
D. aff.	*Dalloz Affaires*
D.S.	*Dalloz Sirey*
Dalloz IP/IT	*Droit de la propriété intellectuelle et du numérique*
DIT	*Droit de l'informatique et des télécoms*
GAPI	*Les grands arrêts de la propriété intellectuelle*
Gaz. Pal.	*Gazette du Palais*
J.-Cl.	*Juris-classeur*
JCP	*Juris-classeur périodique, (Semaine juridique)*
JCP A	*Juris-classeur périodique, (Semaine juridique), édition administration et collectivités territoriales*
JCP E	*Juris-classeur périodique, (Semaine juridique), édition entreprise*
JCP G	*Juris-classeur périodique, (Semaine juridique), édition générale*
JDI	*Journal du Droit International*
JEEA	*Journal of the European Economic Association*
JOAN	*Journal officiel de l'Assemblée nationale*
JOCE	*Journal officiel des Communautés européennes*
JOOEB	*Journal officiel de l'office européen des brevets*
JORF	*Journal officiel de la République française*
JOUE (ex JOCE)	*Journal officiel de l'Union européenne (ex. Journal officiel des Communautés européennes)*

LEPI	*L'Essentiel Droit de la propriété intellectuelle*
LCN	*Les Cahiers du Numérique*
LGDJ	*Librairie Générale de Droit et de Jurisprudence*
LLL	*Les Liens qui Libèrent*
LPA	*Les petites affiches*
PI	*Propriétés Intellectuelles*
Propr. industr.	*Propriété industrielle*
PUF	*Presses Universitaires de France*
PUC	*Presses Universitaires de Caen*
PUJP	*Presses Universitaires Juridiques de Poitiers*
RDC	*Revue des contrats*
RDLF	*Revue des Droits et Libertés Fondamentaux*
RDTI	*Revue du droit des technologies de l'information*
Rec.	*Recueil Lebon des décisions du Conseil d'État*
Rec. ADCC Lamy	Recueil des avis et décisions du Conseil de la concurrence
Rec. CJCE – CJUE	*Recueil de la jurisprudence de la Cour de justice et du Tribunal de première instance de l'Union européenne*
Rép. cont. adm.	*Répertoire de contentieux administratif – Encyclopédie Dalloz*
Rép. dr. civ.	*Répertoire de droit civil – Encyclopédie Dalloz*
Rép. resp. puiss. Pub.	*Répertoire de la responsabilité de la puissance publique - Encyclopédie Dalloz*
Rev. Aff. eur.	*Revue des affaires européennes*
RFAP	*Revue française d'administration publique*
RFDA	*Revue française de droit administratif*
RIDA	*Revue internationale du droit d'auteur*
RIDC	*Revue internationale de droit comparé*
RIDE	*Revue internationale de droit économique*
RJC	*Revue de jurisprudence commerciale*
RJE	*Revue Juridique de l'Environnement*
RJEP	*Revue juridique de l'économie publique*
RJPF	*Revue Juridique Personne & Famille*
RLC	*Revue Lamy de la Concurrence*
RLDA	*Revue Lamy Droit des Affaires*
RLDC	*Revue Lamy Droit civil*
RLDI	*Revue Lamy Droit de l'Immatériel*
RRJ	*Revue de recherche juridique – Droit prospectif*
RSC	*Revue de science criminelle et de f comparé*
RTD civ.	*Revue trimestrielle de droit civil*
RTD com.	*Revue trimestrielle de droit commercial*
RTD eur.	*Revue trimestrielle de droit européen*

S.	*Sirey*

Autres abréviations

ACTA	Association de coordination technique agricole
AFDA	Association française pour la recherche en Droit Administratif
AGD	Administrateur Général des Données
al.	*alinéa*
AN	Assemblée Nationale
APIE	Appuie au Patrimoine Immatériel de l'État (ex. Agence du Patrimoine Immatériel de l'État)
art.	article
Ass. Plèn.	Assemblée Plénière de la Cour de cassation
Aut. Conc.	Autorité de la Concurrence
Av. gén.	Avocat général
BOCC	Bulletin officiel des conventions collectives.
C. civ.	Code civil
C. com.	Code de commerce
C. conso.	Code de la consommation
C. constit.	Conseil constitutionnel
C. env.	Code de l'environnement
C. pén.	Code pénal
C. rech.	Code de la recherche
C.J.C.E	Cour de justice des Communautés européennes
c/	contre
CA	Cour d'appel
CAA	Cour administrative d'appel
CCI	Chambre du Commerce et de l'Industrie
CDC	Cour des comptes
CE (Sect., Ass.)	Conseil d'État (Section du contentieux, Assemblée du contentieux)
CEDH	Cour Européenne des Droits de l'Homme
CEPD (ex. G29)	Comité européen de la protection des données (ex. Groupe de travail « article 29 » sur la protection des données)
CEIPI	Centre d'études internationales de la propriété intellectuelle
CESE	Comité économique et social européen
CGPPP	Code Général de la Propriété des Personnes publiques
Ch. Réunies	Chambres réunies de la Cour de cassation
Chr.	Chronique
Circ.	Circulaire

Civ. (1ère, 2ème, 3ème)	Chambre civile de la Cour de cassation (1ère chambre, 2ème chambre, 3ème chambre)
CJA	Code de Justice Administrative
CMP	Commission mixte paritaire
CNIL	Commission Nationale de l'Informatique et des Libertés
CNNum	Conseil National du Numérique
CNRS	Centre National de la Recherche Scientifique
codif.	codification
Coll.	Collection
Com.	Chambre commerciale de la Cour de cassation
Comm.	Commission
comm.	commentaire
concl.	conclusion
cons.	considérant
Cons. const.	Conseil Constitutionnel
Conv. EDH	Convention Européenne des Droits de l'Homme
CPI	Code de la propriété intellectuelle
Crim.	Chambre criminelle de la Cour de cassation
CRPA	Code de Relations entre le Public et l'Administration
CSPLA	Conseil Supérieur de la Propriété Littéraire et Artistique
D.	Décret
déc.	décision
Dir.	Directive
DRAAF	Direction Régionale de l'Alimentation, de l'Agriculture et de la Forêt
DUDH	Déclaration Universelle des Droits de l'Homme
éd.	édition
EDCE	Études et documents du Conseil d'État
EFL	Édition Francis Lefebvre
ENA	École National d'Administration
et *al.*	et *alii* (et autres)
ét.	étude
Fasc.	Fascicule
FNSEA	Fédération Nationale des Syndicats des Exploitations Agricoles
G29	Groupe de travail « Article 29 » sur la protection des données
Ibid.	*Ibidem* (au même endroit)
Id.	*Idem*.
Infra.	Ci-dessous
INPI	Institut National de la Propriété Industrielle
JA	Jeunes Agriculteurs – Syndicat agricole
Jurisp.	Jurisprudence

L.	Loi
LO	Loi organique
LPF	Livre des Procédures fiscales
LRN	Loi pour une République Numérique
n°	numéro
Nouv. bibl. de thèse	Nouvelle bibliothèque de thèse
obs.	observations
OCDE-OECD	Organisation de coopération et de développement économiques
OEB ch. rec. tech.	Office européen des brevets chambre de recours techniques
op. cit.	*opere citato* (ouvrage cité)
ord.	ordonnance
p.	page
PAC	Politique agricole Commune
Pan.	Panorama
PM	Premier ministre
Prat.	Pratique
Préc.	Précité
Préf.	Préface
pt.	point
R.	Recueil de jurisprudence
Reco.	Recommandation
Règl.	Règlement
Req.	Requête
s.	suivant
Soc.	Chambre sociale de la Cour de cassation
Somm.	Sommaire
spéc.	spécialement
ss. dir.	sous la direction de
Sté	Société
Supra.	Ci-dessus
t.	Tome
T. confl.	Tribunal des conflits
TA	Tribunal administratif
TGI	Tribunal de grande instance
TI	Tribunal d'instance
TPI	Tribunal Pénal International
TPICE - TPIUE	Tribunal de première instance des Communautés européennes – Tribunal de première instance de l'Union européenne
vol.	volume

Introduction

1- **Le secteur agricole en mutation**. L'évolution du secteur agricole vers la numérisation de ses activités nécessite une évaluation des risques juridiques et la recherche d'un régime adéquat pour l'exploitation des données de l'agriculture numérique. La multiplicité et la variété des données doivent encourager l'étude de chacune des réglementations qui leur sont applicables afin de ne pas les passer au lit de Procuste. Une telle déformation consisterait à les intégrer dans des catégories juridiques préexistantes peu adaptées. Les données de l'agriculture numérique doivent donc nécessairement être étudiées dans toutes leurs spécificités afin de leur octroyer le régime juridique le plus adéquat selon les intérêts en jeu.

En effet, le droit s'est toujours adapté aux évolutions de la société, il doit aujourd'hui s'adapter à ce que les observateurs nomment la « disruption numérique ». Ce nouveau paradigme est un puissant vecteur de changement qui engendre de nouveaux modèles économiques et sociétaux auxquels tous les pans de la société doivent s'adapter. Le secteur agricole est également impacté par cette transformation numérique.

2- **Le *Big Data* agricole**. Chaque jour des milliards de données sont produites et collectées par des machines-outils, des satellites, des drones afin de calculer la température, les teneurs en phosphores ou en potassium des sols, la hauteur d'eau tombée, la quantité et la qualité du lait collecté, ou encore la quantité de produits phytosanitaires répandue sur une exploitation. Ces données permettent, entre autres, d'utiliser les bonnes doses de produits au bon moment, au bon endroit ou de détecter d'éventuelles maladies des plantes et des bêtes. Dans un contexte économique instable, de changements climatiques et de modification des habitudes des consommateurs, l'agriculture numérique permet l'innovation et l'amélioration de la productivité de l'agriculture française. En effet, des start-ups, des multinationales, mais aussi, les instituts de recherche agricole, proposent des solutions numériques afin d'offrir des outils d'aide à la décision et des prédictions dans le but d'améliorer les conditions de travail des agriculteurs. Toutes les filières agricoles sont concernées (céréalière, viande, lait…). L'exploitation du *Big Data* agricole offre, ainsi, la possibilité d'obtenir une agriculture d'une plus grande précision, une aide à la prise de décision, une meilleure rentabilité, une plus grande prévisibilité, ou encore, la possibilité d'une mise en commun des informations entre exploitants. Finalement, l'agriculture numérique entraîne un déplacement de la valeur du travail de la terre à celui de la détention des données et du contrôle des algorithmes.

3- **Un marché en pleine expansion.** L'économie du numérique est marquée par la multitude, tant en termes de données, d'acteurs, que d'activités ou encore de services proposés qui ne trouvent de limites que dans l'imagination des acteurs du secteur agricole. Aussi, sur le marché de l'agriculture numérique cohabitent les exploitants agricoles, les prestataires de services, les fournisseurs de matériels, les intégrateurs de logiciel, les plateformes d'intermédiation, les scientifiques, les administrations ainsi que les plateformes telles que les places de marché. Les données collectées peuvent avoir une origine publique ou privée, être brutes, agrégées, ou encore transformées. Elles peuvent, également, avoir un caractère personnel ou non. Cette pluralité de données, d'acteurs, d'activités, mais aussi de relations (publiques, privées, commerciales, collaboratives, etc.) complique l'analyse du cadre juridique de la collecte, de l'utilisation et du partage des données agricoles.

4- **L'impulsion de la recherche.** Le cadre juridique entourant les données agricoles interroge les acteurs du secteur. C'est pourquoi l'Institut de Convergences Agriculture Numérique #DigitAg[1] créé en 2017 à Montpellier porté par l'IRSTEA et l'INRA, s'est positionné largement sur le secteur de l'agriculture numérique de manière interdisciplinaire et a proposé de construire « *les socles scientifiques et les compétences indispensables aux innovations technologiques, organisationnelles, marketing, économiques, sociales, qui verront le jour en agriculture* »[2]. En droit, initialement, la question se posait de savoir quel était le cadre juridique des plateformes collaboratives dans le secteur de l'agriculture numérique. Au cours de la recherche, cependant, il est apparu assez rapidement que les plateformes n'étaient en réalité qu'un outil de partage des données agricoles devant faire l'objet d'un développement sous-jacent. En effet, l'objet principal de la recherche a été recentré sur les données du secteur agricole, objet de toutes les préoccupations. La question s'est donc déplacée sur celle de savoir quels sont les enjeux et les risques liés à la collecte, au partage et à l'exploitation des données agricoles.

5- La grande pluralité de données collectées et produites dans le secteur agricole rend difficile l'appréhension des notions. Néanmoins, ce n'est qu'une fois que ces notions ont été délimitées

[1] #DigitAg créé en 2017, dirigé par Mme V. Bellon-Maurel, réunit des instituts de recherche (INRAE, INRIA et Cirad), des établissements d'enseignement supérieur (Université de Montpellier, Institut Agro – Montpellier SupAgro et AgroParisTech), des structures de transfert (Instituts Techniques Agricoles de l'ACTA et SATT AxLR), et des entreprises (Agriscope, Fruition Sciences, IDATE, ITK, Pera-Pellenc, SMAG, TerraNIS et Vivelys). #DigitAg offre une recherche interdisciplinaire sur les questions de l'agriculture numérique entre sciences humaines et sociales, sciences agricoles ou encore sciences de l'ingénieur. Cet institut finance plusieurs thèses parmi lesquelles cette recherche a fait partie des premières cofinancées en partenariat avec l'Université de Montpellier.

[2] BELLON-MAUREL, V. et HUYGHE, C., « avant-propos », *Sciences Eaux & territoires*, 2019/3, n°29, pp. 3 à 5.

qu'il est possible d'envisager les droits applicables ainsi que leur titularité. La juste mesure est toutefois de mise afin de trouver un équilibre entre l'exploitation de tout le potentiel des données agricoles et leur protection. Par conséquent, s'il faut prendre acte de l'avènement des données dans l'agriculture numérique (**I**), il demeure que leur cadre juridique est difficile à appréhender (**II**), c'est pourquoi il est aujourd'hui nécessaire d'envisager l'élaboration d'un cadre adapté aux données agricoles (**III**).

I. L'avènement des données dans l'agriculture numérique

6- L'étude des données agricoles suppose d'envisager le contexte de la recherche qui conduit à mener une réflexion sur les enjeux du développement du numérique dans ce secteur. Le numérique, en effet, est le nouveau moteur de l'agriculture (**A**) et pour alimenter ce moteur, les données font figure de carburant (**B**). En outre, plusieurs personnes gravitent autour de ces données (**C**).

A. Le numérique : le nouveau moteur de l'agriculture

7- L'agriculture est, par essence, un secteur d'activité lié à la terre et à son observation. Les connaissances se transmettent souvent dans le cercle familial et restent cantonnées à l'échelle de l'exploitation. Néanmoins, aujourd'hui, l'humanité est confrontée à des enjeux majeurs pour la perpétuation de son espèce et pour l'environnement. L'agriculture est l'un des secteurs les plus durement touchés par ces nouvelles problématiques. Le secteur agricole devra, en effet, dans un futur très proche, nourrir plus de huit milliards d'êtres humains tout en répondant à des problématiques notamment sociétales, économiques, environnementales ou climatiques. L'explosion démographique, les changements climatiques, l'amenuisement des ressources en eau et en terres disponibles, la disparition de la biodiversité sont donc autant de défis auxquels les agriculteurs sont confrontés. À ces problématiques s'ajoutent celles de la pénibilité du travail et des risques du métier d'agriculteur qui en font une profession peu attractive, largement délaissée par les nouvelles générations. Les agriculteurs sont en effet bien souvent confrontés, entre autres, à l'*imbroglio* administratif, à la volatilité des prix, à l'exigence des réglementations, ou encore, à de nombreux contrôles administratifs.

Si d'une part le numérique apporte des solutions non négligeables aux défis que rencontre le secteur agricole (**1**), d'autre part, des points de vigilance doivent être soulevés concernant l'utilisation du numérique dans l'agriculture (**2**).

1. L'aubaine du numérique pour répondre aux défis de l'agriculture

8- **De nouveaux enjeux.** Afin de répondre aux nouveaux enjeux que rencontre le secteur agricole, le numérique et les nouvelles technologies offrent des solutions en disruption avec les pratiques agricoles d'antan. De ce fait, les agriculteurs doivent s'adapter à cette digitalisation de leur activité et prendre une part prépondérante dans ce nouveau paradigme afin de parvenir à une agriculture viable et pérenne. L'objectif étant de « *produire plus et mieux* »[3]. D'ailleurs, le rapport de mission *Agriculture & innovation 2025*[4] retient la solution du numérique dans ses recommandations en ce que la technologie et le numérique révolutionnent l'agriculture et permettent de faire émerger de nouveaux modèles plus durables[5].

9- **L'agriculture de précision.** L'agriculture numérique est au territoire et à l'exploitation agricole ce que l'agriculture de précision est à la parcelle. L'agriculture de précision est, en effet, un « *principe de gestion de parcelles agricoles qui vise l'optimisation des rendements et des investissements, en cherchant à tenir compte des variabilités intra-parcellaires* »[6]. L'objectif est donc d'apporter de manière spécifique et précise ce dont la parcelle ou les animaux ont besoin. Pour ce faire, des capteurs ou des objets connectés[7] sont placés sur la parcelle, ils collectent des données sur les cultures, les animaux d'élevage, leur état de santé, leurs comportements ou encore leurs besoins. Ces données permettent ensuite de poser un diagnostic qui élabore une recommandation, voire l'applique immédiatement. Il peut s'agir, par exemple, d'un apport en produits phytopharmaceutiques afin de traiter de manière précise la présence de nuisibles. En somme, ces outils fournissent de l'aide à la décision aux agriculteurs et aux éleveurs et sont utiles afin d'apporter « *la bonne dose, au bon moment, au bon endroit* ». Ils permettent également d'éviter « *le gaspillage et les pollutions* », grâce à l'observation et à

---

[3] BELLON-MAUREL, V., BOURNIGAL, J.-M. et LENAIN, R., « L'équation technologique et numérique en agriculture », *Le Démeter,* 2019, pp. 125 à 141.
[4] BOURNIGAL, J.-M., HOULLIER, F., LECOUVEY, P. et PRINGUET, P., *30 projets pour une agriculture compétitive et respectueuse de l'environnement*, #AgricultureInnovation2025, Propositions, oct. 2015.
[5] BELLON-MAUREL, V., BOURNIGAL, J.-M. et LENAIN, R., *opere citato.*
[6] *Ibis in idem.*
[7] Les objets connectés sont définis comme des objets physiques disposant de capteurs ou de puces, capables d'échanger des informations à courte ou longue distance ; voir la définition autour des objets connectés par la Commission de régulation de l'énergie (CRE), https://www.smartgrids-cre.fr/encyclopedie/linternet-des-objets-au-coeur-des-smart-grids/definitions-autour-des-objets-connectes.

la géolocalisation[8] et facilitent le travail des agriculteurs, leur dégage du temps et leur offre une meilleure prévisibilité. En outre, les sources de ces données[9] sont multiples et variées. Les objets connectés, tels que les stations météorologiques, les capteurs d'humidité du sol, ceux installés sur les animaux pour connaître leur état de santé, ou encore ceux posés sur les agroéquipements, peuvent communiquer entre eux au moyen de l'internet des objets[10]. Les satellites et les Smartphones, toujours plus équipés et performants, offrent, aussi, de nouvelles perspectives pour l'agriculture. En définitive, tous ces nouveaux outils « *contribuent fortement à la création de données* »[11] et participent au phénomène du *Big Data*. Ce concept, apparu à la fin des années 1990, fait référence à la collecte et à l'agrégation de grandes masses de données et implique quatre dimensions que l'on nomme les 4 V, il s'agit du Volume des données, de leur Variété, par leur nature, leur source, leur format, de la Vitesse croissante à laquelle elles sont produites et transférées dans le réseau, mais également de leur Véracité. C'est donc à partir de ce réservoir constitué de milliards de données qu'a pu se développer l'agriculture numérique.

10- **L'agriculture numérique va au-delà de l'agriculture de précision.** Il est possible de définir l'agriculture numérique comme une agriculture « *qui utilise les technologies de l'information et de la communication (TIC) : technologies d'acquisition de données (satellites, capteurs, objets connectés, Smartphones…), de transfert et de stockage (couverture 3G/4G, réseaux bas débit terrestre ou satellitaire, clouds) et technologies de traitement embarquées ou déportées (supercalculateurs accessibles par des réseaux de communication très haut débit) […] et ceci à toutes les échelles de la production agricole et de son écosystème que ce soit au niveau de l'exploitation (optimisation des opérations culturales, de la conduite de troupeau…), dans les services d'accompagnement (nouveaux services de conseil agricole basés sur des données collectées automatiquement), ou à des échelles plus grandes comme dans un territoire (gestion de l'eau) ou dans une chaîne de valeur (amélioration des intrants comme les semences, meilleure adéquation entre la production et le marché…)* »[12]. L'agriculture numérique vise

[8] BELLON-MAUREL, V., BOURNIGAL, J.-M. et LENAIN, R., « L'équation technologique et numérique en agriculture », *op. cit.*

[9] BELLON-MAUREL, V., NEVEU, P., TERMIER, A. et GARCIA, F., « Le *Big Data* en agriculture », *Enjeux numériques, n°2, Annales des Mines*, juin 2018, p. 78.

[10] L'Internet des objets ou *Internet of Things* (IoT) est défini comme « *un réseau de réseaux qui permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs mobiles sans fil, d'identifier directement et sans ambiguïté des entités numériques et des objets physiques. Cela afin de pouvoir récupérer, stocker, transférer et traiter, sans discontinuité entre les mondes physiques et virtuels, les données s'y rattachant* » ; BENGHOZI, P.-J., BUREAU, S. et MASSIT-FOLLEA, F., *L'internet des objets, Quels enjeux pour l'Europe*, MSH, 2009, n°5.

[11] SERONIE, J.-M., *Vers un big bang agricole ? Révolution numérique en agriculture*, Nouvelles pratiques, autonomie et créativité, France agricole, 2016, p. 54.

[12] BELLON-MAUREL, V. et HUYGHE, C., « L'innovation technologique dans l'agriculture », *Géoéconomie 80*, mai/juin 2016, pp. 159 à 180.

donc « *la gestion des risques, la résilience et la démarche holistique, sur les plans techniques (on gère l'optimisation du système de culture/de l'élevage dans son ensemble, avec les échanges de flux associés) et économiques (produire pour un objectif de marché)* »[13]. En outre, l'agriculture numérique facilite la collecte et l'échange de données[14], afin de développer les expérimentations dont l'objectif est de produire des connaissances agronomiques[15]. Elle permet également d'obtenir plus de transparence quant aux usages et aux techniques agricoles.

11- **L'intérêt du numérique pour le secteur agricole.** L'intelligence artificielle permet aux machines d'apprendre de manière autonome grâce au *Deep Learning* et au *Machine Learning*. Appliqué à l'agriculture, certains véhicules et robots sont autonomes et, en partie, autoapprenants[16]. Les données collectées associées à l'intelligence artificielle permettent de fournir des connaissances utiles aux agriculteurs. La valorisation des données est devenue un secteur économique lucratif dans lequel tant la recherche que des entreprises privées se sont positionnées afin de développer des outils d'aide à la décision, d'analyse de données, de services de partage, des infrastructures de stockage, etc. Le partage des données est en effet fondamental pour développer des connaissances et tirer des informations utiles au secteur agricole. Cela permet donc de « *développer des services à destination des agriculteurs, principalement sous forme d'outils d'aide à la décision, en développant des algorithmes basés sur la modélisation, permettant d'obtenir des modèles prédictifs* »[17]. C'est pourquoi des infrastructures doivent être construites afin de stocker les données et les analyser, ce qui nécessite en outre la création d'ontologie afin de « *coupler entre elles les différentes sources de données* »[18].

2. Les points de vigilance du développement du numérique pour les défis de l'agriculture

12- **Le numérique au service de l'agriculture n'est pas que panacée.** Des obstacles et des risques naissent du développement de l'agriculture numérique. Ces difficultés doivent être prises en compte dans la construction du cadre juridique des données agricoles. L'objectif principal est donc de permettre un partage équitable de la valeur des données lors de la construction du

[13] BELLON-MAUREL, V. et HUYGHE, C., « avant-propos », *Sciences Eaux & territoires, op. cit.*
[14] BELLON-MAUREL, V. et HUYGHE, C., « L'innovation technologique dans l'agriculture », *Géoéconomie 80,* mai/juin 2016, 159 à 180.
[15] *Ibid.*
[16] SERONIE, J.-M., *Vers un big bang agricole ?, op. cit.,* p. 54.
[17] BELLON-MAUREL, V., BOURNIGAL, J.-M. et LENAIN, R., « L'équation technologique et numérique en agriculture », *op. cit.*
[18] BELLON-MAUREL, V. et HUYGHE, C., « L'innovation technologique dans l'agriculture », *op. cit.*, pp. 159 à 180.

modèle économique. Aussi, l'idée au départ vertueuse de la construction d'une économie collaborative « *qui résulte de la mise en commun de ressources et d'efforts* »[19] est aujourd'hui dévoyée par la récupération des valeurs créées par des « *agents économiques cyniques étrangers à l'idéologie de partage altruiste qui sous-tend cet écosystème* »[20]. Le risque tient au fait que les très grandes entreprises s'arrogent les jeux de données massives de l'agriculture et imposent à terme leurs choix tant économiques que pratiques ainsi que des modèles agricoles aux agriculteurs. Ceux-ci pourraient alors se retrouver asservis à ces entreprises. Les exploitants agricoles n'auraient dans ce cas plus la maîtrise des données de leur exploitation et, par extension, la maîtrise de leur métier. Ils pourraient donc perdre leur autonomie et être dirigés à distance, ce qui aurait pour effet de les reléguer au rôle de manutentionnaire des machines pour le compte des agro-industriels. En outre, si le développement du numérique favorise la transparence et permet de contrôler les éventuelles dérives de certains producteurs, pour autant cela ne doit pas non plus être un prétexte pour surcontrôler les activités des agriculteurs au risque de les asphyxier dans leur pratique. Également, des obstacles techniques limitent le partage des données. La première difficulté réside dans les restrictions d'accès aux infrastructures de données et au manque d'interopérabilité entre les différents services proposés. La seconde repose sur « *[l']absence d'ontologies largement partagées* »[21]. L'objectif est donc de faire du numérique un allier de l'agriculture et non un ennemi, en trouvant un équilibre lors du partage de la valeur des données agricoles.

B. Les données : le carburant de l'agriculture numérique

13- Afin d'étudier les données agricoles, il convient d'abord d'envisager les difficultés d'appréhension de la notion même de « donnée » (**1**) pour, ensuite, s'intéresser à la circonscription de la recherche aux seules données agricoles (**2**).

1. Les difficultés d'appréhension de la notion de donnée

14- L'étude des données produites et collectées dans le secteur agricole suppose d'en délimiter l'objet et d'en définir la notion. Dans une acception technique de la notion de « donnée », il

[19] BENABOU, V.-L. et ROCHFELD, J., *À qui profite le clic ?, Le partage de la valeur à l'ère numérique*, Odile Jacob, 2015, p. 22.
[20] *Ibid.*
[21] BELLON-MAUREL, V., NEVEU, P., TERMIER, A. et GARCIA, F., *Le Big Data en agriculture, op. cit.*

s'agit de la « *description élémentaire d'une réalité qui ne relève que des éléments de fait* »[22]. Les juristes n'ont pas encore déterminé la nature juridique de la donnée, elle doit donc, tout d'abord, faire l'objet d'une qualification. L'arrêté du 22 décembre 1981 définit la donnée comme « *la représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement* ». Mais cette définition ne permet pas d'appréhender pleinement la notion de donnée dans toutes ses acceptions. La définition de la « donnée » doit en effet être envisagée selon son objet, la personne qui l'exploite ou bien sa fonction[23]. C'est d'ailleurs cette pluralité d'acceptions qui retient le juriste d'établir une définition globale et générale de la notion de « donnée ». Aussi, sans prétendre donner une définition de la « donnée », il convient, néanmoins, d'essayer d'en dessiner les contours (**a**) pour, ensuite, envisager l'asymétrie qui existe entre la notion de « données » et celle d'« informations » (**b**).

a. Les contours de la notion de donnée

15- **Un objet multiple.** Les données sont très nombreuses et variées, en témoigne l'ouvrage de Rob Kitchin[24], *The Data Revolution*, dans lequel l'auteur s'évertue à définir précisément ce qu'est une donnée et à fournir une présentation complète des différents types de données. Par exemple, il existe les données collaboratives, les données issues des capteurs et autres objets connectés, les données issues des systèmes de gestion, ou encore, les données transactionnelles[25]. Le domaine agricole n'échappe pas à la règle. Il existe dans ce secteur une pluralité de données de nature et d'objet hétérogènes et ayant leurs caractéristiques propres. Ces données ont, également, leur propre valeur qui peut fluctuer dans l'espace et le temps. Une donnée n'a en effet pas la même valeur lorsqu'elle est conservée dans les serveurs d'une entreprise ou lorsqu'elle est diffusée à un large public.

16- **Notion de « donnée ».** La notion de « donnée » revêt plusieurs réalités qu'il convient d'envisager tour à tour. Tout d'abord, la donnée peut être envisagée selon son niveau de

[22] ABITEBOUL, S. et PEUGEOT, V., *Terra Data. Qu'allons-nous faire des données numériques ?,* Cité des sciences et de l'Industrie, éd. Le Pommier, p. 30

[23] ZOLYNSKI, C., « Un nouveau droit de propriété intellectuelle pour valoriser les données, le miroir aux alouettes », *Dalloz IP/IT* 2018, p. 94 ; mission du CSPLA, présidée par BENABOU, V.-L., avec la coll. De ZOLYNSKI, C., rapporteur, et CYTERMANN, L., *Droit de la propriété littéraire et artistique, données et contenus numériques*, rapport présenté le 11 oct. 2018, p. 17 : La définition de la donnée est liée à « *l'objet mis en données, avec la personne dont elles émanent ou encore au vu de la fonction qu'on tend à leur assigner* ».

[24] KITCHIN, R., *The Data revolution, Big Data, Open Data, Data infrastructures and their consequences*, Sage, 2014.

[25] CHIGNARD, S. et BENYAYER, L.-D., *Datanomics, Les nouveaux business models des données*, FYP éd., 2015, pp. 30 et 31.

traitement. En effet, la donnée collectée par un objet connecté est d'abord brute avant d'être agrégée et traitée. Ce sont celles qui sont « *collectées par les capteurs, sans aucune forme de traitement* »[26], il s'agit donc de simples observations collectées au moyen d'objets connectés. Ces données brutes peuvent aussi être qualifiées de données industrielles[27]. À l'inverse, les données traitées sont celles qui ont fait l'objet d'un traitement au moyen de processus, c'est-à-dire, d'algorithmes qui permettent d'extraire des informations ou de produire du savoir. Les données agrégées sont, en revanche, celles qui sont agglomérées dans une base de données. Le contexte de la collecte joue également un rôle dans la qualification des données. La nature publique ou privée du contexte de la collecte peut influer sur leur nature publique ou privée. Elles peuvent également être produites dans le cadre de la recherche scientifique. Enfin, les données peuvent aussi être distinguées selon leur objet. Par exemple, elles peuvent contenir des informations personnelles ou non, ou encore, porter sur des informations publiques ou d'intérêt général.

17- **Évolution de la notion.** En réalité, chaque catégorie de données, nommées et définies par le législateur ou la doctrine, correspond à un objet dont la qualification était nécessaire. La qualification des données permet effectivement de les régir ou de leur offrir un cadre en raison de la prise en compte de nouveaux enjeux. C'est pourquoi le législateur, au fil des textes, a fait émerger de nouvelles catégories de données, telles que les ensembles de données de forte valeur[28] dernières nées d'une longue liste. Le législateur encadre, donc, juridiquement une nouvelle catégorie de données chaque fois que cela est utile afin d'atteindre un objectif tel que la protection de la vie privée, le développement économique, ou encore, la diffusion de l'information.

b. L'asymétrie des notions de données et d'informations

18- **Notion d'« information ».** Des auteurs se sont évertués à définir la notion d'« information ». M. le Professeur P. Catala, qui est l'instigateur de ce mouvement, retient la fonction de communicabilité de l'information, en précisant qu'elle est « *d'abord expression, formulation,*

[26] *Ibid.*
[27] ZOLYNSKI, C., « Un nouveau droit de propriété intellectuelle pour valoriser les données, le miroir aux alouettes », *op. cit.*
[28] Dir. n°2019/1024 du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public : *JOUE* L 172/56 du 26 juin 2019 (PSI III).

destinée à rendre un message communicable (et) est ensuite communiquée ou peut l'être »,[29] et ce quelle que soit sa forme[30], ou encore comme *« un élément de connaissance susceptible d'être présenté à l'aide de conventions pour être conservé, traité ou communiqué* »[31]. Il a, alors, ouvert la voie à de nombreux auteurs qui ont repris cette doctrine. M. le Professeur M. Vivant, notamment, retient l'information comme « *vecteur de communication* »[32]. Au contraire, M. le Professeur J. Passa retient l'acte d'informer, l'information est alors « *[l'] action consistant à communiquer à un public des faits ou des opinions* »[33]. La notion d'information n'a, donc, pour l'heure, pas trouvé de consensus. Elle peut toutefois être définie comme « *un produit objectivé* » qui peut être « *doté d'une valeur économique* »[34]. En ce qui concerne le statut juridique de l'information, si « *certaines informations peuvent devenir des biens, […] d'autres restent à l'état de choses informationnelles* »[35]. M. le Professeur J. Passa considère ainsi que l'information est avant tout une chose sans s'attacher à la notion de communicabilité[36]. Il semble, néanmoins, que la valeur de l'information permette de la reconnaître comme un bien[37]. Par conséquent, le droit de propriété permet de « *protéger la confidentialité de l'information* »[38] et d'en réserver l'accès.

19- **Distinction des notions d'« information » et de « donnée ».** Si l'information est « *une séquence de signes pouvant être interprétés […] la donnée est [elle] une valeur variable* »[39]. Aussi, s'agissant de la donnée, lorsqu'elle est brute, et donc non traitée ou non analysée, elle ne peut être déchiffrée. Elle ne répond pas aux critères de communicabilité et de transmission de connaissance de l'information. Les données traitées ne sont, quant à elles, rien de plus qu'un

---

[29] CATALA, P., « Ébauche d'une théorie juridique de l'information » *RDD*, 1983, n°1, p. 185, *D.* 1984, chron. p. 975 ; CATALA, P., *Le droit à l'épreuve du numérique, Jus Ex Machina,* PUF, 1998.

[30] PASSA, J., « La propriété de l'information : un malentendu ? », Communication au colloque « Renouveau du droit de propriété ? » organisé par l'Université Lyon 2 en octobre 2000, *Droit et patrimoine*, n°91, mars 2001, pp. 64 à 72 : L'information est définie comme « *[l'] action consistant à communiquer à un public des faits ou des opinions* ».

[31] CATALA, P., *Les transformations du droit par l'informatique. Émergence du droit de l'informatique*, éd. Des Parques, 1983, pp. 264 et s.

[32] VIVANT, M., « La privatisation de l'information par la propriété intellectuelle », *RIDE,* 2006/4 (t. XX. 4).

[33] PASSA, J., « La propriété de l'information : un malentendu ? », *op. cit.*, p. 64, spéc. p. 65 ; AUBY, J.-M. et DUCOS-ADER, R., *Droit de l'information*, Dalloz, 1982, p. 1.

[34] BRUGUIERE, J.-M., *La diffusion de l'information publique. Le service public face au marché de l'information*, dir. VIVANT M., Montpellier, 1995, p. 5.

[35] BINCTIN, N., « Le statut juridique des informations non appropriées », *Légicom*, 2013/1, n°29 et s.

[36] GALLOUX, J.-C., « Ébauche d'une définition juridique de l'information » *D.*, 1994. Chron., n°26, p. 229.

[37] CATALA, P., « Ébauche d'une théorie juridique de l'information » *op. cit.*, 1983, p. 97 ; GALLOUX, J.-C., « Ébauche d'une définition juridique de l'information », *op. cit.*, n°29, p. 229, , MALLET-POUJOL, N, « Appropriation de l'information : l'éternelle chimère », *D.*, 1997, n°38, p. 330 ; DARAGON, E., « Étude sur le statut juridique de l'information », *D.*, 1998. Chron. n°7, p. 63.

[38] ZENATI, F., *La nature juridique de la propriété : contribution à la théorie du droit subjectif*, thèse, dir. RUBELLIN-DEVICHI J., Lyon III, 1981 ; d'autres moyens juridiques permettent toutefois de réserver l'information et la donnée, voir *infra*, n°303 et s.

[39] DELORT, P., *Le Big Data,* PUF, 2018, n°57 et 58.

contenu pour l'information[40]. Elles sont des choses immatérielles qui contiennent des informations.

Il semblerait donc que la « donnée » comme l'« information » soient des notions « fuyantes »[41]. Ce constat décourage certains auteurs à en trouver une définition n'en voyant tout simplement pas l'intérêt[42]. Par conséquent et à première vue, la notion d'« information » s'apparenterait à une notion générale dans laquelle il serait possible d'y ranger les données. Plusieurs textes de loi[43], mais aussi des textes européens[44] laissent ainsi entendre une synonymie entre ces deux notions[45]. Cette conception est, par ailleurs, reprise par de nombreux auteurs qu'ils soient publicistes[46] ou privatistes[47]. Par exemple, la directive 2003/98/CE du 17 novembre 2003 concernant les données ouvertes et la réutilisation des informations publiques[48] ne différenciait pas les données des informations. Le législateur européen n'évoquait dans cette directive la notion de « donnée » que pour se saisir des données personnelles[49]. Dans la doctrine, M. M. Boul affirme même que « *les données publiques sont d'abord des informations* » et « *[qu']il est d'ailleurs d'usage de considérer ces deux notions comme synonymes* »[50]. D'autres auteurs vont jusqu'à ignorer la catégorie des données brutes ou des données industrielles et ne retiennent que les données ayant fait l'objet d'un traitement[51]. Cette exclusion pourrait se justifier dans le secteur public qui n'utilise en réalité que les informations issues des données traitées au cours d'une mission de service public. Dans le secteur privé néanmoins, la distinction de ces deux notions est utile, voire fondamentale. Certains acteurs, en effet, détiennent des données brutes qu'ils n'exploitent pas nécessairement

[40] BOUL, M., « Réflexions sur la notion de donnée publique », *RFAP*, n°167, 2018/3, pp. 471 à 478.
[41] VIVANT, M., « La privatisation de l'information par la propriété intellectuelle », *RIDE*, 4, 2006, (t. XX, 4), pp. 361 à 388.
[42] LUCAS, A., *Le droit de l'informatique*, PUF, 1987, n°304 et seconde édition, LUCAS, A., DEVEZE, J. et FRAYSSINET, J., *Le droit de l'informatique*, PUF, 2001, n°470.
[43] Circ. 14 févr. 1994 relative à la diffusion des données publiques : *JORF* n°42 du 19 févr. 1994 : La donnée « … *sera entendue ici au sens large d'information collectée ou produite sur n'importe quel support, pas seulement informatique* » ; Arrêté du 22 décembre 1981 relatif à l'enrichissement du vocabulaire informatique, précité.
[44] Dir. 2003/98/CE du 17 nov. 2003 concernant la réutilisation des informations du secteur public : *JOUE* L 345/90 du 31 déc. 2003 ; BOUL, M., « Réflexions sur la notion de donnée publique », *op. cit.*, n°167, 2018/3, pp. 471 à 478.
[45] BOUL, M., « Réflexions sur la notion de données publiques », *op. cit.*, p. 473 : « *Les données publiques sont d'abord des informations* ».
[46] *Ibid.* : « *Les données publiques sont d'abord des informations* » ; ROUX, C., « La propriété publique à l'épreuve des données publiques », in AFDA, ss. dir., *Le droit administratif au défi du numérique*, 14-15 juin 2018, *D.S.*, 2019, p. 48 ; CLUZEL-METAYER, L., « La construction d'un service public de la donnée », *RFAP*, 2018/3, p. 495.
[47] SAINT-AUBIN, T., « Les nouveaux enjeux juridiques des données (*Big Data*, web sémantique et linked Data) Les droits de l'opérateur de données sur son patrimoine numérique informationnel », *RLDI*, 2015, p. 4.
[48] *JOUE* L 172/6 du 26 juin 2019.
[49] Dir. préc., art. 2., 5).
[50] BOUL, M., « Réflexions sur la notion de donnée publique », *op. cit.*, n°167, 2018/3, pp. 471 à 478.
[51] BRUGUIERE, J.-M., *Les données publiques et le droit,* Litec, 2002, p. 474.

parce qu'ils ne savent ou ne peuvent pas encore les exploiter. Cette réservation vise à conserver un monopole sur des données afin potentiellement d'en tirer toute la valeur d'usage dans le futur. Certains acteurs conservent donc les données brutes dans l'attente d'un futur usage potentiel, c'est ce que l'on appelle la « *valeur d'option* » des données. Aussi, la prise en compte de la notion de « données brutes » permet de proposer un régime juridique afin d'organiser leur protection, leur réservation ou, au contraire, leur circulation et leur partage.

Parvenir à la conclusion que la notion de « donnée » est synonyme de celle d'« information » aurait, en outre, d'importantes conséquences en termes de régime applicable aux données. En effet, l'information peut, dans certaines circonstances, être considérée comme un bien[52]. Or la donnée dans sa forme brute, c'est-à-dire lorsqu'elle est non traitée, non analysée n'est pas porteuse d'un message et ne semble pas pouvoir être confondue avec l'information[53]. C'est ainsi que certains auteurs publicistes n'ont pas manqué de relever que la prise en compte du terme « données » par le législateur a permis « *d'insister sur l'importance de l'informatique et subséquemment, sur la numérisation des ensembles détenus par l'État* »[54]. Si pour certains, « *la notion de donnée s'entend comme une information mise en forme pour être traitée informatiquement* »[55], pour d'autres, « *les notions d'information publique et de donnée publique ne se recouvrent toutefois pas entièrement en ce que les premières ne se transforment pas systématiquement en secondes. De même, les données publiques ne sont pas toutes exploitables. L'ouverture et la réutilisation des données dites brutes ou primaires ne sont réalisables que lorsqu'elles deviennent élaborées [c'est la] plus-value technique, intellectuelle ou documentaire [qui] permet d'en retirer les utilités* »[56]. Ce raisonnement peut être transposé aux données privées. La notion de « donnée » ne semble donc pas immédiatement synonyme à celle d'information, il faut d'abord en retirer les utilités, la rendre intelligible pour en tirer des informations exploitables.

Par conséquent, si les notions de données et d'informations peuvent sembler de prime à bord, similaires, incitant certains auteurs à conclure « *[qu'] une donnée est une information qui*

---

[52] CATALA, P., « La propriété de l'information », in Marty, G., ss. dir., *Mélanges offerts à P. Raynaud*, Paris, D.S., 1985, p. 97 ; GALLOUX, J.-C., « Ébauche d'une définition juridique de l'information », *op. cit.*, n°29 ; MALLET-POUJOL, N., « L'appropriation de l'information : l'éternelle chimère », *op. cit.*, n°38, p. 330 ; DARAGON, E., « Étude sur le statut juridique de l'information », *op. cit.*, n°7.

[53] DARAGON, E., « Étude sur le statut juridique de l'information », *op. cit.:* « *… l'information ne se confond pas avec le message, l'idée, la donnée, ou la connaissance, même si elle intervient d'une manière ou d'une autre dans leur définition* ».

[54] TERESI, L., *Droit de réutilisation et exploitation commerciale des données publiques*, Paris, La documentation française, CERIC, 2011, p. 113.

[55] BRUGUIERE, J.-M., *Les données publiques et le droit, op. cit.*, n°3.

[56] BOUL, M., « Réflexions sur la notion de donnée publique », *op. cit.*

est de principe de libre parcours »[57], elles reflètent de toute évidence deux réalités bien distinctes et ne sont donc pas synonymes[58]. Elles peuvent, dans certains cas, être les deux faces d'une même pièce[59]. Mme E. Daragon retient par ailleurs en ce sens que « *l'information ne se confond pas avec le message, l'idée, la donnée ou la connaissance, même si elle intervient d'une manière ou d'une autre dans leur définition* »[60]. L'information n'est donc pas toujours immédiatement et directement lisible à partir de la donnée chiffrée.

2. La circonscription de la recherche aux données agricoles

20- **La circonscription de la recherche suppose de déterminer exactement son objet.** L'étude porte sur les données produites ou collectées dans le cadre des activités du secteur agricole. Pourtant, la recherche ne peut se résumer aux données de l'agriculture numérique. En effet, les données de l'agriculture numérique sont celles qui sont collectées au moyen d'objets connectés, de robots ou encore de capteurs sur les exploitations agricoles[61]. Cette notion ne permet pas de prendre en compte les données collectées par d'autres moyens, tels que des questionnaires, des observations, ou encore, des enquêtes. Elle ne concerne pas non plus les données incluses dans une base de données et celles qui ont fait l'objet d'un traitement ultérieur.

Par ailleurs, ce travail de recherche ne porte pas non plus seulement sur les données des exploitations agricoles. Une telle notion ne permettrait pas d'envisager les données produites dans le cadre de la recherche ou encore les données de télédétection. L'objectif est donc d'englober l'ensemble des données produites ou collectées dans le secteur agricole. La notion de données agricoles recouvre donc les données produites dans le cadre d'une mission de service public ainsi que celles collectées au moyen d'objets connectés sur les exploitations agricoles, ou encore, les données de la recherche en agronomie, les données satellitaires, sans oublier les données traitées dans des logiciels de gestion et des bases de données agricoles. Par conséquent, afin de rassembler toutes ces acceptions dans une seule et même notion, il est convenu que le terme de « *donnée agricole* » est suffisamment générique pour toutes les recouvrir. L'épithète « agricole » fait donc référence à toutes les données collectées ou produites

[57] SAINT AUBIN, T., « Les nouveaux enjeux juridiques des données (*Big Data*, web sémantique et linked Data) Les droits de l'opérateur de données sur son patrimoine numérique informationnel », *op. cit.*, p. 4.
[58] BLAIZOT-HAZARD, C., « Données publiques et patrimoine immatériel des personnes publiques », Colloque – Circulation des données et propriétés intellectuelles, *PI*, avr. 2020, n°75, p. 24 ; BINCTIN, N., « Données et secret des affaires », Colloque – Circulation des données et propriétés intellectuelles, *PI*, avr. 2020, p. 43.
[59] BLAIZOT-HAZARD, C, *ibid.*, p. 64.
[60] DARAGON, E., « Étude sur le statut juridique de l'information », *op. cit.*, n°8.
[61] Voir *supra*, n°8 et s.

dans le secteur agricole que ce soit dans un cadre privé, public, scientifique ou encore à des fins de protection de l'intérêt général.

Néanmoins, il faut d'ores et déjà noter que s'agissant des questions portant sur la maîtrise de l'usage des données agricoles étudiées dans la deuxième partie, la recherche se concentrera plutôt de manière concentrique sur les données produites ou collectées sur les exploitations agricoles, c'est-à-dire les données de l'agriculture numérique. En effet, l'objectif étant d'envisager la maîtrise de l'agriculteur sur l'usage des données, celui-ci ne peut prétendre obtenir un droit de contrôle sur toutes les données agricoles, mais seulement sur celles qui sont issues de son exploitation ou qui y sont produites.

C. Les personnes gravitant autour des données agricoles

21- Afin d'identifier les personnes qui gravitent autour des données agricoles dans le marché de l'agriculture numérique, il faut nécessairement distinguer chacun des rôles que peuvent avoir ces différentes personnes. Tout d'abord, il y a la personne qui détient les données (**1**), puis celle qui les utilise (**2**), mais aussi, celle qui les produit ou les collecte (**3**).

1. La notion de détenteur de données

22- La notion de détenteur de données est définie dans la Proposition de règlement sur les données du 23 février 2022 comme « *une personne morale ou une personne physique qui […] a le droit ou l'obligation, ou, dans le cas des données à caractère non personnel et par le contrôle de la conception du produit et des services liés, a la possibilité de rendre disponibles certaines données à caractère personnel* »[62]. Le Règlement sur la gouvernance des données du 30 mai 2022[63], quant à lui, retient que l'utilisateur est la « *personne morale, y compris des organismes du secteur public et des organisations internationales, ou [la] personne physique qui n'est pas une personne concernée pour ce qui est des données spécifiques considérées, qui […] a le droit d'octroyer l'accès à certaines données à caractère personnel ou non personnel* ». Ces définitions ne sont pas en tout point similaires. Ce qu'il en ressort toutefois c'est que le détenteur ou possesseur des données est celui qui définit les modalités d'accès aux données

[62] Proposition de règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), COM(2022) 68 final, art. 2.
[63] *JOUE* L 152/1 du 3 juin 2022.

qu'il possède ou collecte pour le compte d'autrui[64] et qui en a le contrôle. Cette maîtrise peut être factuelle ou juridique. Le détenteur de données sera donc le plus souvent une entreprise qui possède les données en raison de son activité de collecte au moyen d'objets connectés ou par l'utilisation d'un logiciel ou d'une plateforme. Une personne physique peut également détenir des données dans son ordinateur, par exemple. En l'occurrence le détenteur de données dans le secteur agricole sera le plus souvent l'entreprise qui conçoit des produits connectés ou fournit des services numériques aux agriculteurs.

2. La notion d'utilisateur de données

23- L'utilisateur des données est tantôt défini comme la personne qui possède ou loue un produit ou reçoit un service[65] tantôt comme celle qui dispose d'un accès licite à certaines données et qui est autorisée à les utiliser à des fins commerciales ou non[66]. La notion de licéité de l'accès repose sur la base d'accords volontaires, tels que la souscription à une licence d'utilisation moyennant le paiement d'une redevance ou gratuitement. L'accès licite peut être fondé également sur une obligation légale, comme c'est le cas pour les données publiques par exemple. En revanche, dans la proposition de règlement sur les données de février 2022, le législateur définit l'utilisateur comme celui qui utilise le produit ou le service. C'est donc lui qui en principe souscrit un abonnement afin d'avoir accès aux données qu'il génère par l'utilisation qu'il fait des objets connectés ou des services liés.

24- Les deux notions d'utilisateur n'ont pas la même acception. Dans la Proposition de règlement sur les données, il s'agira le plus souvent de l'agriculteur qui utilise les objets connectés, les logiciels et autres plateformes. En revanche, dans le Règlement sur la gouvernance des données, l'utilisateur de données peut être toute personne qui a accès de manière licite aux données, qu'il s'agisse d'une personne publique, d'une personne morale de droit privé ou encore d'une personne physique. Les administrations, les entreprises de l'*AgTech*, les scientifiques, les agriculteurs, etc., peuvent donc tour à tour être considérées comme utilisateur de données, selon cette acception.

[64] CASSAR, B., « La gouvernance des données », *Dalloz IP/IT*, 2022, n°34.
[65] Proposition de règlement sur les données, préc., art. 2, 5).
[66] Règl. n°2022/868, préc., art. 2, 9).

3. Les notions de producteur et de collecteur de données

25- Deux autres notions ne sont pas expressément définies dans les réglementations de la Commission européenne, mais sont, toutefois, évoquées dans la Stratégie européenne sur les données[67]. Le producteur est celui qui produit les données au cours de son activité soit parce qu'il utilise un objet connecté, soit parce qu'il crée les données. C'est ainsi que les administrations, les entreprises de l'*AgTech*, les chercheurs et les agriculteurs peuvent une nouvelle fois être considérés tour à tour comme producteur de données, selon qu'ils créent ou non des données. Le collecteur de données est également évoqué dans la Stratégie européenne sur les données de la Commission européenne. Il peut être défini comme la personne qui collecte les données chez le possesseur ou le détenteur des données. Il faut noter, en outre, qu'une nouvelle notion a fait son apparition dans la doctrine, il s'agit de la notion de co-contractant générateur de données. Cette notion doit permettre d'identifier la personne qui détient des droits sur les données au cours d'une relation contractuelle. Elle fera l'objet d'un développement détaillé au cours de la recherche.

Il semble donc qu'une même personne peut se retrouver à la fois producteur, utilisateur, collecteur ou encore détenteur des données selon ses activités.

II. L'appréhension laborieuse du cadre juridique des données agricoles

26- « *La guerre des données agricoles aura-t-elle lieu ?* », cette question soulevée par l'Académie d'Agriculture de France (AAF) lors d'une séance hebdomadaire publique du 9 mars 2022[68] démontre l'importance que porte les acteurs du secteur agricole aux questions entourant l'accès et l'usage de leurs données. La matière du droit des données est en effet encore jeune et balbutiante, et s'avère particulièrement complexe à étudier tant les catégories de données et les règles qui leur sont applicables sont nombreuses et variées. Celles-ci ne cessent de s'accroître à mesure que de nouveaux défis concernant la protection de la vie privée, le développement économique ou encore la diffusion de l'information obligent le législateur à développer de nouvelles réglementations sur les données, créant ainsi un *patchwork* de droits. Or, pour le profane, bien souvent, le droit des données se réduit à celui des données à caractère personnel, une simple recherche Google suffit pour s'en convaincre. Cependant, de très nombreuses

[67] Commission européenne, *Une stratégie européenne pour les données*, COM(2020) 66 final, 19 févr. 2020.
[68] https://www.academie-agriculture.fr/actualites/academie/seance/academie/la-guerre-des-donnees-agricoles-aura-bien-lieu.

données collectées et produites dans le secteur agricole n'ont pas de caractère personnel et ne répondaient jusqu'à récemment à aucune réglementation. Or, en l'absence de législation c'est le contrat qui prend le relais et dans ce cas, bien souvent, c'est la loi du plus fort qui règne : selon la règle « premier arrivé, premier servi ». Comme un drapeau posé sur une terre encore vierge, le contrat et la réservation par la technique permettent alors aux entreprises, qui en ont les moyens techniques et financiers, de s'arroger de grands jeux de données. Elles affirment donc leur autorité sur les données qu'elles détiennent et elles imposent leurs conditions d'accès et d'utilisation à toute personne qui souhaiterait les obtenir et/ou les utiliser. La doctrine et la jurisprudence sont encore peu développées à ce sujet, il convient donc d'envisager, tout d'abord, l'évolution empirique de la législation encadrant ces données (**A**) pour étudier ensuite les effets du puzzle du droit des données (**B**).

A. L'évolution empirique de la législation sur les données agricoles

27- L'encadrement juridique des données se fait par étape selon les politiques et les intérêts en présence. En effet, à mesure que les données ont eu un impact dans la société, le législateur a souhaité encadrer leur accès. Le législateur français a, donc, établi le cadre de l'accès aux données publiques, celui des bases de données et enfin celui de la protection de la vie privée (**1**). Aujourd'hui, le législateur européen développe un cadre juridique pour la création d'un marché européen de la donnée (**2**).

1. L'appréhension de la donnée par le droit français

28- **De l'accès aux documents administratifs à la réutilisation des informations publiques.** Si, dans un premier temps, le législateur ne s'est intéressé qu'aux « documents administratifs »[69], il a par la suite élargi la notion aux « informations publiques », puis aux « données publiques ». En effet, à la fin des années 1970, le législateur a souhaité favoriser la transparence de la vie publique en facilitant l'accès aux documents administratifs. Ce souhait a permis de rompre « *avec la tradition bien établie du secret* »[70] qui régnait jusqu'alors au sein de l'Administration. Le mouvement a été impulsé en 1978 à travers deux dispositions législatives majeures. D'une

[69] CRPA, art. 300-2 : « *Documents produits ou reçus, dans le cadre de leur mission de service public, par l'État, les collectivités territoriales ainsi que par les autres personnes de droit public ou de droit privé chargées d'une telle mission* ».
[70] BOURCIER, D. et FILIPPI (De), P., *Open Data & Big Data, Nouveaux défis pour la vie privée*, mare & martin, 2016, p. 30.

part, la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite « Loi Informatique et Libertés » (LIL)[71], a pour objet de trouver un équilibre dans les rapports entre les administrés et les administrations et réglemente la liberté de traitement des données personnelles. D'autre part, la loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal dite « loi CADA »[72], offre un cadre légal au droit d'accès aux documents administratifs pour toute personne qui en exige la communication auprès de l'Administration concernée. En contrepartie, cette dernière doit assurer spontanément la diffusion de certains des documents sous forme électronique. De plus, comme le relève M. le Professeur J. Chevallier « *la publication n'étant qu'une simple faculté laissée aux administrations ; l'information est donc moins "portable" que "quérable"* »[73]. En effet, « *l'obligation de diffusion est l'exception* »[74] compensée par la faculté laissée aux personnes de pouvoir demander la communication des documents administratifs. En cas de litige, la juridiction compétente est la Commission d'accès aux documents administratifs (CADA). Ce dispositif a connu, par la suite, plusieurs modifications[75].

29. Le législateur a élargi le champ d'ouverture de la vie publique en employant la notion de « *réutilisation des informations publiques* » dès 2005. Cette modification du champ lexical proposait un changement de paradigme avec la transposition de la directive n°2003/98/CE du 17 novembre 2003 concernant la réutilisation des informations du secteur public (*Public Sector Information* ou PSI)[76] par l'ordonnance n°2005-650 du 6 juin 2005[77] relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques qui a modifié la

---

[71] *JORF* du 7 janv. 1978.
[72] *JORF* du 18 juill. 1978.
[73] CHEVALLIER, J., « Le droit français et la question des données publiques », in BOURCIER D. et FILIPPI (De), P., ss. dir., *Open Data & Big Data, op. cit.*, p. 32.
[74] BOUCHOUX, C., *Rapport d'information au nom de la mission commune d'information sur l'accès aux documents administratifs et aux données publiques*, Sénat, n°589, 5 juin 2014 (2 t.).
[75] Loi n°79-587, 11 juill. 1979, relative à la motivation des actes administratifs et à l'amélioration des relations entre l'administration et le public : *JO* n°160 du 12 juill. 1979 ; Décret n°81-860, 15 sept. 1981, portant codification des textes réglementaires concernant les procédures fiscales (deuxième partie : Réglementaire) : *JO* n°219 du 18 sept. 1981 en vigueur le 1er janv. 1982 ; Loi n°82-599, 13 juill. 1982, relative aux prestations de vieillesse d'invalidité et de veuvage : *JO* n°162 du 4 juill. 1982 ; Loi n°2000-321, 12 avr. 2000 relative aux droits des citoyens dans leurs relations avec les administrations : *JO* n°88 du 13 avr. 2000 ; Ord. n°2005-650, 6 juin 2005, relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques : *JO* n°131 du 7 juin 2005.
[76] *JOUE* L. 345/90, 31 déc. 2003, refondue par Dir. n°2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public : *JOUE* L 175/1 du 27 juin 2013 et par Dir. n°2019/1024, 20 juin 2019, concernant les données ouvertes et la réutilisation des informations publiques (refonte) : *JOUE* L 172/56 du 26 juin 2019.
[77] Ord. n°2005/650 du 6 juin 2005, relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques : *JORF* n°131 du 7 juin 2005.

loi CADA. Cette ordonnance a réuni « *l'accès et la réutilisation des données publiques dans la même loi [ce qui a permis] dès lors une simplification louable* »[78]. En termes sémantiques, les informations publiques sont considérées comme celles « *figurant dans les documents communiqués ou publiés par les administrations* »[79]. La notion ne s'éloigne donc pas vraiment de celle de « document administratif », la vraie révolution tient à la faculté de réutiliser les informations contenues dans ces documents « *par toute personne qui le souhaite* » et « *à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus* »[80].

30- Le développement du numérique et les enjeux de la digitalisation de la société ont conduit une nouvelle fois à un « *glissement sémantique* » de la part du législateur, « *l'accès aux documents administratifs [a] fait place à l'ouverture des données publiques* »[81]. Cet élargissement de l'amplitude des « choses » communicables a eu lieu dès 2011 avec la création de la mission *Etalab* chargée de créer un portail interministériel unique de données publiques : Data.gouv.fr. La mission devait aussi concevoir un dispositif juridique nouveau pour encadrer la politique d'ouverture[82]. Le gouvernement a ainsi posé les jalons de l'ouverture généralisée des données publiques. Ce souhait a, d'ailleurs, été retranscrit dans la Charte pour l'ouverture des données publiques des États du G8 du 18 juin 2013[83].

31- Avec la loi pour une République numérique du 7 octobre 2016[84], le législateur est allé encore un peu plus loin dans l'ouverture des données publiques en affichant la volonté de mettre en place « *un véritable service public de la donnée* »[85]. De cette manière, l'ouverture devient la règle et non plus l'exception[86]. Néanmoins, l'ouverture des données publiques « *n'a jamais obtenu le "label service public" de la part du législateur, alors même qu'elle en a sans doute tous les attributs* »[87]. La mission de service public est en effet limitée aux données de référence[88]. Mais de toute évidence, la façon dont a été conçu le régime de l'ouverture des

[78] MORALES, M., « La réutilisation des données publiques : le cas particulier de la culture », *RFDA*, 2018, p. 39. cite TABAKA, B., « De l'accès à la réutilisation : le nouveau régime applicable aux données publiques », *RLDI*, 2005, n°7, p. 46.
[79] CRPA, art. L.321-1 modifié par L. n°2016-1321 du 7 oct. 2016, préc.
[80] *Ibid.*
[81] BOUL, M., « Réflexions sur la notion de donnée publique », *RFAP*, n°167, 2018/3, pp. 471 à 478.
[82] CHEVALLIER, J., « Le droit français et la question des données publiques », *op. cit.*, p. 36.
[83] Charte du G8 pour l'Ouverture des Données Publiques, Irelande du Nord, 18 juin 2013.
[84] Loi n°2016-1321, du 7 oct. 2016 pour une République numérique : *JORF* n°0235 du 8 oct. 2016.
[85] PERRAY, R., « La loi pour une république numérique », *RLDI*, n°144, 1er janv. 2018.
[86]https://www.vie-publique.fr/eclairage/20301-loi-republique-numerique-7-octobre-2016-loi-lemaire-quels-changements.
[87] CLUZEL-METAYER L., « La construction d'un service public de la donnée », *RFAP*, 2018/3, n°167, p. 492.
[88] CRPA, art. L. 321-4.

données publiques par le droit d'accès et de réutilisation laisse transparaître un véritable service public de la donnée[89].

32- **La protection de la vie privée lors du traitement des données.** C'est, d'abord, en réponse au projet SAFARI[90] proposé par le ministre de l'Intérieur en 1973 qu'a été créée la Loi Informatique et Liberté (LIL). Ce projet avait pour objectif, telle une application de *Big Brother* dans *1983* de George Orwell, d'identifier chaque français et française, au moyen du croisement de différents fichiers administratifs. Dénoncé dans un article paru dans le journal Le Monde en 1974, le Gouvernement a pris l'initiative de créer la Commission informatique et liberté, devenue par la suite la Commission Nationale Informatique et Libertés (CNIL). Cette commission devait proposer un projet de loi visant à protéger la vie privée et les libertés publiques lors du développement de l'informatique. La Loi informatique et liberté est ainsi entrée en vigueur le 6 janvier 1978[91] et c'est à la CNIL qu'est revenue la mission de faire respecter son application. Par la suite la LIL a été refondue à plusieurs reprises, par différentes lois et directives[92]. Mais c'est avec l'adoption du « *Paquet européen sur la protection des données personnelles* »[93] que les modifications ont été les plus significatives. En effet, le Règlement Général sur la Protection des données[94] et la directive n°2016/680[95] ont contribué à un changement de paradigme. Dorénavant le Règlement européen repose sur une logique de responsabilisation renforcée des acteurs responsables de traitements et sous-traitements, alors que la Loi Informatique et Liberté reposait, en grande partie, sur une logique de formalités préalables. La loi pour une République Numérique du 7 octobre 2016[96] a, quant à elle, permis de prendre acte de l'évolution de la société vers le tout numérique, elle encadre l'innovation et

[89] MAISL H., « La diffusion des données publiques ou le service public face au marché de l'information », *AJDA*, 1994, spéc. p. 355.
[90] Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus (SAFARI).
[91] Loi n°78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés (LIL) : *JO* n°6 du 7 janv. 1978.
[92] Dir. n°95/46/CE du 24 oct. 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 : *JO* L 281 du 23 nov. 1995 ; Dir. n°2002/58/CE du 12 juill. 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) : *JO* L 201 du 31 juill. 2002.
[93] Si le RGPD est d'application direct en droit français depuis le 25 mai 2018, la Directive a dû, quant à elle, faire l'objet d'une retranscription. Il s'agit du « Paquet européen sur la protection des données personnelles ». Un projet de loi adaptant au cadre juridique européen la loi informatique et liberté a été adopté de manière définitive le 14 mai 2018 et le Conseil constitutionnel a jugé l'essentiel du texte conforme à la Constitution le 12 juin 2018.
[94] Règl. n°2016/679 du 27 avr. 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 : *JOUE* L 119/1 du 4 mai 2016.
[95] Dir. n°2016/680 du 27 avr. 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 : *JOUE* L 119/89 du 4 mai 2016.
[96] *JORF* n°0235 du 8 oct. 2016.

le développement de l'économie numérique en essayant de protéger au mieux les citoyens. Elle dispose, également, d'un volet données personnelles et renforce les droits des individus[97]. Aujourd'hui, la protection des données à caractère personnel est, en outre, en passe d'être protégée par la Constitution[98].

33- **La protection de l'investissement par le droit des bases de données.** Si le droit d'auteur protégeait déjà la base de données originale dans sa disposition, le législateur est venu accorder une seconde protection en faveur du producteur de la base de données. En 1996, le législateur a, en effet, créé le droit des producteurs de bases de données aussi appelé droit *sui generis*. L'objectif était de protéger l'investissement lors de la constitution de la base de données. Avec le développement des outils de collecte des données et de l'internet des objets, la question se pose, aujourd'hui, de savoir si les données créées par une activité principale lors de l'utilisation d'objets connectés par exemple peuvent bénéficier du droit *sui generis* des bases de données.

2. La volonté de créer un marché européen des données

34- **Direction du législateur européen.** La création du marché européen des données par le législateur européen se fait en plusieurs étapes. Tout d'abord, il a fallu poser les bases de la confiance dans l'échange et le partage des données. L'instauration d'un cadre solide est, en effet, essentielle afin de développer la confiance dans l'économie du numérique. C'est pourquoi, le législateur européen a pris acte du partage des données à caractère personnel et de leur utilisation par les entreprises, les pouvoirs publics et par les personnes physiques et a souhaité les encadrer. C'est donc le RGPD promulgué le 27 avril 2016[99] qui a permis de poser les jalons du futur marché européen des données. Cette volonté de la Commission européenne a été confirmée dans sa communication « *créer une économie européenne sur les données* » du 10 janvier 2017[100]. Pour compléter les bases de cette nouvelle économie, le législateur européen a, ainsi, adopté dans un premier temps trois textes, le premier porte sur la circulation des données à caractère non personnel[101], le second concerne la réutilisation des données

[97] Le droit à l'autodétermination informationnelle, le droit à l'oubli pour les mineurs, la possibilité d'organiser le sort des données personnelles après la mort, mais également, la possibilité d'organiser ses droits par voie électronique.
[98] FERAL-SCHUHL, C., ss. dir., *Cyberdroit, Le droit à l'épreuve de l'Internet*, Dalloz, 7e éd., 2018-2019, n°111.142.
[99] La loi n°2018-493 du 20 juin 2018, relative à la protection des données personnelles (1) : *JORF* n°0141 du 21 juin 2018 a mis en conformité la Loi Informatique et Libertés avec le Règl. n°2016/679 du 27 avr. 2016.
[100] COM(2017) 9 final.
[101] Règl. n°2018/1807 du 14 nov. 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne : *JOUE* L 303/59 du 28 nov. 2018.

ouvertes[102] et le troisième concerne la cybersécurité[103]. Ces trois règlements complètent le RGPD et constituent à eux quatre les piliers de l'économie européenne des données. Dans un second temps, en 2020, la Commission a précisé sa Stratégie européenne pour les données dans une nouvelle communication[104]. Plusieurs nouveaux objectifs ont alors été affichés par le législateur, il s'agissait de « *mettre en place un environnement attrayant pour parvenir à ce que, d'ici à 2030, la part de l'Union dans l'économie fondée sur les données corresponde au moins à son poids économique, non par le fruit du hasard, mais par choix* »[105]. Pour cela, les données doivent pouvoir circuler à l'intérieur de l'Union européenne et entre les différents secteurs. Les règles et les valeurs européennes, en particulier la protection des données à caractère personnel, la protection des consommateurs et le droit de la concurrence, doivent être pleinement respectées et les règles d'accès et d'utilisation des données doivent être à la fois équitables, pratiques et claires que des mécanismes de gouvernance des données claires et fiables soient en place : que les flux internationaux de données soient l'objet d'une approche ouverte, mais affirmée, fondée sur les valeurs européennes[106].

À la suite de cette communication, un premier Règlement a été proposé, le 25 novembre 2020 qui est la première grande étape de la stratégie européenne des données portant sur la gouvernance des données. L'objectif est de créer les procédés et les structures destinés à faciliter le partage des données par les entreprises, les particuliers et le secteur public, il a été approuvé par le Parlement européen et le Conseil en novembre 2021 et finalement adopté le 30 mai 2022[107]. S'agissant de la régulation des plateformes de partage des données, le législateur a également retravaillé la directive 2000/31/CE du 8 juin 2000 dite « commerce électronique »[108] et proposé un système de gouvernance européenne des plateformes au travers deux propositions de règlements, le *Digital Services Act* (DSA)[109] et le *Digital Market Act* (DMA)[110] en date du 15 décembre 2020. Finalement, le DMA a été approuvé par le Parlement européen le 11 juillet 2022. Enfin, la seconde grande initiative législative et la dernière en date

[102] Dir. n°2019/1024 du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public : *JOUE* L 172/56 du 26 juin 2019.
[103] Règl. n°2019/881 du 17 avr. 2019 relatif à l'ENISA (Agence de l'Union européenne pour la cybersécurité) et à la certification de cybersécurité des technologies de l'information et des communications : *JOUE* L 151/15 du 7 juin 2019.
[104] COM(2020) 66 final.
[105] *Ibid.*
[106] *Ibid.*
[107] JOUE L 152/1 du 3 juin 2022.
[108] *JOUE* L 178 du 17 juill. 2000.
[109] Proposition de règlement relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE du 15 déc. 2020, COM(2020) 825 final.
[110] Proposition de règlement relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques) du 15 déc. 2020, COM/2020/842 final.

résultant de la Stratégie européenne pour les données repose sur deux textes. D'abord, la Proposition de règlement sur les données du 23 février 2022, aussi nommé Acte sur les données ou *Data Act*[111]. Cette Proposition de règlement n'est pas encore promulguée et vient préciser qui peut créer de la valeur à partir des données et dans quelles conditions. Ensuite, le Règlement sur la gouvernance des données du 30 mai 2022[112], dont l'objectif est de créer les procédés et les structures destinés à faciliter le partage des données par les entreprises, les particuliers et le secteur public.

B. Les effets du puzzle du droit des données

35- L'ensemble des réglementations développées ces dernières années par le législateur crée un puzzle de droits des données qui répondent à différentes injonctions législatives (**1**). Aussi, les acteurs de l'agriculture numérique se sont concertés afin de s'autoréguler sur ces questions, ce qui complexifie un peu plus la matière (**2**).

1. Les injonctions législatives sur les données

36- Les données recouvrent des usages et des utilités si divers, que de nombreux régimes leur sont applicables, certains auteurs allant même jusqu'à nommer cet ensemble de réglementations : le « *puzzle du droit des données* »[113]. En effet, comme il l'a été vu plus haut, le droit des données s'étend de l'organisation de la circulation des données agricoles à celle de leur protection. Toutes ces réglementations peuvent s'appliquer à un moment ou à un autre aux données agricoles. Les acteurs doivent donc savoir composer avec l'ensemble de ces textes et répondre à des injonctions différentes, voire parfois contradictoires, selon leurs activités[114], le contenu des données[115] ou encore les intérêts en présence[116]. Le risque de telles contradictions de la part du législateur tient au fait que la lecture du droit ne soit pas suffisamment claire pour un profane et qu'un climat de confusion se crée pouvant entraîner, en outre, une réservation excessive des données.

---

[111] COM(2022) 68 final.
[112] Règl. n°2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement n°2018/1724 (règlement sur la gouvernance des données) : *JOUE* L 152/1 du 3 juin 2022.
[113] « Dossier : La libre circulation des données non personnelles : le contenu du principe », L'essentiel, *Dalloz IP/IT*, 2020, p. 400.
[114] Mission de service public, entreprise privée, scientifiques, etc.
[115] Informations personnelles, information d'intérêt général, etc.
[116] En termes concurrentielles (infrastructure essentielle) ou de diffusion de l'information (diffusion des données publiques), par exemple.

2. La part d'autorégulation sur l'exploitation des données agricoles

37- En l'absence de règles impératives, c'est le contrat, outil fondamental s'il en est dans les relations commerciales, qui prend le relais afin de tenir compte des spécificités de chaque secteur et de chaque relation. Afin de réglementer leur propre contrat, les acteurs de l'agriculture numérique ont proposé des textes de droit souple dans le but d'encadrer les pratiques commerciales pour une utilisation plus juste et équitable des données agricoles[117]. Les réglementations additionnées aux règles de droit souple créent un halo juridique autour des données agricoles qui complexifie un peu plus la matière. De plus, cette dernière étant relativement nouvelle, il existe encore peu de doctrine sur la question spécifique de l'encadrement juridique des données agricoles. Certains auteurs se sont néanmoins intéressés à la question[118].

III. L'élaboration d'un cadre adapté aux données agricoles

38- **Appareil méthodologique.** Ce travail de recherche a été ponctué par de nombreuses rencontres avec les différentes parties prenantes afin d'identifier leurs besoins et leurs requêtes. Notamment, les différentes rencontres avec les ingénieurs agronomes, les entreprises privées ou encore les artisans de la plateforme API-AGRO ont permis de cerner les difficultés entourant l'accès, la maîtrise et le partage des données agricoles. Il a alors été constaté que les agriculteurs ont pour principale exigence de conserver leur autonomie, les entreprises désirent quant à elles valoriser leurs investissements, tandis que les chercheurs souhaitent accéder aux données et les réutiliser pour la recherche et le développement. En outre, l'Administration doit répondre à son obligation de diffusion de l'information et les citoyens souhaitent avoir accès à celle-ci. En revanche, la loi du secret en raison de pratiques commerciales encore fragiles a complexifié la collecte de certaines informations et notamment celles entourant le contenu des contrats commerciaux.

---

[117] FNSEA et JA, *Valoriser et sécuriser les données des exploitations agricoles dans les contrats*, Charte Data-agri, 2018 et Copa Cogeca, *Code de conduite de l'UE relatif au partage des données agricoles par accord contractuel*, 2018.

[118] DOUVILLE, T., ss. dir., « Le droit des données agricoles », *Droit rural* n°469, janv. 2019, dossier 1 ; ALLEAUME C., « À propos de la propriété des données agricoles… », *idem*, dossier 2 ; CHONE-GRIMALDI, A.-S., « Données agricoles et droit de la concurrence », *id.*, dossier 3 ; DOUVILLE, T., « Contrat et données agricoles », *id.*, dossier 4 ; LEBRETON-DERRIEN, S., ss. dir., « Dossier - Agriculture numérique et droit », *Droit rural* n°479, janv. 2020, coll. 1 ; BEGUIN-FAYNEL, C., « La problématique de l'appropriation des données agricoles », *id.*, coll. 2 ; AUBIN-BROUTE, R.-J., « Le contrat pour la maîtrise des données agricoles », *id.*, coll. 3 ; GRUGER H., SOULIEZ, M. et LEBRETON-DERRIEN, S., « Pour une utilisation négociée et éthique des données agricoles : l'exemple de la Charte Data-agri », *id.*, coll. 4 ; JUILLET-REGIS, H., « Quelle régulation pour les données agricoles ? », *id.*, coll. 5.

L'étude du cadre juridique des données agricoles conduit à une recherche pluridisciplinaire et transversale. Tout d'abord, le droit de la propriété intellectuelle, le droit du numérique, le droit des biens, le droit public, ou encore, le droit des contrats et le droit pénal sont sollicités. Autant de matières qui intéressent l'accès et/ou la maîtrise des données. Cette recherche requiert également d'étudier l'économie des données afin de comprendre les effets du contrôle de l'accès et de la maîtrise sur le marché des données agricoles. Les sciences de gestion sont également sollicitées afin d'envisager les pratiques des nouveaux acteurs. La recherche fait, toutefois, l'impasse sur le droit international privé. En effet, les enjeux de l'extranéité concernant les conflits de juridictions et de lois afin de connaître l'ordre juridique applicable ne sont pas étudiés pour ne pas surcharger le travail de recherche concentré sur le droit français et européen. De même, le développement d'internet et de nouvelles technologies ont permis de développer une nouvelle discipline qu'est la cybersécurité. Ce domaine rassemble les lois, les politiques, les dispositifs et les mécanismes de sécurité permettant de protéger les personnes et le matériel des États et des organisations, appliqué au numérique. Cette thèse n'a pas vocation à développer cette question.

39. **Problématique générale.** Les enjeux apparaissent à mesure que l'agriculture se digitalise. Néanmoins, le droit positif ne parvient pas encore à répondre efficacement à toutes les questions soulevées. D'aucuns pourraient se demander si la solution finalement ne serait pas l'autorégulation afin de permettre aux acteurs du secteur de l'agriculture numérique d'encadrer eux-mêmes l'accès et l'usage des données qu'ils produisent et collectent. Toutefois, les enjeux qui naissent de ces activités, que ce soient en termes d'autonomie, de maîtrise de l'usage, de diffusion de l'information ou encore de protection de la vie privée semblent trop complexes pour se contenter d'un droit souple non contraignant. C'est pourquoi un encadrement par le droit positif semble opportun. Une réglementation adaptée permettrait, en effet, de considérer tous les intérêts en présence et de trouver un équilibre entre ces différents enjeux. Ceci éviterait, d'une part, de porter une atteinte excessive à l'accès et à l'utilisation des données, qui pourrait avoir pour conséquence de limiter le droit à l'information, mais aussi, la recherche et le développement. D'autre part, une meilleure prise en compte des intérêts de chacun dans la valorisation des données agricoles permettrait également d'éviter d'accorder une trop large ouverture à l'accès aux données. Un accès trop large aux données pourrait effectivement avoir pour effet de porter atteinte aux investissements et de créer un préjudice pour les agriculteurs. De même, définir précisément les règles du droit de contrôle des données permettrait de clarifier en amont les droits de chacun dans les relations contractuelles des acteurs de l'agriculture numérique. Finalement, le caractère nouveau du droit des données et le constat des dangers que

font naître la collecte et l'utilisation de ces données pour le secteur agricole nécessite de trouver un point d'équilibre entre les différents intérêts en présence afin de protéger à la fois la liberté d'information, l'investissement, la vie privée, la concurrence, etc. Ce travail de recherche ambitionne donc d'apporter une pierre à l'édifice à l'encadrement juridique des données agricoles. La question se pose alors de savoir quelles sont les conditions et les modalités d'accès et d'utilisation des données agricoles permettant de conserver un équilibre dans les relations entre les différents acteurs de l'agriculture numérique.

40- **Annonce de plan.** Les enjeux autour des questions sur la maîtrise de l'accès et de l'usage des données agricoles, mais aussi de la diffusion et de la protection de ces données sont tout à fait fondamentaux. En effet, l'objectif est de trouver un équilibre dans les relations commerciales entre les différents acteurs de l'agriculture numérique tout en répondant aux injonctions[119] du législateur qui sont à la fois de rendre accessibles et de valoriser certaines données, mais aussi, d'en protéger d'autres.

L'étude du régime juridique des données agricoles suppose d'étudier de manière spécifique et granulaire les différentes catégories de données de leur collecte à leur utilisation. L'encadrement des données agricoles doit alors être envisagé à deux étapes : celle de leur accès et celle de leur maîtrise.

Tout d'abord, une fois que les données sont collectées sur les exploitations, les personnes qui les détiennent en organisent l'accès. Si la culture du secret a depuis longtemps laissé la place à celle de la diffusion de l'information, il n'en demeure pas moins que cette ouverture ne concerne qu'une part infime des données agricoles, à savoir les données publiques et les données scientifiques dont les régimes particuliers seront développés. Au contraire, les données issues ou produites au cours d'activités privées sont de nature à rester confidentielles tant qu'aucun texte de loi ne contraint leur détenteur à les diffuser ou à les partager. Pourtant il semble que l'accès à certaines données de nature privée peut être nécessaire afin de répondre à des problématiques d'intérêt général ou commun. Par exemple, les informations sur l'utilisation des produits phytosanitaires ont un intérêt quant à leur impact sur l'environnement et sur la santé. La rétention de l'information peut ainsi parfois s'avérer délétère tant pour la réalisation de missions de services publics que pour la recherche, la santé publique, l'environnement, ou encore le libre jeu de la concurrence et la liberté d'information. La question de l'ouverture des données du secteur agricole apparaît alors comme un des piliers du cadre juridique des données

[119] PADOVA, Y., « Entre patrimonialité et injonction au partage la donnée écartelée (Partie I et II) », *RLDI*, n°155, 2019.

agricoles afin de les valoriser et suppose d'envisager leur catégorisation. Par conséquent, la question se pose de savoir qui peut avoir accès aux données, quel que soit leur niveau de traitement, et à quelles conditions. *A contrario*, la question de l'accès suppose également de s'intéresser à son corollaire, à savoir la réservation des données agricoles. En effet, plusieurs outils permettent à ceux qui les détiennent d'en réserver l'accès. Il s'agira alors d'envisager les différentes possibilités de réservation, leur validité et leurs effets. Cette recherche suppose de trouver un équilibre entre ouverture et réservation pour prendre en compte, à la fois, l'intérêt général et les intérêts particuliers de chaque acteur de l'agriculture numérique. La première partie sera donc consacrée à l'accessibilité des données agricoles (**Partie I**).

Ensuite, une fois les conditions de l'accès déterminées, il apparaît que cette question est préliminaire à celle plus problématique de la maîtrise de l'usage des données. En effet, une fois que sont définis les titulaires du droit d'accès et leurs modalités, la question se pose de savoir s'il est possible et envisageable de reconnaître un droit de contrôle de l'usage sur les données, et dans l'affirmative, il faut se demander qui pourrait détenir ce pouvoir de contrôle. En outre, si la question de la réutilisation des données publiques ne pose pas de grande difficulté, celle des données privées s'avère plus délicate. Le législateur a d'abord favorisé la libre circulation des données afin de créer un écosystème de partage dans lequel les plateformes sont les intermédiaires privilégiés, l'objectif étant de faciliter la circulation des données entre collecteurs, producteurs, utilisateurs, citoyens, etc. Néanmoins, la question se pose de savoir à quel point cet écosystème est efficient. Par ailleurs, les données à caractère non personnel souffraient jusqu'à récemment d'un manque de cadre juridique. En conséquence, les agriculteurs n'avaient aucun droit sur les données issues de leur exploitation, hormis celles revêtues d'un caractère personnel. Aussi, afin de définir les règles de contrôle d'utilisation des données, certains observateurs ont brandi le droit de propriété comme solution ultime à ce problème. La reconnaissance d'un tel droit permettrait assurément d'accorder purement et simplement les droits d'un propriétaire sur les données. Celles-ci seraient alors supposées appartenir tantôt au producteur ou générateur de la donnée, tantôt au collecteur ou encore à la personne qui est visée par la donnée. Néanmoins, de manière raisonnable, les syndicats du secteur agricole ont proposé des solutions alternatives à la propriété, parmi lesquelles se trouve l'obtention du consentement qui fait figure de proue de ce mouvement. En outre, l'étude de la maîtrise des données suppose d'en étudier les effets dans les relations contractuelles de l'agriculture numérique. Ainsi, ces dernières années, le législateur a pris en considération les différentes injonctions existantes sur les données afin de proposer un cadre juridique efficient

qu'elles aient un caractère personnel ou non. C'est pourquoi l'étude de la maîtrise des données implique d'envisager les évolutions du droit positif qui en constituent le terreau (**Partie II**).

Partie I. L'accessibilité des données agricoles

41.- De très nombreux acteurs gravitent autour des données agricoles. Tant l'Administration que les chercheurs ou encore les entreprises privées et les agriculteurs, eux-mêmes, trouvent un intérêt à obtenir, puis valoriser, ou même diffuser les données du secteur agricole. Aussi, le caractère polymorphe des données agricoles induit l'application de régimes juridiques différents qui peuvent s'avérer parfois contradictoires. D'une part, l'accessibilité aux données permet, entre autres, de répondre aux exigences de diffusion du savoir pour la recherche et de réalisation de mission de service public, d'autre part, leur privatisation permet notamment leur valorisation par les entreprises privées et assurent leur réservation. Par conséquent, la question de leur accessibilité suppose de s'interroger sur la maîtrise et l'organisation de l'accès aux données agricoles selon leur nature publique ou privée (**Titre I**). L'accès aux données agricoles n'est pas la règle, des outils techniques et juridiques permettent en effet de les réserver (**Titre II**).

Titre I. L'accès aux données agricoles : l'émergence d'un droit d'accès pour l'agriculteur

42- Le droit d'accès pensé comme une prérogative et non plus comme une exception doit « *permettre à ses bénéficiaires de prendre connaissance de données détenues secrètement ou protégées juridiquement par des tiers* »[120]. Ce changement de paradigme proposé par l'auteur permet d'envisager le droit des données en dehors du carcan de l'exclusivité. Il ne serait pas question pour autant d'accorder un accès gratuit et illimité aux données mais il serait nécessaire de prévoir des règles d'ouverture selon les bénéficiaires et la nature des données. Aussi, le droit d'accès doit être pensé comme un droit granulaire, de l'accès le plus large (données ouvertes) au plus restreint (secret des affaires). Afin d'éviter la loi du plus fort[121] et l'accaparement des données par les acteurs du numérique qui ont les moyens financiers et techniques d'en conserver une maîtrise exclusive, le droit d'accès est mis en avant comme un des moyens qui permettent de mieux répartir la valeur des données. Le premier chantier sur lequel a travaillé le législateur a été celui des données publiques. Aujourd'hui, l'attention se porte en particulier sur l'accès aux données privées[122]. Aussi, il convient de distinguer, dans un premier temps, l'accessibilité des données agricoles publiques (**Chapitre 1**) pour, dans un second temps, envisager l'accessibilité des données agricoles privées (**Chapitre 2**).

[120] GALLOUX, J.-C., « Libre propos sur le droit d'accès », colloque – circulation des données et propriétés intellectuelles, *PI*, juill. 2020, n°76, pp. 11 à 19.
[121] BENABOU, V.-L. et ROCHFELD, J., *À qui profite le clic ?*, éd. Odile Jacob, 2015, p. 57.
[122] Proposition de règlement du 23 février 2022 fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), COM(2022) 68 final . Voir *infra*, n°180.

Chapitre 1. L'accessibilité des données agricoles publiques

43- Certaines données collectées, traitées et diffusées dans le secteur agricole peuvent être qualifiées de données publiques, ce qui conduit à mener une étude sur le régime qui leur est applicable. Dans un premier temps, l'identification des données soumises au régime des données publiques suppose d'étudier la notion de données agricoles publiques (**Section 1**). Dans un second temps, une fois que les contours de la politique d'ouverture des données agricoles publiques auront été dessinés, il sera nécessaire d'envisager sa mise en œuvre (**Section 2**).

Section 1. La notion de données agricoles publiques

44- L'étude de la notion de données agricoles publiques doit, d'abord, passer par leur qualification **(§1**) pour, ensuite, en étudier l'origine (**§2**).

§1. *La qualification des données agricoles publiques*

45- Après avoir caractérisé les données publiques (**I**), il faudra déterminer précisément celles provenant du secteur agricole (**II**).

I. La caractérisation des données publiques

46- La première étape de la caractérisation des données publiques consiste à les définir (**A**), la seconde étape nécessite d'en connaître la nature juridique (**B**).

A. La définition de données publiques

47- Tout d'abord, il s'agit de se demander ce qu'on entend par « données publiques » (**1**). Ensuite, il sera question de connaître l'étendue de la catégorie des données publiques (**2**).

1. La spécificité des « données publiques »

48- **Notion de donnée publique.** La « donnée publique » est avant tout une « donnée ». Or, au vu de la difficulté de définir précisément ce qu'est une donnée[123], nous retiendrons, *a minima,* que la donnée est un contenu numérique renfermant des informations formatées. Un arrêté du 22 décembre 1981 relatif à l'enrichissement du vocabulaire informatique définit la « donnée » comme « *la représentation d'une information sous une forme conventionnelle destinée à faciliter son traitement* ». À la lecture de cet arrêté, certains auteurs retiennent que « *dans sa réalité plus élémentaire, la donnée est en quelque sorte l'"atome d'information", mais en fait le droit n'appréhende cette réalité qu'à partir du moment où elle* est *mise dans une forme permettant son traitement* »[124]. Cependant, les données brutes, non analysées, ne sont pas dénuées d'intérêt et représentent une certaine valeur pour les acteurs privés et les entités publiques qui les collectent. Or, la doctrine majoritaire[125] ainsi que la circulaire du 14 février 1994 relative à la diffusion des données publiques[126] estiment que les notions d'information et de données sont synonymes. Selon cette thèse, la donnée serait une information susceptible d'appropriation. Il apparaît néanmoins, après analyse, que ces deux notions ne sont pas équivalentes, puisque les données ne sont justement pas susceptibles d'appropriation[127].

L'épithète « public » vient en complément de la notion de « donnée » afin de préciser l'usage de ces données lors d'une mission de service public et désigne celles qui sont soumises à la politique de données ouvertes. Afin de déterminer l'impact de l'épithète « public » une fois accolé au terme « donnée », il faut rechercher sa définition. Or, ni la Loi pour une République Numérique de 2016 (LRN)[128], ni les directives successives encadrant la diffusion des informations publiques (PSI I, PSI II, PSI III)[129] n'ont apporté de définition à la notion de « donnée publique ». Aussi, il apparaît que cette notion est subséquente à celle de documents

---

[123] Voir *supra,* n°14 et s.

[124] AUBY, J.-B., « Données publiques-définitions. Principes. Orientation », fasc. 109-30, *JCP A*., 2018.

[125] AUBY, J.-B., « La réutilisation des données publiques », *AJDA,* 2011, n°8 à 9, p. 1 ; ROUX, C., « La propriété publique à l'épreuve des données publiques », in AFDA, ss. dir., *Le droit administratif au défi du numérique, D.S.*, 2019, pp. 43 et s. ; SCHMALTZ, B., *Les personnes publiques propriétaires*, préf. SESTIER, J.-F., Nouv. Bibl. de Thèse, Dalloz, 2016.

[126] Circ. 14 févr. 1994, relative à la diffusion des données publiques : *JORF* n°42 du 19 févr. 1994 qui retient que la donnée « … *sera entendue ici au sens large d'information collectée ou produite sur n'importe quel support, pas seulement informatique* ».

[127] Pour une étude détaillée sur la question, voir *infra,* n°504 et s.

[128] Loi n°2016-1321 du 7 oct. 2016 pour une République numérique (LRN) : *JORF* n°0235 du 8 oct. 2016.

[129] Dir. 2003/98/CE du 17 nov. 2003 concernant la réutilisation des informations du secteur public : *JOUE* L 345/90 du 31 déc. 2003 (PSI I) ; Dir. 2013/37/UE du 26 juin 2013 modifiant la directive 2003/98/CE concernant la réutilisation des informations du secteur public : *JOUE* L 175/1 du 27 juill. 2013 (PSI II) ; Dir. n°2019/1024 du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public : *JOUE* L 172/56 du 26 juin 2019 (PSI III).

administratifs, comme définie à l'article 1er de la loi CADA transposée à l'article L. 300-2 du CRPA : sont donc considérés comme documents administratifs « *les documents produits ou reçus dans le cadre de leur mission de service public, par l'État, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission* ». Mais « *les dispositions encadrant l'ouverture de l'accès des données publiques issues de la LRN ont eu pour effet d'accroître la liste des objets susceptibles, comme les bases de données, de donner lieu à diffusion et ne plus faire du seul document administratif "l'alpha et l'oméga" du dispositif "données publiques"* »[130]. Également, la directive PSI III retient la notion de « données ouvertes » dans son intitulé, elle ne concerne plus seulement la réutilisation des informations du secteur public, mais concerne désormais également les données ouvertes définies comme « *les données présentées dans un format ouvert qui peuvent être librement utilisées, réutilisées et partagées par tous, quelle qu'en soit la finalité* »[131]. La reconnaissance d'une telle notion doit encourager les politiques d'ouverture des données avec « *une large disponibilité et réutilisation des informations du secteur public à des fins privées ou commerciales* »[132]. Les documents étant eux-mêmes définis comme « *a) tout contenu quel que soit son support (papier ou forme électronique, enregistrement sonore, visuel ou audiovisuel) ; ou, b) toute partie de ce contenu* ». En outre, si la notion de « donnée publique » semble étroitement liée à celle de documents administratifs, telle que définie par le CRPA, il apparaît néanmoins que cette idée « *n'est plus tout à fait conforme à la réalité* » puisque des données publiques peuvent être produites ou coproduites par « *des acteurs qui n'ont pas nécessairement de lien avec l'administration* »[133].

2. L'étendue de la catégorie des données publiques

49- **Différentes catégories de données publiques**. L'obligation de communication du CRPA s'étend à quatre objets. D'abord, les « *documents que les administrations communiquent en application […]* » du droit d'accès du public aux documents administratifs[134]. Pour cela, les documents doivent être disponibles sous forme électronique et ils ne doivent pas être non communicables en vertu des articles L. 311-5 et L. 311-6 du CRPA. Ensuite, l'obligation de

[130] ROBIN, A., *Droit des données de la recherche, Science ouverte, innovation, données publiques*, Larcier, 2022, n°220, p. 169.
[131] Dir. PSI III, préc., cons. 16.
[132] *Ibid.*
[133] CLUZEL-METAYER, L., « La construction d'un service public de la donnée », *RFAP*, 2018/3, n°167, p. 495.
[134] CRPA, art. L. 312-1-1, 1e.

communication s'applique aux données de référence introduites par la loi n°2016-1321 pour une République numérique du 7 octobre 2016 et codifiées à l'article L. 321-4 du CRPA. Elles sont définies comme « *des informations publiques figurant dans des documents communiqués ou publiés par les personnes publiques qui peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus* »[135]. Trois conditions cumulatives permettent de qualifier les données de référence[136] : il doit s'agir d'informations publiques qui constituent une référence commune pour nommer ou identifier des produits, des services, des territoires ou des personnes. Elles doivent être réutilisées fréquemment par des personnes publiques ou privées autres que les administrations qui les détiennent. Leur réutilisation nécessite qu'elles soient mises à disposition avec un niveau élevé de qualité. Elles sont listées à l'article R. 321-5 du CRPA et leurs modalités de mise à disposition sont contenues aux articles R. 321-6 et suivants du même code. Ce sont bien des données publiques, mais recouvertes d'une sorte de « *label lié au service public* »[137], ainsi les données de référence sont gages de qualité[138].

L'obligation de communication s'applique également aux bases de données des administrations[139]. Deux conditions cumulatives permettent de savoir si les bases de données doivent être publiées ou non. D'une part, les bases de données peuvent être produites ou reçues par les administrations. Il ne s'agit donc pas seulement des bases de données dont l'Administration est à l'origine, cette obligation concerne également les bases de données qu'elle reçoit au cours de ses activités de service public. D'autre part, ces bases de données ne doivent pas avoir fait l'objet d'une diffusion publique par ailleurs. Il est alors inutile de publier une base de données qui a déjà fait l'objet d'une diffusion afin d'éviter les doublons. Enfin, l'Administration doit répondre à une obligation qui est de mettre à jour régulièrement les bases de données qu'elle publie. Cette dernière obligation concerne les données dont la publication présente un intérêt économique, social, sanitaire ou environnemental[140]. Par conséquent, les personnes morales de droit privé ou public exerçant une activité de service public qui détiennent des données dont le contenu présente un de ces intérêts doivent les diffuser.

---

[135] CRPA, art. L. 321-4 et L. 321-1.
[136] CRPA, art. L. 321-4.
[137] TRUCHET, D., « Nouvelles récentes d'un illustre vieillard : label de service public et statut de service public » *AJDA*, 1982, p. 427.
[138] VERDIER, H., *La donnée comme infrastructure essentielle*, Rapport au premier ministre sur la donnée dans les administrations 2016-2017 de l'AGD, *La documentation française*, 2018, p. 16 : « *[…] puisque toutes les données publiques ne se valent pas et que certaines présentent un potentiel d'usage plus élevé que d'autres* ».
[139] CRPA, art. L. 312-1-1, 3e.
[140] CRPA, art. L. 312-1-1, 4e.

50- **Catégorie spéciale des données d'intérêt général**. Il faut noter, dès à présent, l'existence d'une catégorie particulière qui sort du cadre des données publiques et de l'obligation de communication développées ici, il s'agit des données d'intérêt général[141]. À la différence des données publiques issues du service public, les données d'intérêt général ont une provenance de nature privée, elles le sont pour la plupart dans le cadre de concessions[142] ou dans le cadre de missions de service public et commercial[143]. Mais « *en raison de leur intérêt pour améliorer les politiques publiques* »[144], elles doivent, également, être ouvertes[145].

B. La nature juridique des données publiques

51- Afin d'envisager la nature juridique des données agricoles publiques, il faut se demander si elles entrent dans la catégorie des biens publics. C'est pourquoi il est nécessaire, d'abord, d'étudier la catégorie des biens publics (**1**) pour, ensuite, comprendre l'exclusion des données agricoles publiques de cette catégorie (**2**).

1. La notion de bien public

52- Comme pour chaque objet de droit, la notion de « bien public » doit nécessairement passer par sa définition. Aussi, faut-il s'intéresser, avant tout, au « bien » pour ensuite analyser les conséquences de son épithète « public ». Aucun consensus n'a pour l'heure été trouvé sur la notion de bien. La doctrine s'accorde au moins sur un élément : « *un bien est avant tout une chose* »[146]. La chose est donc le préalable de la notion de bien, mais elle ne suffit pas pour acquérir ce statut, elle doit répondre à plusieurs conditions établies par la doctrine. Mais avant d'aller plus en amont, la question se pose de savoir si la doctrine civiliste s'applique aux biens des personnes publiques. Ainsi, le droit de propriété des personnes publiques comporte-t-il des spécificités par rapport à celui des personnes privées ? Certains évoquent l'idée que le droit de propriété serait un concept privatif « *nullement [...] pensé pour les administrations* »[147].

---

[141] Voir *infra*, n°141 et s.
[142] LRN, art. 17 ; CRPA, art. 53-1.
[143] LRN, art. 18, art. 10 de la loi n°2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations : *JORF* n°88 du 13 avril 2000.
[144] https://www.economie.gouv.fr/republique-numerique-ouverture-donnees-d-interet-general ; https://www.vie-publique.fr/eclairage/20301-loi-republique-numerique-7-octobre-2016-loi-lemaire-quels-changements
[145] Voir *infra*, n°154 et s.
[146] CHAMARD-HEIM, C., *La distinction des biens publics et des biens privés : contribution à la définition de la notion de biens publics*, préf. INTERMAIER, J., Dalloz, Nouv. bibl. de thèses, t.33, 2004, n°329, p. 234.
[147] YOLKA, P., « Les patrimoines publics à l'épreuve de la propriété intellectuelle », *AJDA*, prat. 1, 2012.

Néanmoins, il est, aujourd'hui, admis que « *le droit de propriété liant les personnes publiques et leurs biens [est] de même nature que celui des personnes privées et que le régime domanial n'interv[ient] que dans un second temps* »[148]. Par conséquent, « *les biens publics sont objets de propriété* »[149]. Il s'agit d'ailleurs d'un droit protégé par le Conseil constitutionnel sous l'égide de l'article 17 de la Déclaration des droits de l'homme et du citoyen qui prévoit que « *la propriété étant un droit inviolable et sacré, nul ne peut en être privé* ». Il semble donc que les théories civilistes sur l'appropriation des biens s'appliquent également à ceux appartenant aux personnes publiques. Par conséquent, et pour en revenir à la notion de bien, au moins deux éléments doivent être réunis pour qualifier une chose de bien : cette chose doit être susceptible d'appropriation et cette appropriation doit être utile à l'Homme et ce, que la chose soit publique ou privée[150]. Concernant l'utilité à la personne, la chose doit satisfaire ses besoins, « *soit directement en les utilisant, soit indirectement en les échangeant contre d'autres choses* »[151]. D'autres auteurs ajoutent, comme conditions, la circulation de la chose ou encore sa valeur économique[152]. Au contraire, certaines choses ne font pas l'objet d'un droit de propriété puisqu'elles sont utiles à l'usage de tous, il s'agit des choses communes qui ne peuvent jamais entrer dans la catégorie des biens[153] et dont la notion n'est pas figée[154]. S'agissant de l'exercice du droit de propriété, la chose doit pouvoir faire bénéficier à son propriétaire d'un droit réel, ce qui se traduit par un droit exclusif et un droit absolu sur celle-ci. Le droit réel permet au propriétaire de disposer de la chose comme il l'entend et son droit est opposable à tous par opposition aux droits personnels, relatifs. Enfin, son droit ne peut entrer en concurrence avec celui d'un tiers.

Si le bien public est donc *a priori* une chose appropriable, qu'en est-il des effets de l'épithète « public » ? Comme on l'a vu, il semble que l'utilisation de l'adjectif « public » est en réalité un abus de langage. Qu'ils soient publics ou privés, les biens restent des biens et répondent toujours à la même définition, « *la notion de bien ne se limite donc pas aux autres choses qui sont la propriété des personnes privées, elle est indépendante de la nature juridique*

---

[148] AUBY, J.-B., BON, P. et TERNEYRE, P., *Droit administratif des biens*, Dalloz, 8e éd., 2020, p. 303.
[149] *Ibid*., n°22, p. 21.
[150] *Idem* ; voir PLANIOL et RIPERT, *Traité élémentaire de droit civil*, 1e éd., t.1, L.G.D.J, 1939, n°2170 et CARBONNIER, J., *Droit civil*, t.3, *Les biens*, PUF, 2017, n°1 et 6.
[151] *Ibid*.
[152] LIBCHABER, R., « Le portefeuille de valeurs mobilières : bien unique ou pluralité de biens ? », *Defrénois*, 1997 n°8, 9 et 66.
[153] Voir *infra*, n°361.
[154] BRUGUIERE, J.-M., MALLET-POUJOL, N. et ROBIN, A., ss. dir., (équipe ERCIM) *Propriété intellectuelle et droit commun*, Université Paul Cézanne Aix-Marseille III, Presses Universitaires d'Aix-Marseille, 11/2007.

de la personne qui peut s'en rendre propriétaire »[155]. Le fait d'y ajouter l'adjectif « public » détermine simplement la personne qui en est effectivement propriétaire puisque les biens publics sont la propriété des personnes publiques. Par conséquent, le domaine public et le domaine privé relèvent de la même condition d'appropriation, même si cela peut parfois être contesté[156]. Néanmoins, « *le bien public se caractérise par l'idée d'une affectation des biens à l'usage de tous* »[157] et non pas aux organes de l'État. De plus, certaines caractéristiques des biens publics les distinguent des biens privés puisqu'ils sont insaisissables[158] et ne peuvent être cédés en dessous de leur valeur[159]. Ceci est dû au fait que l'essence même du droit administratif était en première intention de protéger le patrimoine matériel public.

2. L'exclusion des données publiques de la catégorie des biens publics

53- **Données publiques, biens publics ?** Concernant la question de l'appropriation des données publiques, au début du XXe siècle, a été discutée la notion de « patrimoine-but », conçue en Allemagne et développée en France par M. L. Duguit. Cette conception est l'antagoniste de la conception personnaliste d'Aubry et Rau. Il s'agit de la théorie selon laquelle « *l'Administration assure la garde et le contrôle des données publiques et surtout selon [laquelle] elle peut les exploiter sans en avoir la propriété* »[160]. Le problème de cette théorie vient du fait que l'Administration serait tenue d'utiliser ce pouvoir de contrôle, puisque la notion de « patrimoine-but » nécessite « *une compétence liée dans la gestion de la chose* »[161]. La compétence liée s'oppose au pouvoir discrétionnaire qui offre à l'Administration une marge de manœuvre dans l'exécution de ses pouvoirs. Aujourd'hui, la doctrine publiciste s'appuie sur l'idée selon laquelle les données ont une valeur et sont commercialisables, ce qui aurait pour

---

[155] MARCHAND, J., *Recherche sur le régime des actions et participations financières publiques,* préf. RAPP L., LGDJ, Bibl. de droit public, t. 219, 2014, n°331, p. 236.
[156] MOYSAN, H., *Le droit de propriété des personnes publiques*, L.G.D.J., Bibl. de droit public, 2001.
[157] ROCHFELD, J., « Entre propriété et accès : la résurgence du commun », in BELLIVIER, F., ss. dir., *La Bioéquité,* Autrement, Frontières, 2009, p. 75.
[158]Civ. 1ère, 21 déc. 1987, *Bureau de recherches géologiques et minières (BRGM)*, n°86-14.167, Bull. civ. 1987, I, n°348, p. 249 ; concl. CHARBONNIER L. et note PACTEAU B., *RFDA* 1988. 771 ; note RICHER L., *CJEG* 1988. 107 ; note VERON O., *Gaz. Pal.* 1988, II, 685 ; note NICOD B., *JCP* 1989, II, 21183 ; note PERROT R., *RTD civ.* 1989. 145 ; note YOLKA Ph., *GDDAB*, Dalloz, 2013, n°75, p. 663.
[159]Cons. const., 26 juin 1986, décision n°86-207, DC, *Loi autorisant le Gouvernement à prendre diverses mesures d'ordre économique et social* : *JORF* du 27 juin 1986 ; Rec., p. 61 ; note RIVERO J., *AJDA 1986*. 575 ; chron. AVRIL P. et GICQUEL J., *Pouvoirs*, 1987, n°40, p. 178 ; chron. FAVOREAU L., *RD publ.* 1989. 399 ; FAVOREAU L. et PHILIP L., S. 1989. 659-682 ; note CHAMARD-HEIM C., *GDDAB* 2013. 644 ; note FAVOREAU L. et PHILIP L., *D.* 2009. 514 ; note GENEVOIS B., *Annuaire int. de just. const.*, 1986, pp. 427 et 454 ; note GUYON Y., *RDS* 1986. p. 606 ; note AMADEI J.-P., *LPA*, 1995, p. 19 ; AUBY J.-B., « La réutilisation des données publiques », *AJDA*, 2011.
[160] CAMUS, A., « La propriété des données publiques », *op. cit.*
[161] *Ibid.*

conséquence de les rendre appropriables[162]. Certains auteurs affirment même avec vigueur l'existence d'un droit de propriété sur les données par la personne publique[163]. Pour exemple, sur la question de la commercialisation des données publiques, M. le Professeur J.-B. Auby, peut-être un brin provocateur, affirme que des données publiques même sans droit d'auteur, mais qui ont une valeur économique, seraient commercialisables et pourraient donc être considérées comme un bien public : « *si celles-ci ont une valeur économique, si elles sont parfois commercialisables, c'est qu'elles sont des biens non ? Étant des biens, et des biens publics, elles doivent être d'une façon ou d'une autre gouvernées par le droit de la domanialité* »[164]. Il n'en reste pas moins que la donnée seule peut ne pas avoir de valeur et n'est donc pas appropriable. Au contraire, c'est un ensemble d'éléments qui permet de créer de la valeur et un modèle économique, par l'agglomération, le traitement, les accès ou encore les utilités de la donnée. Ainsi, il semblerait que la donnée soit un objet à part entière qui ne doit pas être confondu avec l'information. Elle suit son propre régime. Pour autant, si les données brutes ne sont pas des œuvres de l'esprit et ne peuvent pas faire l'objet d'un droit de propriété[165], il n'en va pas de même pour les données élaborées ou enrichies[166]. C'est pourquoi des données organisées dans une base de données peuvent parfaitement faire l'objet d'un droit de propriété au titre du droit d'auteur ou du droit *sui generis*[167]. D'ailleurs, c'est ce qu'avait admis pour les personnes publiques, le Conseil d'État dans l'avis *Ofrateme*[168] de 1972 dans lequel les juges ont constaté l'existence d'un droit d'auteur sur les informations produites et organisées par le service public[169]. Cet avis a conduit à l'adoption de la loi n°2006-691 du 1er aout 2006 qui a permis de reconnaître le droit d'auteur du créateur de l'œuvre, tout en réservant *de facto* à l'Administration des droits quant à la divulgation et l'exploitation des œuvres. De même, dans l'arrêt *Cegedim*[170], les juges se sont rattachés à la notion d'œuvre de l'esprit pour reconnaître

---

[162] CAMUS, A., « La propriété des données publiques », *RFDA*, 2018/3, n°167.

[163] SCHMALTZ, B., *Les personnes publiques propriétaires*, *op. cit.*, n°449, p. 374 ; BLAIZOT-HAZARD, C., « Données publiques et patrimoine immatériel des personnes publiques », *op. cit.*, p. 34 : « *La réflexion ne doit pas porter sur la propriété qui demeure, mais sur les droits qui en découlent […] Il semble plus juste de parler de domaine, de propriété des personnes publiques, affecté à la fonction générale […]* ».

[164] AUBY, J.-B., « La commercialisation des données publiques », rep., *RFDA*, n°11, 2002.

[165] CA Paris, 1e ch., sect. conc., 18 mars 1993, *Sté du journal téléphoné*, n°92/1499 ; note DRAGO R., *RJC*, 1993. 320 ; note COUSIN A, *Gaz. Pal.*, 9 juill. 1993, p. 317.

[166] DAVID BEAUREGARD-BERTHIER (de), O., « Le patrimoine immatériel de l'État », *Bien public, Bien commun, Mélanges en l'honneur d'Etienne Fatôme*, Dalloz, 2011, p. 23.

[167] Voir *infra*, n°218 et s.

[168] CE, avis, 21 nov. 1972, *Ofrateme*, pourvoi n°309721 : comm. KUPERFILS G., *GACE*, 2e éd., Dalloz, 2002, p. 105 ; comm. YOLKA Ph., *GDDAB*, Dalloz, 2e éd., 2015.

[169] TARLET, F., *Les biens publics mobiliers*, thèse, Lyon 3, préf. CAUDAL S., Nouv. Bibl. de Thèse, vol. 170, Dalloz, 2017, n°749, p. 517.

[170] CE, 29 juill. 2002, *Sté Cégédim*, pourvoi n°200886 : *Rec*. p. 280 ; note NICINSKI S., *AJDA* 2002, p. 1072 ; obs. GONZALEZ G., *Dr. adm.* 2002, p. 901 ; note BAZEX M. et BLAZY S., *Dr. adm.* 2002, 13 ; note et comm. BRUGUIERE J.-M., *JCP E* 2003. 149 ; concl. MAUGÜE C., *AJDA* 2004, veille p. 166 ; note SCHMIDT-SZALEWSKI J., *PI*, 2004.

les données publiques comme des biens appropriables notamment au sujet de la base de données « INSEE » : « *l'État peut percevoir des droits privatifs à l'occasion de la communication des données publiques en vue de leur commercialisation lorsque cette donnée peut être regardée, au sens des lois sur la propriété littéraire et artistique, comme une œuvre de l'esprit* ». Ainsi, la jurisprudence exigeait que les données publiques soient organisées en base de données pour détenir un droit de propriété sur les données. Toutefois, des évolutions textuelles[171] et un revirement de jurisprudence ont modifié cette analyse[172]. Désormais les administrations ne peuvent plus se prévaloir de leur droit de propriété intellectuelle sur bases de données qu'elles créent dès lors que celles-ci contiennent des données publiques[173].

De plus, depuis la Loi pour une république numérique de 2016[174], les données publiques font l'objet d'une obligation de diffusion spontanée et doivent donc être ouvertes. Selon le CNNum[175], le régime des données publiques qui implique une mise à disposition à titre gratuit peut laisser entendre qu'il s'agit de choses communes. Par conséquent, les données publiques sont exclues de la propriété publique[176], ainsi « *les données en elles-mêmes ne sont pas objets de propriété* »[177]. Ce défaut d'appropriation fait naître un risque pour la puissance publique de perdre la main sur l'exploitation économique des données qu'elle produit[178].

54- **Données publiques, patrimoine immatériel de l'État ?** Au vu des éléments précédemment développés, l'absence de droit de propriété sur les données publiques interroge sur leur intégration dans le patrimoine immatériel de l'État. Il s'agit, alors, de se demander si l'appropriation est une condition d'intégration du bien dans le domaine public[179]. Cette condition d'appropriation transparaît jusque dans le titre du Code organisant les règles

28 ; note LUCAS A., *PI* 2003. 57 ; MALAURIE-VIGNAL M., *CCC*. 2003. 12 ; chron. BOITEAU C., *JCP* 2002. 2278 ; LATREILLE A., *Dr. et patr*. 2007. 28 ; note BOISSE (de) H., *Expertises*, 2003. 23 ; HOURSON S., RGD. 2008. 1.

[171] Loi n°2015-991 du 7 août 2015 portant la nouvelle organisation territoriale de la République (loi NOTRe) : *JORF* n°0182 du 8 août 2015 ; Loi n°2015-1779 du 28 déc. 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public (loi Valter) : *JORF* n°0301 du 29 déc. 2015 ; Loi n°2016-1321 du 7 oct. 2016 pour une République numérique (LRN) : *JORF* n°0235 du 8 oct. 2016.

[172] CE, 8 févr. 2017, n°389806, *Sté Notrefamille.com* : Rec ; *AJDA* 2017. 318 ; obs. LARRIEU J., LE STANC C. et TREFIGNY P., *D.* 2017. 2390, ; obs. DREYFUS J.-D. *AJCT* 2017. 350 ; obs. LAMBOT, *JCP Adm*. 2015, 2239.

[173] Pour une analyse plus détaillée, voir *infra*, n°120.

[174] Loi n°2016-1321 du 7 oct. 2016 pour une République numérique (LRN) : *JORF* n°0235 du 8 oct. 2016.

[175] CNNum, *Ambition numérique, Pour une politique française et européenne de la transition numérique*, 2015, p. 276.

[176] ROUX, C., « La propriété publique à l'épreuve des données publiques », in AFDA, ss. dir., *Le droit administratif au défi du numérique*, 14-15 juin 2018, D.S., 2019, p. 43.

[177] AUBY, J.-B., BON, P. et TERNEYRE, P., *Droit administratif des biens*, Dalloz, 8e éd., 2020, p. 22.

[178] ROUX, C., « La propriété publique à l'épreuve des données publiques », in AFDA, ss. dir., *Le droit administratif au défi du numérique*, 14-15 juin 2018, D.S., 2019, pp. 43 à 44.

[179] AUBY, J.-B., « La réutilisation des données publiques », *op. cit.*, n°8 et 9, p. 1.

applicables aux biens publics[180] : Code général de la Propriété des Personnes Publiques (CGPPP). Si elle est aujourd'hui largement admise[181], certains auteurs retiennent néanmoins la thèse selon laquelle les choses ne peuvent relever du domaine public que lorsqu'elles sont affectées à un service public[182]. De prime abord, le CGPPP ne prend pas en compte les biens incorporels du domaine public[183], il a plutôt vocation à protéger ce qui est utile au service public que ce qui en est issu. Mais il faut relever que, depuis quelques années, nous assistons à une « *valorisation du patrimoine immatériel public* »[184]. Les biens immatériels prennent de plus en plus d'importance pour l'État[185] ainsi que les résultats de la recherche en cas de propriété[186]. C'est pourquoi deux décrets du 10 février 2009 ont aménagé la rémunération de certains services rendus par l'État[187] et, en particulier, la valorisation de son patrimoine immatériel[188]. Preuve de l'importance apportée au patrimoine immatériel, l'Appui au Patrimoine Immatériel de l'État (APIE)[189] a été créé à cette occasion et a pour mission de promouvoir une gestion optimisée des actifs immatériels publics[190]. De plus, le patrimoine d'une personne n'est pas constitué que de biens. Aussi, si les droits sur les bases de données sont « *indiscutablement des éléments du patrimoine immatériel des personnes publiques* »[191], la valorisation des données, en dehors de toute base, ne saurait écarter la question préalable de leur statut afin de déterminer leur domanialité[192].

---

[180] BLAIZOT-HAZARD, C., « Données publiques et patrimoine immatériel des personnes publiques », *op. cit.*, p. 24 ; BRUGUIERE, J.-M., « Le patrimoine immatériel de l'État est-il l'objet d'une propriété publique ? », *CDST*, 2010, n°3, pp. 59 à 73.

[181] AUBY, J.-B., BON, P. et TERNEYRE, P., *Droit administratif des biens*, *op. cit.*, n°82, pp. 76 et s.

[182] LEONETTI, R., « La protection de l'affectation au service public des biens incorporels », *AJDA*, 2009, n°1689.

[183] AUBY, J.-B., « L'immatériel dans l'État », repère 6, *AJDA*, juin 2007, p. 1 ; YOLKA, P., « Les meubles de l'administration », *AJDA*, 2007, p. 964 ; BRUGUIERE, J.-M., « Le patrimoine immatériel de l'État est-il l'objet d'une propriété publique ? », *op. cit.*

[184] MALWE, C., « La valorisation du patrimoine immatériel de l'État », *AJDA*, n°4, avr. 2009, comm. 52 ; DREYFUS, J.-D., « La valorisation par l'État de son patrimoine immatériel », *AJDA*, 2009, n°696 ; DAVID BEAUREGARD-BERTHIER, (de) O., « Le patrimoine immatériel de l'État », *op. cit.*, p. 27 ; TERNEYRE, P., « Les actifs immatériels des personnes publics », *RJEP*, étude 16, 2013, p. 6 ; YOLKA, P., « Le droit de l'immatériel public », *AJDA*, 2017, p. 2047 ; LEVY M. et JOUYET, J.-P., *L'économie de l'immatériel, la croissance de demain*, La documentation française, 2007 ; BLANCHET, P.-A., *La valorisation du patrimoine immatériel des personnes publiques*, thèse, ss. dir., BRACONNIER, S., Paris, 2018, publié éd. L'Harmattan, 2020.

[185] AUBY, J.-B., « L'immatériel dans l'État », *op. cit.*, p. 1.

[186] ROBIN, A., « Le patrimoine scientifique de l'État : un patrimoine immatériel en quête de statut », *CCE*, n°10, oct. 2014, ét. 18 ; FORT, F.-X. et ROBIN, A., « Remarques sur le régime de gestion de la propriété industrielle entre personnes publiques », *AJDA*, 2010, p. 2292 ; ROBIN, A., *Droit des données de la recherche - Science ouverte, innovation, données publiques*, Larcier, 2022, pp. 45 et s.

[187] AUBY, J.-B., « L'immatériel dans l'État », *op. cit.*, p. 70.

[188] MALWE, C., « La valorisation du patrimoine immatériel de l'État », *op. cit.*, comm. 52.

[189] Avant le 1er janv. 2020, Agence du Patrimoine Immatériel de l'État (APIE).

[190] APIE, *le patrimoine immatériel public : une ressource pour moderniser et créer de la valeur*, rapport d'activité 2018 sur www.economie.gouv.fr. : l'APIE définit les données comme des actifs stratégiques pour les acteurs privés et pour les entités publiques.

[191] BLAIZOT-HAZARD, C., « Données publiques et patrimoine immatériel des personnes publiques », *op. cit.*, p. 33.

[192] LEONETTI, R., « La protection de l'affectation au service public des biens incorporels », *op. cit.*, p. 1689.

II. La détermination des données agricoles publiques

55- Parmi les données produites dans le cadre d'une mission de service public, les données agricoles peuvent être produites directement par les organismes publics ou bien collectées auprès de personnes privées. Il convient d'envisager, dans un premier temps, les données produites dans le cadre d'une mission de service public (**A**) puis, dans un second temps, les données produites dans le cadre de la recherche scientifique (**B**).

A. Les données produites dans le cadre de missions de service public

56- Le ministère de l'Agriculture et de l'Alimentation (MAA) détient à lui seul un patrimoine de données de plus de trois cents jeux de données comptabilisés en 2018 dans le dernier plan de transformation numérique[193]. Il serait donc vain d'essayer d'être exhaustif. Néanmoins, quelques exemples peuvent être relevés. Pour cela, les données agricoles publiques seront classées selon leur utilité. Deux catégories de données publiques seront envisagées : d'abord, celles produites ou collectées dans le cadre d'une mission de service public à des fins de statistiques (**1**), ensuite, celles collectées ou produites à des fins d'information (**2**).

1. Les données produites à des fins de statistiques

57- Parmi les données collectées et produites par le ministère de l'Agriculture et de l'Alimentation, nombre d'entre elles sont produites à des fins de statistiques par l'Agence de Service et de Paiement (ASP). Il s'agit d'un établissement public interministériel qui contribue à la mise en œuvre des politiques publiques. Cet organisme diffuse notamment des données de référence : les données cadastrales et parcellaires agrémentées par les données déclarées chaque année par les agriculteurs. Ces données permettent de suivre et d'évaluer les politiques agricoles dans le cadre de la Politique Agricole Commune (PAC). Ensuite, elles sont diffusées dans une base de données géographique, le Registre Parcellaire Graphique (RPG), administré par l'Institut National de l'Information Géographique et Forestière (IGN) qui sert notamment à l'instruction des aides de la politique agricole commune (PAC). Également, le Service de la Statistique et de la Prospective (SSP) a pour mission d'établir chaque année des statistiques sur les cheptels

[193] CDC, *Les données du ministère de l'agriculture et de l'alimentation : un potentiel à mieux explorer*, 2020, p. 126 ; https://www.ccomptes.fr/system/files/2020-02/20200225-RPA-2020-tome-II.pdf.

ovins, caprins et porcins[194], ou encore sur les pratiques culturales qui impliquent notamment de relever les informations générales sur l'application des traitements phytosanitaires[195]. De plus, tous les dix ans, le SSP procède au recensement agricole général auquel les exploitants agricoles ont l'obligation de se soumettre en vertu de la loi n°51-711 du 7 juin 1951[196]. Le recensement agricole est donc une enquête obligatoire qui sert à des fins statistiques et permet de collecter des données sur les parcelles concernant l'occupation du sol, les cheptels et les exploitations. Ces données sont par la suite publiées dans la base de données Agreste. D'autres organismes produisent des données à des fins de statistiques, c'est le cas par exemple de l'Agence Bio ou encore de FranceAgriMer.

2. Les données produites à des fins d'information

58- Certaines données sont soumises à une politique d'ouverture sur l'impulsion d'une obligation réglementaire à des fins de transparence. Premièrement, les données sur la composition nutritionnelle des aliments et des productions « bio » doivent être publiées afin de respecter l'obligation d'information des consommateurs. Ces données sont publiées par l'Anses dans la table Ciqual[197]. Secondement, les données environnementales ont été réglementées après la Convention Aarhus sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement, entrée en vigueur le 30 octobre 2001, et la directive 2003/4/CE du 28 janvier 2003 concernant l'accès du public à l'information en matière d'environnement[198]. Ces données sont également soumises au principe général de diffusion des données publiques dans un objectif de transparence. Les données environnementales sont toutes celles contenant des informations citées à l'article L.124-2 du

[194] Dir. comm. 93/23/CEE (statistiques sur le cheptel et la production du secteur porcin) et 93/25 (statistiques sur le cheptel et la production du secteur des ovins et des caprins) ; abrogées et remplacées par le Règl. n°1165/2008 du 19 novembre 2008 concernant les statistiques du cheptel et de la viande : *JOUE* L 321/1 du 1e déc. 2008.

[195] SOLEILHAVOUP, M. et CRISAN, M., *Enquête Pratiques culturales en grandes cultures et prairies 2017* – Principaux résultats (version modifiée), actualisée le 24 juin 2020, https://agreste.agriculture.gouv.fr/agreste-web/disaron/Chd2009/detail/

[196] Loi n°51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques : *JO* du 8 juin 1951.

[197] Règl. n°1169/2011 du 25 oct. 2011 concernant l'information des consommateurs sur les denrées alimentaires : *JOUE* L 304/18 du 22 nov. 2011 ; Règl. n°1337/2013 du 13 déc. 2013 portant modalités d'application du règlement n°1169/2011 du Parlement européen et du Conseil en ce qui concerne l'indication du pays d'origine ou du lieu de provenance des viandes fraîches, réfrigérés et congelées des espèces ovine, caprine, porcine et des volailles : *JOUE* L 335/19 du 14 déc. 2013 ; Décret n°2015-447 du 17 avr. 2015 relatif à l'information des consommateurs sur les allergènes et les denrées alimentaires non préemballées : *JORF* n°0092 du 19 avr. 2015 ; Décret n°2014-1489 du 11 déc. 2014 modifiant le code de la consommation en ce qui concerne notamment l'information des consommateurs sur les denrées alimentaires : *JORF* n°0287 du 12 déc. 2014.

[198] Transposée en droit français par la Loi n°2005-1319 du 26 oct. 2005 portant diverses dispositions d'adaptation au droit communautaire dans le domaine de l'environnement : *JORF* n°251 du 27 oct. 2005.

Code de l'environnement[199]. Elles sont définies comme celles contenant des informations « *décrivant des objets localisés à la surface de la Terre (réseaux routiers, bâtis, végétation, etc.) par leur géométrie et certaines de leurs propriétés (taille, fonction, etc.) les données localisées sont manipulées dans des systèmes d'information géographique (SIG) : système informatique de matériels, de logiciels et de processus conçus pour permettre la collecte, la gestion, la manipulation (traitement, analyse) et l'affichage de données à référence spatiale* »[200]. Dans cette même veine, une réglementation européenne a imposé aux administrations de publier leurs données environnementales géographiques[201]. Ce sont les données les plus publiées par les collectivités territoriales, elles permettent des initiatives citoyennes et collaboratives[202]. Elles sont encadrées par la directive européenne du 14 mars 2007 dite INSPIRE[203] qui vise à établir une infrastructure d'information géographique pour favoriser des politiques environnementales communautaires et des politiques ou des activités de la Communauté susceptibles d'avoir une incidence sur l'environnement. Afin de répondre à cette obligation, plusieurs services ont été mis en place. D'abord, un service de recherche sur le site *Géocatalogue* mis en œuvre par le Bureau de recherches géologiques et minières (BRGM), ensuite un service de consultation sur le site *Géoportail* mit à disposition par l'Institut national de l'information géographique et forestière (IGN).

---

[199] « *Est considérée comme information relative à l'environnement au sens du présent chapitre toute information disponible, quel qu'en soit le support, qui a pour objet : 1° L'état des éléments de l'environnement, notamment l'air, l'atmosphère, l'eau, le sol, les terres, les paysages, les sites naturels, les zones côtières ou marines et la diversité biologique, ainsi que les interactions entre ces éléments ; 2° Les décisions, les activités et les facteurs, notamment les substances, l'énergie, le bruit, les rayonnements, les déchets, les émissions, les déversements et autres rejets, susceptibles d'avoir des incidences sur l'état des éléments visés au 1° ; 3° L'état de la santé humaine, la sécurité et les conditions de vie des personnes, les constructions et le patrimoine culturel, dans la mesure où ils sont ou peuvent être altérés par des éléments de l'environnement, des décisions, des activités ou des facteurs mentionnés ci-dessus ; 4° Les analyses des coûts et avantages ainsi que les hypothèses économiques utilisées dans le cadre des décisions et activités visées au 2° ; 5° Les rapports établis par les autorités publiques ou pour leur compte sur l'application des dispositions législatives et réglementaires relatives à l'environnement* ».

[200] NOUCHER, M. et GAUTREAU, P., « Le libre accès rebat-il les cartes ? Nouvelles perspectives pour les données géographiques », *LCN*, 2013/1, vol. 9. p. 57.

[201] Ord. n°2010-1232 du 21 oct. 2010 portant diverses dispositions d'adaptation au droit de l'Union européenne en matière d'environnement : *JORF* n°0246 du 22 oct. 2010, ratifiée par la loi n°2011-12 du 5 janv. 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne (1) : *JORF* n°0004 du 6 janv. 2011, a transposée la dir. n°2007/2/CE du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE) : *JOUE* L 108/1 du 25 avr. 2007 ; C. env., art. L. 127-1 à L. 127-10.

[202] PLANTIN, J.-C. et VALENTIN, J., « Données ouvertes et cartographie libre, Autour du cas de Montpellier », *LCN*, 2013/1, vol. 9, pp. 85 à 107.

[203] Dir. 2007/2/CE du 14 mars 2007 établissant une infrastructure d'information géographique dans la communauté européenne (INSPIRE) : *JOUE* L 108/1 du 25 avr. 2007.

B. Les données produites à des fins de recherche scientifique

59- Tout d'abord, il convient d'envisager la notion de données scientifiques (**1**) pour, ensuite, envisager leur régime spécial (**2**). Néanmoins, la production de données agricoles publiques n'est pas l'apanage de la seule administration et de la recherche scientifique ou industrielle[204]. Des initiatives citoyennes et participatives sont à l'origine de projets visant à la création et à la mutualisation de données dans le but également de produire de la connaissance. Il conviendra donc d'envisager également les initiatives citoyennes et participatives (**3**).

1. La notion de données de la recherche scientifique

60- **Qualification des données scientifiques.** Les organismes de la recherche publique produisent des données à des fins de recherche scientifique, environnementale et de développement territorial ainsi que pour leurs applications à la gestion et aux politiques publiques. Les données de la recherche scientifique, sans être qualifiées de données publiques[205], sont toutes les données issues ou produites lors d'activités de recherche[206]. La Loi pour une république numérique de 2016 ne définit pas le terme de données scientifiques, « *ou plus exactement, des données issues d'une activité de recherche* »[207]. L'étude d'impact du projet de la LRN définit les données de la recherche comme « *des données factuelles issues d'observations d'enquêtes de corpus, d'archives et d'expériences ou d'analyses computationnelles, enregistrées sous tout format et sur tout support dans une forme brute ou après avoir été traitées ou combinées, et sur lesquelles se fondent les raisonnements du chercheur et qui sont jugées nécessaires à la validation des résultats de la recherche* »[208]. Le terme « factuel » renvoie aux données « brutes »[209]. En effet, Mme A. Robin retient que la donnée brute est une « *donnée non*

---

[204] JOLY, P.-B., « Recherches scientifiques et recherches industrielles », *in Construire la recherche avec la société civile : les enjeux de la démarche d'intermédiation*, Cahiers de l'action n°55, juill. 2020, pp. 47 à 54.
[205] BLAIZOT-HAZARD, C., « Données publiques et patrimoine immatériel des personnes publiques », *op. cit.*
[206] Pour le choix étymologique voir ROBIN, A., *Droit des données de la recherche - Science ouverte, innovation, données publiques, op. cit.*, pp. 19 à 21. *Id.*, « Les données scientifiques au prisme du dispositif *Open Data* » *CCE*, 2017, n°9 (ét. 14).
[207] ROBIN, A., « Valorisation de la recherche scientifique, propriété intellectuelle, innovation », chr., *CDST*, 7/2017.
[208] LRN, art. 30 codif. C. rech., art. L. 533-4-II ; l'OCDE dans ses Principes et lignes directrices pour l'accès aux données de la recherche financée sur des fonds publics définit les données de la recherche comme telle : « *les données de recherche sont définies comme des enregistrements factuels (chiffres, textes, images et sons), qui sont utilisés comme sources principales pour la recherche scientifique et sont généralement reconnus par la communauté scientifique comme nécessaires pour valider des résultats de recherche. Un ensemble de données de recherche constitue une représentation systématique et partielle du sujet faisant l'objet de la recherche* ».
[209] AZZI, T., « *Open Data* et propriété intellectuelle », *D.*, n°11, 2017 ; ROBIN, A., « Les données scientifiques au prisme du dispositif *Open Data* », *op. cit.*

travaillée et non mise en forme (au sens du droit d'auteur) et donc non appropriable »[210]. Toutefois, cette notion recouvre également les données qui ont fait « *l'objet d'un premier travail de "purification", de "nettoyage" […] ou d'"appauvrissement" des données, afin qu'elles soient rendues lisibles par des systèmes informatiques et qu'elles puissent ensuite donner lieu à une analyse et une exploitation* »[211].

Par conséquent, toutes les données produites ou issues des activités de recherche du secteur agricole sur les exploitations seront soumises à l'*Open Access*. L'accès ouvert (ou accès libre) désigne « *le projet d'ouvrir les savoirs à tous les publics, sans contrainte économique ou juridique* ». L'objectif est « *de mettre la ressource scientifique en accès libre et ouvert* »[212]. Sont soumises à ce régime notamment les données météorologiques, les données sur les caractéristiques des sols, les données géographiques ou encore cadastrales produites lors d'activité de recherche par des instituts ou des établissements de recherche. Pour schématiser les données de la recherche scientifique sont donc celles qui passent entre les mains des instituts et des établissements de recherche (INRAE, CIRAD, etc.) du secteur agricole. Il faut relever des régimes particuliers pour les données environnementales (Aarhus) et les données géographiques (INSPIRE). Par exemple, les données satellitaires produites par le projet *Equipex-Geosud* coordonné par l'INRAE sont des données géographiques dont le régime repose à la fois sur la directive de 2019, relative à la réutilisation des données du secteur public et sur la directive INSPIRE de 2007, relative à l'interopérabilité des données géographiques[213].

2. Le régime spécial des données de la recherche scientifique

61- **Zone grise des données scientifiques.** Les données scientifiques se situent dans une zone grise entre les biens publics et les communs. En effet, les publications de la recherche peuvent être présentées comme des **«** *communs susceptibles d'appropriations non souhaitables, permises par le fait que leur accès peut faire l'objet d'un prix* »[214]. D'un côté, leur utilisation est non

[210] ROBIN, A., *Droit des données de la recherche - Science ouverte, innovation, données publiques, op. cit.*, n°102, p. 88.
[211] *Ibid.*
[212] ROBIN, A., « Accès ouvert (*Open Access*) », in CORNU M., ORSI F. et ROCHFELD J., ss. dir., *Dictionnaire des biens communs*, PUF, 2017, pp. 20 à 24, spéc. 21.
[213] Dir. 2007/2/CE du 14 mars 2007 établissant une infrastructure d'informations géographique dans la communauté européenne (INSPIRE) : *JOUE* L 108/1 du 25 avr. 2007, p. 1.
[214] BENHAMOU, F., « L'*Open Access* domaine des communs éditoriaux. Du modèle encastré au modèle émancipé », *in* CORIAT B., BANCEL J.-L., ALIX N., SULTAN, F., ss. dir., *Vers une République des biens communs*, LLL, 2018, p. 145.

rivale et non exclusive, ce qui correspond aux caractéristiques des biens publics. De l'autre, le partage des données scientifiques s'inscrit dans la mission de diffusion de la connaissance.

62- **Communs scientifiques.** Les communs scientifiques sont issus des travaux de Science Commons eux-mêmes issus des réflexions de Benkler[215] et de Lessig[216]. Les communs scientifiques sont régis par le contrat qui « *constitue la figure majeure de la régulation de la maîtrise des ressources, incitant d'autres auteurs, comme Judith Rochfeld, à parler de "commun contractuel", en référence à l'accord de volontés institué entre personnes souhaitant mettre en commun des biens et ressources susceptibles de faire l'objet d'une appropriation privative et qui préside à leur gouvernance* »[217]. Ainsi, l'*Open Access* des revues scientifiques répond à deux objectifs selon Mme la Professeure F. Benhamou, le premier consiste en la démocratisation, c'est-à-dire à « *l'accès au plus grand nombre aux résultats des travaux de recherche* » et le second, au « *rayonnement de la recherche dans un contexte de forte concurrence internationale entre universités* ». D'ailleurs, la notion de « commun » a été un temps, envisagée dans le projet de loi pour une République numérique, mais elle n'a pas été reprise dans la loi définitive.

63- **Données scientifiques et bien commun.** Le mouvement du partage des données s'inscrit dans « *une tendance communautaire qui considère l'information publique comme un bien commun, tel que défini par Elinor Ostrom dont la diffusion est d'intérêt commun et non d'intérêt public ou d'intérêt général* »[218]. Ceci s'explique par l'importance dans la communauté scientifique de partager les connaissances pour faire évoluer la recherche. « *Au-delà du droit c'est donc à l'éthique, à la fois pré-droit ou soft law, qu'il faut s'intéresser* »[219]. Pour Mme D. Bourcier, « *la notion de communs scientifiques ne concerne plus l'accès aux données, mais de nouvelles formes de partage de données* ». Aussi, *Creative commons* a été créé en 2001 en Amérique du Nord afin de diffuser des plateformes de *Commons* numérique à travers le monde. Pour cela, les auteurs adoptent de nouvelles règles du jeu, *Soft law,* qui sont efficaces pour la visibilité et la circulation des œuvres[220].

---

[215] BENKLER, Y., « Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain », *74 New York University Law Review* 354, 1999.
[216] LESSIG, L., « Code and the Commons », Keynote, *Conference on Media Convergence*, Fordham Law School New York, NY, Fevruary 9, 1999 : cyber.law.harvard.edu/works/Lessig/Fordham.pdf. ; BOURCIER, D., « Réflexion éthique sur le partage des données en science : entre communs scientifiques et *Open Data* », *in* BOURCIER, D. et FILIPPI (De), P., ss. dir., *Open Data & Big Data*, 2016, p. 219.
[217] ROBIN, A., « Communs scientifiques » in CORNU, M., ORSI, F. et ROCHFELD, J., ss. dir., *Dictionnaire des biens communs*, PUF, 2017, pp. 316 à 318, spéc. p. 316.
[218] *Ibid.*
[219] *Ibid.*, p. 233.
[220] Voir *infra*, n°436 et s.

En ce qui concerne la « science ouverte », elle vise à aller au-delà même de l'accès ouvert aux résultats de la recherche en facilitant une réutilisation non seulement des données et de l'information, mais aussi des données brutes et des outils, logiciels et ontologies[221]. Néanmoins, le partage et le libre accès aux travaux et données scientifiques ne sont pas souhaités par tous. Certains voudraient au contraire favoriser « *l'efficacité et la rationalité économique* » contre la « *qualité de la recherche* »[222]. Aussi, la communauté scientifique a été instigatrice du partage des données qu'elle produisait ou recevait[223]. En effet, les chercheurs ont depuis longtemps partagé les résultats de leurs recherches afin de favoriser les avancées de la Science. La spécificité de la recherche tient au fait qu'elle repose sur le partage des connaissances et la certification par les pairs. Aussi, les établissements de recherche publient des jeux de données brutes, « *Data paper* », sous forme d'articles examinés par les pairs, soit dans une revue scientifique classique, soit *via* une plateforme de stockage et d'édition de données (ex. HumaNum)[224], l'objectif étant de rendre les jeux de données lisibles et réutilisables à l'aide des métadonnées[225]. Cependant, les éditeurs ont cherché à profiter de la démocratisation d'internet pour mettre en ligne les publications des chercheurs et à augmenter les coûts tarifaires. C'est en réaction à ces pratiques que les chercheurs ont souhaité favoriser l'accès à leurs recherches. Comme l'écrit Mme la Professeure C. Bernault : « *C'est parce que les éditeurs commerciaux ont cherché à profiter du numérique pour accroître leur contrôle sur les publications et augmenter les tarifs des abonnements que les chercheurs ont souhaité, en réaction, favoriser l'accès de tous à leurs recherches* »[226]. Les données produites ou issues des activités de recherche n'étaient alors pas concernées par le dispositif *Open Access.* Ce dernier n'avait en effet vocation qu'à encadrer les écrits scientifiques[227]. Finalement, la pratique a développé la

[221] La question fait l'objet d'un projet de recherche #Commondata porté par la Maison des sciences de l'Homme de Montpellier dirigé par Mme A. Robin, commencé en 2018, dont la problématique est : « *les données de la recherche : des communs scientifiques ?* ». L'objectif est « *d'engager une réflexion collective entre différents champs disciplinaires de la communauté scientifique montpelliéraine (agronomie, informatique, écologie, environnement, santé…), sur les dimensions juridiques et sociales des données scientifiques et sur les pratiques des chercheurs et institutions » ;* https://doranum.fr/2018/07/13/le-projet-commondata-les-donnees-de-la-recherche-des-communs-scientifiques/

[222] BENHAMOU, F., « L'*Open Access*, domaine des communs éditoriaux. Du modèle encastré au modèle émancipé », *op. cit.*, p. 145.

[223] BOURCIER, D., « Réflexion éthique sur le partage des données en science : entre communs scientifiques et *Open Data* », *op. cit.*, pp. 213 et s.

[224] *Ibid.*, voir DEDIEU, L., « Rédiger et publier un *Data paper* dans une revue scientifique en 5 points », Montpellier : CIRAD, 2014.

[225] Les métadonnées sont des informations précises sur les données.

[226] BERNAULT, C., « Revues scientifiques et droit d'auteur : la rupture de l'*Open Acces* », *Hermès, La Revue*, vol. 71, n°1, 2015, pp. 92 à 99.

[227] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique*, LexisNexis, 5e éd., 2017, p. 740.

notion de FAIR (*Findable, Accessible, Interoperable, Reusable*)[228] afin de faciliter la réutilisation des données de la recherche tout en assurant leur qualité. Ce n'est qu'à compter de 2012 que les chercheurs ont été entendus par le législateur, la Commission européenne a préconisé le libre accès des résultats de recherche financée sur fonds publics[229]. Aussi, l'ouverture des données de la recherche a pour objectif de les rendre « *accessibles par tous après leur exploitation par le chercheur qui les a produites* »[230]. Néanmoins, les établissements et institutions d'enseignement et de recherche bénéficiaient alors d'une exception[231] quant à la réutilisation des données scientifiques qu'ils produisaient[232], c'est la loi Valter de 2015 qui est venue intégrer le volet réutilisation des données de la recherche dans le dispositif *Open Data* en supprimant l'exception de la recherche scientifique. Finalement, en 2016, la loi pour une République numérique a renforcé le droit d'accès aux données scientifiques en imposant une obligation de partage et en contraignant les établissements et les institutions de recherche à communiquer les données issues de la recherche publique[233]. Cette obligation est néanmoins redondante avec celle du Code de la recherche qui régissait déjà le partage et la diffusion des données scientifiques[234]. Elle dispose que les résultats de travaux de recherche financés au moins pour moitié par des fonds publics doivent être mis en ligne en libre accès par leurs auteurs après une période d'embargo de six (pour les travaux scientifiques) et douze mois (pour les travaux en sciences humaines et sociales). Cette mesure permet de faciliter la libre diffusion des résultats de la recherche qui était auparavant restreinte. La loi autorise également, désormais, la fouille de textes et de données en ligne et crée ainsi des exceptions au droit *sui generis* des bases de données. Ces pratiques permettent de faciliter la recherche et la citation des résultats[235]. Les données issues ou produites lors d'activités de recherche financées au

---

[228] WILKINSON, M. D., DUMONTIER, M., AALBERSBERG, I. J., APPLETON, G., AXTON, M., BAAK, A., Mons, B., "The FAIR Guiding Principles for scientific Data management and stewardship". *Scientific Data* n°3, 2016. https://doi.org/10.1038/sdata.2016.18.

[229] Programme cadre de la recherche Horizon 2020 (2014-2020) de l'UE.

[230] BERNAULT C., LUCAS A., LUCAS-SCHLOETTER A., *Traité de la propriété littéraire et artistique, op. cit.*, n°906, p. 740.

[231] ROBIN, A., « Les données scientifiques au prisme du dispositif *Open Data* », *op. cit.*

[232] Ord. 2005-650 du 6 juin 2005, art. 11 : « *Par dérogation au présent chapitre, les conditions dans lesquelles les informations peuvent être utilisées sont fixées, le cas échéant, par les administrations mentionnées aux a et b du présent articles lorsqu'elles figurent dans des documents élaborées ou détenus par a) des établissements et institutions d'enseignement et de recherche ; b) des établissements, organismes ou services culturels* ».

[233] LRN, art. 30 codif. C. rech., art. L. 533-4 : « *II.-Dès lors que les données issues d'une activité de recherche financée au moins pour moitié par des dotations de l'Etat, des collectivités territoriales, des établissements publics, des subventions d'agences de financement nationales ou par des fonds de l'Union européenne ne sont pas protégées par un droit spécifique ou une réglementation particulière et qu'elles ont été rendues publiques par le chercheur, l'établissement ou l'organisme de recherche, leur réutilisation est libre* ».

[234] ROBIN, A., « Les données scientifiques au prisme du dispositif *Open Data* », *op. cit.*

[235] BENHAMOU, F., « L'*Open Access* domaine des communs éditoriaux. Du modèle encastré au modèle émancipé », *op. cit.*

moins pour moitié par des fonds publics répondent à trois régimes cumulatifs. Elles sont soumises à la règle générale d'ouverture des données publiques à condition qu'elles soient contenues dans des documents administratifs et qu'elles aient une forme exploitable[236].

64- **Obligation de diffusion spécifique.** Les données de la recherche scientifique sont soumises à l'obligation de diffusion du dispositif *Open Data* et au régime qui en découle. Cependant, le régime du partage des données scientifiques n'est pas en tout point similaire à celui des données publiques. Les établissements de recherche ne sont pas simplement soumis à une obligation de diffusion des données qu'ils reçoivent ou produisent, mais ils ont une véritable mission de partage et de diffusion des connaissances scientifiques[237]. La dernière réforme en date a, d'une part, renforcé cette obligation en incitant les chercheurs à partager leurs données « *en priorité au format libre* »[238], et, d'autre part, a ajouté une nouvelle mission qui est « *d'organiser l'accès libre aux données scientifiques* »[239]. Les chercheurs disposent néanmoins de la possibilité de choisir le moyen de diffusion qu'ils souhaitent pour publier les travaux et jeux de données qui y sont associés[240]. Afin de soutenir la politique de science ouverte, les pouvoirs publics et notamment la Commission européenne[241] ont « *énoncé […] un principe général d'articulation, selon lequel les résultats doivent être "aussi ouverts que possible et pas plus fermés que nécessaire"* »[242]. Aussi, l'ouverture des données de la recherche peut être limitée à la fois par le secret et par le droit d'auteur[243]. Ainsi, les données publiques sous une forme exploitable et contenues dans des documents administratifs doivent être diffusées[244]. Les moyens de diffusion doivent passer par des licences d'exploitation qui peuvent être des licences libres issues du mouvement du libre ou des instituts de recherche. Ces licences sont homologuées par le gouvernement français et la mission *Etalab* a établi sa propre licence. Ces licences permettent le partage des connaissances scientifiques. La loi du 22 juillet 2013 a renforcé la nouvelle mission de l'organisation de l'accès en donnant priorité aux formats libres d'accès[245]. Les

[236] CRPA, art. L. 312-1-1.
[237] C. rech., art. L. 112-1 issue de plusieurs réformes : Loi n°82-610 du 15 juill. 1982, d'orientation et de programmation pour la recherche et le développement technologique de la France : *JO* du 16 juill. 1982 ; Loi n°2006-450 du 18 avr. 2006 : *JO* du 19 avr. 2006.
[238] C. rech., art. L. 112-1, c).
[239] Loi n°2013-660, 22 juill. 2013, C. rech. art. L. 112-1, e).
[240] ROBIN, A., « Les données scientifiques au prisme du dispositif *Open Data* », *op. cit.*
[241] Commission européenne, Reco. n°2018/790, 25 avr. 2018, relative à l'accès aux informations scientifiques et à leur conservation, (C [2018] 2375 final), n°3 : *JOUE* L 134, 31 mai 2018, p. 12.
[242] ROBIN, A., « L'ouverture des données publiques scientifiques de l'examen de la règle "*Open as possible, closed as necessary*" » *CCE*, n°9, sept. 2020, ét. 15.
[243] *Ibid.*
[244] CRPA, art. L. 321-1.
[245] C. rech., art. L. 112-1 ; L. 18 avr. 2006, arts. 12 et 16.

organismes du secteur agricole produisant des données de recherche tels que INRAE, CIRAD, ou Arvalis sont soumis à cette politique d'ouverture des données de la recherche.

3. Les initiatives citoyennes et participatives

65- De nombreux acteurs issus de la société civile produisent des données de manière volontaire et bénévole, sous la forme associative afin de créer de la connaissance[246]. Ainsi, ces initiatives démontrent la capacité du secteur privé à agir pour le bien commun ou public[247]. Les données sont donc produites et diffusées par les utilisateurs des services eux-mêmes. C'est ce que l'on appelle le *crowdsourcing* qui « *consiste à mettre à contribution des utilisateurs pour produire, mettre à jour et enrichir des données* »[248]. Plusieurs initiatives sont nées sur ce modèle, telles qu'OpenStreetMap qui est un service collaboratif de cartographie en ligne créé en 2004 visant à constituer une base de données géographiques libre du monde bâti par des contributeurs bénévoles et utilisant le système GPS et d'autres données libres. Les données ainsi mises en ligne sont réutilisables librement sous licence ODbL[249] que ce soit dans l'objectif d'obtenir des rendus géographiques, du géocodage ou encore des calculs d'itinéraires. Aujourd'hui, le service comporte plus de 7,5 millions de membres à travers le monde. Ce projet est porté par l'association à but non lucratif du même nom, OpenStreetMap, créée en 2011. Grâce à ce service, il est possible de cartographier des exploitations agricoles qui seraient délaissées par les entreprises privées d'imagerie satellitaire, telles que Google Map.

66- Parfois les initiatives citoyennes de production de données contribuent directement à la recherche scientifique. Il s'agit alors d'une recherche citoyenne qui prend place au côté de la recherche scientifique et industrielle[250]. Ces projets auxquels participe la société civile sont portés par des organisations composées de professionnels, de scientifiques et d'amateurs en collaboration avec des institutions publiques de la recherche, dans le but de créer de la connaissance libre. Ces données « citoyennes » ainsi créées sont ouvertes volontairement et intègrent les communs scientifiques[251]. Elles ne répondent pas au régime des données de la recherche scientifique, mais sont dans le domaine public. Par exemple, l'association Tela Botanica est une Organisation nationale gouvernementale qui a pour objet d'assurer la gestion

[246] ROBIN, A., *Droit des données de la recherche, op. cit*., pp. 58 et s.
[247] *Ibid.*
[248] NOUCHER, M. et GAUTREAU, P., « Le libre accès rebat-il les cartes ? Nouvelles perspectives pour les données géographiques », *op. cit.*, p. 61.
[249] Voir *infra*, n°437.
[250] ROBIN, A., *Droit des données de la recherche, op. cit*., n°66, p. 60.
[251] Voir *supra*, n°62 et s.

et la direction du réseau du même nom créée en 1999. L'objectif de ce réseau est d'échanger des informations, d'animer des projets et de produire des données libres de droits au service des botanistes. Il est composé aujourd'hui de 22 000 membres. Ce réseau, avec, entre autres, la participation de plusieurs instituts de recherche tels que le CIRAD, l'INRAE et l'INRIA, a contribué, notamment, à la création de plusieurs outils permettant d'identifier des espèces végétales à travers le monde. Par exemple, l'application Pl@ntNet permet d'identifier une plante à partir d'une simple photo. Les données ainsi collectées sont libres d'utilisation et sont à l'origine de plusieurs projets géographiques, thématiques sur les plantes ornementales et cultivées et de microprojets. Les différents membres de ces réseaux contribuent ainsi de manière collaborative à des projets de mise en commun de données dans un but de recherche scientifique participative.

§2. *L'origine des données agricoles publiques*

67- Les données agricoles publiques peuvent être produites par une personne publique (**I**) ou bien être collectées par le secteur privé dans le cadre d'une mission de service public (**II**).

I. La production de données agricoles publiques dans le cadre d'une mission de service public

68- Tout d'abord, il convient d'envisager la notion de service public (**A**) pour ensuite s'intéresser aux personnes chargées d'une mission de service public (**B**).

A. La notion de service public

69- La notion de service public doit, dans un premier temps, faire l'objet d'une définition (**1**) pour, dans un second temps, être caractérisée (**2**).

1. La définition du service public

70- Afin d'étayer le propos, une définition du service public s'impose. Au début du XXe siècle, Léon Duguit définissait le service public comme : « *Toute activité dont l'accomplissement doit être assuré, réglé et contrôlé par les gouvernants parce que l'accomplissement de cette activité*

est indispensable à la réalisation et au développement de l'interdépendance sociale, et qu'elle est de telle nature qu'elle ne peut être réalisée complètement que par l'intervention de la force gouvernante »[252]. Les commentateurs ont pu observer, par la suite, une crise de la notion. C'est finalement en 1999 que le Conseil d'État a rendu dans un rapport une définition qui repose « *toujours* »[253] sur les mêmes principes. Cette définition retient que le service public est « *une activité d'intérêt général, soit directement prise en charge par une personne publique, soit exercée sous son contrôle étroit* »[254]. Mais cette seule définition ne permet pas de déterminer en substance la mission de service public. Les nombreuses jurisprudences sur la question démontrent toute la difficulté qu'il y a à caractériser cette notion.

2. La caractérisation du service public

71- **Intérêt général.** En toute logique, les missions de service public sont confiées principalement aux administrations dès lors qu'un texte de loi le prévoit. L'agent public qui exerce une mission de service public est celui qui accomplit « *à titre temporaire ou permanent, volontairement ou sur réquisition des autorités, un service public quelconque* »[255]. L'objectif de la personne chargée d'une mission de service public est d'accomplir sa mission en recherchant la satisfaction de l'intérêt général. Cependant, « *il importe peu que les intéressés soient des personnes privées (alors collaborateurs bénévoles d'un service public) ou publiques (fonctionnaires ou contractuels qui n'exercent pas des fonctions d'autorité)* »[256]. En effet, une personne privée peut tout à fait, elle aussi, exercer une mission de service public à condition de satisfaire un besoin légitime de la population et d'être fondée sur la carence de l'initiative publique[257]. La jurisprudence a dégagé divers critères afin d'apprécier l'existence d'une telle mission lorsqu'elle est exercée par une personne privée. Afin de déterminer le caractère de service public de l'activité d'une entreprise privée, la jurisprudence a soulevé plusieurs hypothèses que l'arrêt APREI a permis de « codifier »[258]. D'abord, dans la plupart des cas,

---

[252] DUGUIT, L., *Traité de droit constitutionnel (t. 1 théorie générale de l'État)*, Fontemoing, 1911, p. 99.
[253] PILCZER, J.-S., « La notion de service public », *Informations sociales*, n°158, 2010/2, pp. 6 à 9.
[254] CE, *Réflexions sur l'intérêt général*, rapport public, (EDCE n°50), La Documentation française, 1999 p. 272.
[255] Circ. n°93.9/F1 du 14 mai 1993 présentant les dispositions du nouveau code pénal, *JO*, sept. 1993.
[256] WAGNER, M., « Le droit pénal spécial et les fonctions publiques : une illustration des affres de la pénalisation à outrance », *RSC*, 2011/1, n°1, p. 37.
[257] CE, 1er févr. 1901, *Descroix et autres boulangers de Poitiers* : concl. ROMIEU J., *S.*, 1991. 17 ; note HAURIOU M., *RGD* 2014. 15150 ; CE, sec., 30 mai 1930, *Chambre syndicale du commerce en détail de Nevers* : req. n°06781 ; Rec. p. 583 ; concl. JOSSE ; note ALIBERT R. ; avis GUYOMAR M. et COLLIN P., *AJDA*, 2000. 12 ; comm. TREPPOZ A., *AJDA*. 2001. 7 ; comm. LOMBARD M., *RJEP*. 2011. 683 ; comm. TOUZEIL-DIVINA M., *JCP A*. 2020. 15.
[258] COSTA, D., « Mission de service public assurée par une personne privée : clarification ou codification ? », *op. cit.*, p. 825.

l'identification des organismes privés en charge d'une mission de service public est faite par le juge. En dehors de cette hypothèse, le Conseil d'État a dégagé deux hypothèses alternatives, la première se révèle être celle de principe : « *une personne privée qui assure une mission d'intérêt général sous le contrôle de l'administration et qui est dotée à cette fin de prérogatives de puissance publique est chargée de l'exécution d'un service public* ». La seconde hypothèse est l'exception : « *même en l'absence de telles prérogatives, une personne privée doit également être regardée, dans le silence de la loi, comme assurant une mission de service public lorsque, eu égard à l'intérêt général de son activité, aux conditions de sa création, de son organisation ou de son fonctionnement, aux obligations qui lui sont imposées ainsi qu'aux mesures prises pour vérifier que les objectifs qui lui sont assignés sont atteints, il apparaît que l'administration a entendu lui confier une telle mission* ».

72- **Critères codifiés.** Le premier critère codifié par l'arrêt *APREI*[259], et repris dans différents arrêts du Conseil d'État[260], est de source légale : « *est service public l'activité sociale que les pouvoirs publics ont entendu ériger comme tel* »[261]. Par conséquent, le législateur peut qualifier un service public au moyen de la loi[262]. Dans cette hypothèse, le caractère de service public s'impose directement. En l'absence de tout texte de loi, le Conseil d'État a dégagé plusieurs critères. D'abord, dans l'arrêt *Narcy*[263] de 1963, le juge a dégagé trois critères cumulatifs[264] pour reconnaître l'exécution d'un service public : la personne privée doit exercer une mission d'intérêt général, et enfin l'exercice de cette mission doit se faire sous le contrôle de l'Administration, la personne privée est dotée de prérogatives de puissance publique afin d'exercer sa mission. Ensuite, dans les arrêts *Bernardi*[265] et *Ville de Melun*[266], cette dernière

---

[259] *Ibid.*

[260] CE, sec. cont., 22 févr. 2007, *Association du Personnel relevant des Établissements pour Inadaptés (APREI)*, n°264541 : Rec. p. 92 ; concl. VEROT. Chron. LENICA et BOUCHER, *AJDA* 2007. 793 ; note GUGLIELMI et KOUBI, *JCP A* 2007. 2145 ; note BOITEAU, *RFDA* 2007. 803 ; CE, 5 oct. 2007, *Société UGC-Ciné-Cité*, n°298773 : Rec., p. 418 : concl. CASAS D., *BJCP* 2007, n°55, p. 483 ; note ECKERT G., *CMP*, 2007, n°11, p. 27 ; note LINDITCH F., *JCP A* 2007, n°56, p. 38 ; note DREYFUS J.-D., *AJDA* 2007, n°41, p. 2260 ; chron. PLESSIX B., *JCP* n°50, p. 19 ; note GLATT J.-M., *LPA*, 2007, n°252, p. 19 ; note MONDOU Ch., *RLCT*, 2008, n°31, p. 26 ; note CLAMOUR G., *RLC*, 2008, n°14, p. 57 ; note MILLET F.-X., *Gaz. Pal.* 2008, n°48-50, p. 12 ; note MOREAU D., *RJEP*, 2008, n°652, p. 27 ; note COURNIL Ch. et RENEAUD F., *JCP E* 2009, n°11, p. 37 ; ét. VIEL M.-Th, *RGCT*, 2010, n°47, p. 163 ; CE, 25 juill. 2008, *Commissariat à l'énergie atomique (CEA)*, n°280163 ; *Rec*, p. 751 ; obs. AÏT-EL-KADI. AJDA. 2008. 1521.

[261] CHEVALLIER, J., *Le service public*, Que sais-je ?, 2018, p. 47.

[262] T. confl., 6 nov. 1978, *Bernardi*, 02086 ; Rec. 652 ; note MODERNE F., *RDSS* 1979. 91 ; chron. DUTHEILLET DE LAMOTHE O. et ROBINEAU Y., *AJDA* 1979, n°1, p. 22.

[263] CE, sect., 18 juin 1963, *Narcy*, req. n°43834 ; Rec. p. 401 ; obs. WALINE M., *RD publ.* 1963. 1186 ; obs. de LAUBADERE A., *AJDA* 1964, p. 91.

[264] « *Une personne privée qui assure une mission d'intérêt général sous le contrôle de l'administration et qui est dotée à cette fin de prérogatives de puissance publique est chargée de l'exécution d'un service public* ».

[265] T. confl. 6 nov. 1978, *Bernardi*, préc.

[266]CE, 20 juill. 1990, *Ville de Melun et association « Melun-culture-loisirs » c/Vivien et autres* : rec. 220 ; concl. POCHARD. *AJDA* 1990. 820 ; note FATOME *JCP* 1991. II. 21663.

condition a été allégée, il est désormais admis qu'une personne privée puisse exercer une mission de service public sans qu'il y ait prérogative de puissance publique[267].

73- **Faisceau d'indices.** La complexité de la notion a conduit la jurisprudence à mettre en place un faisceau d'indices selon les conditions de création, d'organisation et de fonctionnement, la nature des obligations imposées ou encore les contrôles de l'entreprise privée. Il s'agit d'éléments matériels permettant de démontrer « *l'intention de l'administration de confier à des personnes privées une telle mission* »[268]. Mais, il faut noter que cette hypothèse « *est réservée à certains contentieux, notamment celui de la qualification de document administratif, comme dans les affaires APREI ou encore ville de Melun, précitées, et Société protectrice des animaux*[269] » et « *non à ceux qui exigent l'exercice de prérogatives de puissance publique en vue de la qualification d'acte administratif ou de la mise en cause de la responsabilité administrative* »[270].

74- **Critère organique.** S'agissant du critère organique, il repose sur le principe selon lequel une personne privée en charge d'une mission de service public ne peut l'exercer sans le contrôle direct ou indirect d'une personne publique. De fait, il suffit qu'une personne publique contrôle ou supervise la personne privée pour reconnaître l'existence d'une mission de service public. Aussi, la Cour de cassation a eu l'occasion de préciser, au sujet d'une prise illégale d'intérêts, que « *doit être regardée comme chargée d'une mission de service public au sens de l'article 432-12 du Code pénal, toute personne chargée directement ou indirectement, d'accomplir des actes ayant pour but de satisfaire l'intérêt général, peu important qu'elle ne disposât d'aucun pouvoir de décision au nom de la puissance publique* »[271]. Au vu de ces éléments, il apparaît que cette catégorie est illimitée et qu'il est impossible d'en dresser une liste exhaustive, ce d'autant que la jurisprudence applique le critère avec une certaine souplesse[272]. En outre, dès lors que les personnes et organismes de droit privé ont obtenu une

---

[267] COSTA, D., « Mission de service public assurée par une personne privée : clarification codification ? », *op. cit.*, p. 825.
[268] CHEVALLIER, J., *Le service public, op. cit*., p. 48.
[269] CE, 26 févr. 2003, *Société protectrice des animaux*, n°212943 : *Rec*. 787 ; note COSTA D., *AJDA*. 2003. 1488 ; concl. GOULARD *BJCL*. 2003. 361.
[270] T. confl. 6 nov. 1978, *Bernardi*, préc. ; CE Sect. 13 oct. 1978, *ADASEA du Rhône*, Lebon 368 ; RD publ. 1979.899, note ROBERT, J., p. 908 et s., concl. GALABERT, D. 1979.249, note AMSELEK, P. et WALINE, J., *AJDA* 1979. II. 35, *ibid.* I. 22, chron. DUTHEILLET DE LAMOTHE ET ROBINEAU ; CE 17 févr. 1992, *Sté Textron* : *Lebon* 66, *AJDA* 1992.450 ; note PENNEAU A., *D*. 1992, Jur. p. 519 ; COSTA, D., « Mission de service public assurée par une personne privée : clarification ou codification ? », *op. cit.*, p. 825.
[271] Crim, 30 janvier 2013, n°11-89.224, *Bull. crim*. 2013, n°33.
[272] CORIOLAN, S., *Responsabilité pénale des personnes publiques : infractions non intentionnelles*, Rép. resp. puiss. Pub., D., 2020.

subvention, il n'est plus exigé qu'elles exercent une mission de service public pour entrer dans la catégorie[273].

75- **Nature publique ou privée des personnes en charge d'une mission de service public.** Par conséquent, la notion de personne publique est un « *point d'ancrage pour toutes les notions par l'intermédiaire desquelles le droit administratif s'applique* »[274]. Or, la mission de service public n'est pas nécessairement confiée à une personne publique, il peut tout aussi bien s'agir d'une personne privée. Aussi, dès lors que la personne publique exerce un droit de regard sur l'exercice de la personne privée, l'activité de cette dernière est qualifiée de mission de service public[275]. En revanche, en l'absence de tout contrôle, même si la mission est d'intérêt général, elle n'est pas qualifiée de mission de service public[276]. Bien que « *le service public [apparaisse] comme une activité assumée directement ou indirectement par une personne publique* »[277], la délimitation n'est pas bien définie, il s'agit plutôt de faire du cas par cas. Par conséquent, la distinction principale entre personne publique et personne privée vient du fait que « *les organismes publics sont créés par les pouvoirs publics avec des droits et prérogatives exorbitants du droit commun* », alors que « *les organismes privés, au contraire, se situent hors de la hiérarchie administrative et en marge de ses principes d'organisation* »[278].

76- **Exclusion des agriculteurs.** Les exploitants agricoles ne produisent pas de données dans le cadre d'une mission de service public. L'activité agricole est une activité de droit privé régie par le Code rural. Les exploitants agricoles exercent en dehors de toute mission de service public, ils ne sont donc pas soumis directement à l'obligation de diffusion des données qu'ils collectent ou produisent. Pour autant, certaines de leurs données sont soumises à des obligations réglementaires qui une fois collectées par les administrations en charge de l'exploitation de ces données doivent être mises à disposition dans le cadre de la politique d'ouverture des données

---

[273] Loi nº 2000-321 du 12 avr. 2000, art. 10 modifié par la loi nº 2016-1321 du 7 oct. 2016 ; BECET J.-M., « Communication des documents des collectivités territoriales au public : Régime général », folio n°12210, 2019-1.

[274] AUBY, J.-B., *La notion de personne publique en droit administratif*, dir. DUCOS-ADER, R., Thèse, Bordeaux, 1979, p. 348.

[275] CE, sect., 06 avr. 2007, *Commune d'Aix-en Provence*, n°284736 ; Rec. 155 ; chron. LENICA F. et BOUCHER J., *AJDA*. 2007. 1020 ; note BAZEX M. et BLAZY S., *AJDA*, 2007. 35 ; note ROUAULT M.-C. *RLCT*. 2007. 26 ; chron. PLESSIX B., *JCP G*. 2007. 21 ; MARAIS B., KOVAR J.-P. et RODRIGUES S., *Concurrences*. 2007. 163 ; note BRUNET P., *Rev. des contrats*. 2007. 867 ; concl. SENERS F., *RJEP*. 2007. 273 ; comm. KARPENSCHIF M., *JCP G*. 2007. 31 ; comm. GLATT, J.-M., *LPA*. 2007. 13 ; note TOUZEIL-DIVINA M., *LGP*. 2007. 4 ; chron. ORSONI G., *RTD com*. 2007. 694 ; note COURNIL C. et RENEAUD F., *JCP E* 2009. 37.

[276] CE, 8e et 3e ch., 15 févr. 2016, *Société cathédrale d'Images*, n°384228 ; note SCHMITT R., *Lexbase* éd. pub. 2016. 407 ; note EXKERT G., *CMP*. 2016 n°4 p. 45 ; comm. BRENET F., *AJDA*. 2016. n°5 p. 34 ; comm. PAULIAT H., *JCP A*. 2016 n°25 p. 37 ; chron. LLORENS F. et SOLER-COUTEAUX P., *CMP* 2017 n°3 p. 11.

[277] CHEVALLIER, J., *Le service public*, Que sais-je ?, 2018, p. 48.

[278] CHEVALLIER, J., « La place de l'établissement public en droit administratif français », *Publications de la faculté de droit d'Amiens*, 2011, pp. 5 à 76.

publiques (*Open Data*)[279]. De plus, de nombreuses données sont produites ou collectées par d'autres acteurs du secteur agricole qui participent à l'enrichissement du savoir en agriculture, telles que les instituts techniques agricoles et les instituts de recherche (INRAE, CIRAD, etc.)[280].

B. Les personnes en charge d'une mission de service public dans le secteur agricole

77- Il est nécessaire d'envisager les personnes publiques (**1**) puis les personnes privées chargées d'une mission de service public (**2**) du secteur agricole, susceptibles de produire des données publiques.

1. Les personnes publiques du secteur agricole

78- Un large panel d'organismes du service public est susceptible de produire ou de collecter des données intéressant le secteur agricole. Parmi ces acteurs, il faut citer les collectivités nationales ou locales, les services du ministère de l'Agriculture et de l'Alimentation (MAA), centraux ou déconcentrés, et les établissements publics administratifs (EPA) ou industriels et commerciaux (EPIC) de l'État ou des collectivités locales.

79- **Le ministère de l'Agriculture et de l'Alimentation.** Le MAA prépare et met en œuvre la politique du gouvernement dans le domaine de l'agriculture, de la forêt et du bois, et établit les statistiques agricoles (Agreste). À cette fin, il produit des jeux de données chaque année afin de recenser notamment la quantité de produits phytosanitaires utilisés, les structures des exploitations, l'occupation du territoire, etc.

80- **Les établissements publics.** Plusieurs EPA et EPIC produisent des données qui intéressent de près ou de loin le secteur agricole. C'est le cas notamment de l'Agence de l'environnement et de la maîtrise de l'énergie (ADEME)[281]. Cet EPIC participe à la construction des politiques nationales et locales de transition écologique. Elle a déjà produit 177 jeux de données. Par exemple, elle produit la base de données Agribalyse qui comporte les références des indicateurs d'impacts environnementaux des produits agricoles produits en France et des produits alimentaires consommés en France. Également, l'Office de développement de l'économie

[279] Voir *infra*, n°100 et s.
[280] Voir *infra*, n°78 et s.
[281] Créée par la Loi n°90-1130 du 19 décembre 1990, arts. L. 131-3 à L. 131-7 et R. 131-1 à R. 131-27, C. de l'env.

agricole dans les départements d'outre-mer (ODEADOM)[282] collecte des données pour aider aux développements économiques dans les départements d'outre-mer, comme la faisabilité de la mise en place d'une filière de canne biologique à la Réunion par exemple. L'ODEADOM a également créé un observatoire en 2016 chargé de rassembler l'ensemble des données économiques, financières et structurelles se rapportant aux agriculteurs d'outre-mer afin de fournir des notes et des analyses relatives à l'agriculture dans les DOM. Parmi les IPA qui produisent des données agricoles, il est possible de citer l'Institut national de l'origine et de la qualité (INAO)[283] qui a pour mission de recueillir et d'analyser les données économiques des produits sous les signes officiels de la qualité et de l'origine. Notamment, cet institut anime en partenariat avec INRAE depuis 2011 un réseau de qualité et un observatoire territorial de ces signes, afin d'obtenir des informations concernant leurs impacts économiques, sociaux et environnementaux sur le territoire. Aussi, l'Institut public de référence pour l'information géographique et forestière (IGN)[284] est un EPA placé sous la tutelle des ministères chargés de l'écologie et de la forêt qui a pour mission de produire et de diffuser des données et des représentations de référence relatives à la connaissance du territoire national et des forêts françaises ainsi qu'à leur évolution[285]. Cet institut produit énormément de données géographiques parmi lesquelles le registre parcellaire de référence qui sert de référence à l'instruction des aides de la PAC. Enfin, FranceAgriMer[286] est l'établissement national des produits de l'agriculture et de la mer qui a une mission de concertation au sein des filières agricole et maritime. Cet EPA a pour objectif de mettre en œuvre des dispositifs de soutien aux filières agricoles et de la pêche et de gérer des dispositifs de régulation des marchés. Il doit collecter, analyser et diffuser des données économiques et enfin soutenir les exportateurs dans le secteur agricole et agroalimentaire. Pour cela, l'institut FranceAgriMer produit notamment des données sur les productions agricoles et alimentaires (enquête variétale, collecte laitière, cotations viandes, chiffres des halles à marée, etc.).

Aussi, les instituts de recherche et les instituts techniques agricoles sont pour certains sous la tutelle principale du ministère en charge de l'agriculture ou du commissaire du gouvernement[287], tandis que d'autres sont sous la tutelle secondaire du ministère en charge de

[282] Créée par le Décret n°84-356 du 11 mai 1984, art. R. 684-1 à R. 684-12 C. rur.
[283] Décret-loi du 30 juill. 1935, R. 642-1 à R. 642-32 C. rur.
[284] Créé par le Décret n°2011-1371 du 27 oct. 2011 relatif à l'institut national de l'information géographique et forestière : *JORF* n°0251 du 28 oct. 2011.
[285] https://www.ign.fr/institut/carte-didentite
[286] Ord. n°2009-325 du 25 mars 2009 ; Décret n°2009-340 du 27 mars 2009.
[287] Dans la sphère agriculture, agroalimentaire, forêt et affaires rurales (Agence bio, Institut national de l'origine et de la qualité, Office de développement de l'économie agricole d'outre-mer, FranceAgrimer, etc.). Dans la sphère enseignement et recherche (Montpellier SupAgro, Acta, Actia, etc.).

l'agriculture (ou membre du conseil d'administration)[288]. Leur rattachement au ministère de l'Agriculture en fait des établissements publics exerçant une mission de service public soumis à la politique d'ouverture des données publiques. Ainsi, les instituts de recherche sont des établissements, laboratoires ou organismes de recherche et d'enseignement spécialisé dans les domaines de recherche scientifique, historique, ou des sciences humaines et sociales. Deux instituts de recherches travaillent en particulier dans la recherche agronomique. Il s'agit de l'INRAE et du CIRAD. Tout d'abord, l'INRAE est l'institut national de recherche pour l'agriculture, l'alimentation et l'environnement. Il s'agit d'un institut public à caractère scientifique et technologique, assimilé à un établissement public administratif, placé sous la tutelle du ministère de l'Enseignement supérieur, de la Recherche et de l'innovation et du ministère de l'Agriculture et de l'Alimentation. Né le 1er janvier 2020[289], il est issu de la fusion entre l'INRA, l'Institut national de la recherche en agronomie et l'Irstea, l'Institut national de recherche en sciences et technologies pour l'environnement et l'agriculture. L'INRAE produit, notamment, la base de données Agribalyse en collaboration avec l'ADEME. Le CIRAD[290] est le centre de coopération internationale en recherche agronomique pour le développement créé en 1984 sous le statut d'EPIC issu de la fusion d'instituts techniques et de recherche agronomique tropicale. Il est placé sous la double tutelle du ministère de l'Enseignement supérieur, de la Recherche et de l'innovation et du ministère de l'Europe et des Affaires étrangères. Il s'agit de l'organisme français de recherche agronomique et de coopération internationale pour le développement durable des régions tropicales et méditerranéennes. Le CIRAD produit par exemple la base de données DetaData qui décline les problématiques de développements des zones cotonnières en Côte d'Ivoire, applicable à d'autres pays de l'Afrique francophone.

81- **Les instituts techniques agricoles.** Ces instituts sont des organismes de recherche appliquée, d'appui technique, d'expérimentation, d'expertise, de formation et d'information. Ils sont spécialisés par filières de production. Ils ont quatre missions qui sont de conduire des travaux de recherche appliquée et de développement pour apporter des solutions opérationnelles et durables aux agriculteurs et aux filières, combiner les compétences scientifiques et l'expertise de terrain pour éclairer les décisions des entreprises et des pouvoirs publics, évaluer et faciliter

[288] Dans la sphère agriculture, agroalimentaire, forêt et affaires rurales : IGN, ONEMA, GEVES ; Dans la sphère enseignement et recherche : INRAE, Agreenium.
[289] Créé par le Décret n°2019-1946 du 10 oct. 2019, relatif à l'organisation et au fonctionnement de l'institut national de recherche pour l'agriculture, l'alimentation et l'environnement : *JORF* n°0238 du 12 oct. 2019.
[290] Créé par le Décret n°84-429 du 5 juin 1984 portant création et organisation du centre de coopération internationale en recherche agronomique pour le développement (CIRAD) : *JORF* du 8 juin 1984.

l'accès à l'innovation, transférer et diffuser des références fiables et objectives[291]. Ils sont fédérés par l'ACTA qui est un institut technique agricole qui porte des projets et développe une expertise transversale dans l'intérêt des filières. Parmi les instituts techniques agricoles, trois seront présentés. Tout d'abord, Arvalis, l'institut du végétal, qui est une association à but non lucratif créé en 1959, financée et gérée par les agriculteurs eux-mêmes. Cet institut a le statut d'association de la loi de 1901. C'est un institut de recherche appliquée dédié aux grandes cultures et aux fourrages, il conduit des recherches spécialement sur les cultures de céréales à paille (blé, orge…), maïs, sorgho, pommes de terre, lin, fibres et fourrages et créé de nombreuses bases de données telles que « base sol » qui permet de faciliter et d'harmoniser le référencement des sols dans des outils d'aide à la décision d'Arvalis afin de fournir les conseils adaptés aux agriculteurs. Ensuite, Idele est l'institut de recherche appliquée et de développement dans le domaine de l'élevage, constitué également sous la forme d'une association loi de 1901 qui a pour vocation d'améliorer la compétitivité des élevages herbivores et de leurs filières. Cet institut a pour mission d'apporter des solutions techniques et innovantes aux éleveurs de bovins, ovins, caprins et équins et aux acteurs des filières. À cette fin, de nombreuses bases de données d'appui technique sont créées, telle que la base de données concernant les ovins par région qui a pour but de fournir une analyse technico-économique sur les élevages ovins dans une région donnée.

82- **Le réseau des chambres d'agriculture.** Il faut également citer les chambres d'agriculture qui sont des établissements publics pilotés par des élus professionnels, représentant les principaux acteurs du monde agricole, rural et forestier[292]. Ce sont des organismes consulaires fondés en France par la loi du 3 janvier 1924. Leurs missions sont décrites aux articles L. 510-1 et suivants du Code rural. Ainsi, le réseau des chambres d'agriculture doit « *contribuer à l'amélioration de la performance économique, sociale et environnementale des exploitations agricoles et de leurs filières. Accompagner, dans les territoires, la démarche entrepreneuriale et responsable des agriculteurs ainsi que la création d'entreprise et le développement de l'emploi, contribuer par les services qu'ils mettent en place, au développement durable des territoires ruraux et des entreprises agricoles, ainsi qu'à la préservation et à la valorisation des ressources naturelles, à la réduction de l'utilisation des produits phytopharmaceutiques et à la lutte contre le changement climatique, assurer une fonction de représentation auprès des pouvoirs publics et*

[291] https://www.acta.asso.fr/le-reseau/

[292]https://chambres-agriculture.fr/chambres-dagriculture/nous-connaitre/le-reseau-des-chambres-dagriculture/#:~:text=Elles%20ont%20un%20statut%20d,la%20tutelle%20des%20pouvoirs%20publics.

des collectivités territoriales »[293]. Afin de répondre à ces différentes missions, les chambres d'agriculture peuvent être amenées à collecter et traiter des données au moyen des services proposés aux agriculteurs ou au travers d'enquête. Mais aussi, le réseau des chambres d'agriculture a conçu le logiciel MesParcelles qui est une solution de gestion des parcelles agricoles pour piloter les exploitations de façon centralisée, optimisée et sécurisée. À travers ce service, les chambres d'agriculture proposent plusieurs solutions numériques telles que Proagri et Proviti. Ce logiciel est un outil d'enregistrement des pratiques agricoles et de gestion technique et économique des exploitations, qui propose un suivi quotidien des exploitations. Cet outil permet notamment de cartographier de manière détaillée l'exploitation en saisissant et en enregistrant l'ensemble des pratiques du travail du sol, à la récolte et ainsi de gérer simplement la fertilisation et les traitements phytosanitaires tout en respectant la réglementation en vigueur. Mais aussi, entre autres, MesParcelles est une plateforme de service permettant d'interconnecter l'ensemble des données de l'exploitation : tracteur, imagerie satellitaire, OAD protection des cultures, OAD fertilisation azotée, dispositif de traçabilité automatique, etc.

2. Les personnes privées en charge d'une mission de service public

83- Parmi les personnes privées, plusieurs avis de la CADA et arrêts du Conseil d'État ont défini celles qui ont la charge d'une mission de service public et qui doivent donc, à ce titre, être soumises à la politique d'ouverture des données publiques (*Open Data*). Ainsi, la CADA a donné un avis favorable pour la communication des documents concernant une société d'économie mixte. Par conséquent, les sociétés d'économie mixte locales qui sont des sociétés anonymes gérant un service public ou une activité d'intérêt général et dans lesquelles les collectivités territoriales sont le plus souvent majoritaires[294] doivent répondre à l'obligation de diffusion des données qu'elles produisent ou collectent. C'est ainsi que, par exemple, dans le secteur agricole, la SEM, Compagnie d'aménagement des coteaux de Gascogne, doit diffuser les données et documents dont elles disposent pour la réalisation de sa mission de service public.

Également, les sociétés d'aménagement foncier et d'établissement rural (Safer) créées en 1960 par la loi d'orientation agricole pour réorganiser les exploitations agricoles, dans le cadre de la mise en place d'une agriculture plus productive et avec l'objectif d'installer des

[293] https://chambres-agriculture.fr/chambres-dagriculture/nos-missions-et-prestations/
[294] CADA, avis, 9 avr. 1998, n°19981017.

jeunes[295] sont des organes chargés de la gestion d'un service public administratif en vue de l'amélioration des structures agricoles. Les SAFER ont pour objectif de contribuer à un aménagement durable de l'espace rural en acquérant des biens agricoles et ruraux et en les attribuant à des candidats privés ou publics dont les projets s'intègrent aux politiques d'aménagement durable des territoires. Par deux décisions le Conseil d'État a confirmé l'obligation des SAFER de diffuser les documents administratifs qu'ils détiennent[296].

La CADA a aussi donné un avis favorable pour la communication des documents produits pour un organisme privé chargé d'une mission de service public, le comité régional des pêches maritimes et des élevages marins (CRPMEM)[297]. Cet organisme est une organisation interprofessionnelle des pêches maritimes et des élevages marins régie par le Code rural et de la pêche maritime, aux articles L. 912-1 et suivants. Il a pour missions de défendre et promouvoir les intérêts des pêcheurs professionnels embarqués et à pied.

En outre, les organismes professionnels et certains acteurs du terrain désignés expressément par des règlements, les organismes professionnels et les filières qui agissent dans l'intérêt des membres de la profession (et non pas celui de l'intérêt général) peuvent aussi se voir reconnaître une mission de service public par l'État dès lors que celui-ci estime que cet intérêt particulier met en cause l'intérêt général[298]. En effet, le Conseil d'État a dû trancher la question de savoir si la nature des actes des organisations professionnelles agricoles était publique. Dans cette décision du 28 juin 1946, le Conseil d'État a décidé que les organismes corporatifs agricoles étaient des organismes privés ayant une mission de service public[299]. Par conséquent, ils sont également soumis à l'obligation de diffusion des documents administratifs et des données publiques. C'est ainsi que les organisations professionnelles agricoles (OPA) dont font partis, entre autres, la Fédération nationale des syndicats d'exploitants agricoles (FNSEA)[300], les Jeunes agriculteurs (JA)[301], la Confédération nationale de la mutualité, de la

[295] https://www.safer-grand-est.fr/quest-ce-quune-safer

[296] CE, 20 nov. 1995, *Borel*, req. n°147026 : Rec. 795, *Gaz. Pal*. 1996, Pan. *Dr. Adm*. p. 84 ; CE 5 mai 2008, *Thiébaux*, req. n°294645, rec., inédit ; *JCP Adm.* 2008. 2182, note DARCY, G., *AJDA* 2008. 1735, *JCP N* 2001. 547 ; *Gaz. Pal.* 3-4 oct. 2001, p. 22.

[297] CADA, avis, 3 juin 2010, nº 20102171.

[298]CE, ass., 31 juill. 1942, *Monpeurt*, n°71398, Rec. p. 239 ; concl. SEGALAT, note P.C. *D.* 1942. 138 ; Concl. LAROQUE P., *JCP* 1942. II. 2046 ; note BONNARD *RD publ.* 1943.57, concl. ; concl. S. 1942.3.37 ; CASSIN R. et WALINE M., *GAJA*. 2017. 304 ; CHEVALLIER, J., « Essai sur la notion juridique de service public », *Publications de la faculté de droit d'Amiens*, n°7, 1976.

[299]CE, 28 juin 1946, *Morand*, n°73774 : rec. 183 ; note P.M. S. 1947.

[300] Syndicat professionnel majoritaire dans la profession agricole en France.

[301] Centre national des jeunes agriculteurs, organisation syndicale créé en 1957 sous l'impulsion de la jeunesse agricole catholique, devenu Jeunes Agriculteurs en 2002.

coopération et du Crédit Agricole (CNMCCA)[302] et l'Assemblée permanente des chambres d'agriculture (APCA), ont l'obligation de diffusion des documents administratifs et des données publiques qu'ils produisent ou collectent.

II. La collecte de données agricoles privées dans le cadre d'une mission de service public

84- Aujourd'hui, se pose la question de la collecte des données confidentielles ou faisant l'objet d'une réservation privative[303] par les personnes en charge d'une mission de service public pour la réalisation de leur mission. Or, il n'existe pas pour l'heure d'obligation générale de mise à disposition des données faisant l'objet d'une réservation privative en faveur de l'administration. Par conséquent, les agriculteurs et les entreprises privées n'ont, *a priori*, pas d'obligation de communiquer les données qu'ils produisent ou collectent *via* les objets connectés sur les exploitations. Aussi, les personnes morales exerçant une mission de service public rencontrent parfois des difficultés pour collecter ces données agricoles et doivent passer par des observatoires, des contrôles et des audits sur les exploitations ou par des formulaires et des enquêtes. Ce n'est qu'une fois que ces personnes exerçant une mission de service public ont traité les données ainsi collectées qu'elles deviennent publiques et communicables. Néanmoins, certaines obligations réglementaires imposent la mise à disposition des données faisant l'objet d'une réservation privative et le législateur européen envisage dans sa Proposition de Règlement sur les données, appelé *Data Act*, du 23 février 2022[304], une nouvelle obligation de mettre des données à la disposition des organismes du secteur public et des institutions, organes ou organismes de l'Union européenne. Cette mise à disposition n'aurait lieu « *[qu'] en raison d'un besoin exceptionnel* »[305] et ne viseraient que les petites et microentreprises telles que définies à l'article 2 de l'annexe de la recommandation 2003/61/CE[306]. Ainsi, si les exploitants

[302] Organisation professionnelle agricole sous forme associative créée en 1910, participe à la représentation des intérêts des entreprises mutualistes et coopératives agricoles françaises tant au niveau national qu'européen.
[303] Pour une définition, voir *infra*, n°134 et s.
[304] Proposition règl. du 23 févr. 2022 fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (Règl. sur les données), COM(2022) 68 final.
[305] *Ibid.* ; La Proposition de règlement entend par besoin exceptionnel la réaction à une urgence publique, la prévention d'une urgence publique ou la contribution au rétablissement à la suite d'une urgence publique. Mais aussi, lorsque l'organe ou l'organisme ne peut pas s'acquitter d'une mission spécifique d'intérêt public, parce qu'elle n'a pas pu obtenir les données par d'autres moyens et que l'obtention des données réduirait substantiellement les charges administratives pesant sur les détenteurs ou sur d'autres entreprises, au sens de l'article 15 de la proposition de règlement précitée.
[306] « *Dans la catégorie des PME, une petite entreprise est définie comme une entreprise qui occupe moins de 50 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 10 millions d'euros* » ;

agricoles seront majoritairement exclus du champ d'application de cet article, les entreprises de l'agriculture numérique pourraient être en revanche contraintes de mettre à disposition les données qu'elles détiennent pour des raisons de santé publique ou pour la réalisation d'une mission d'intérêt public spécifique (la réalisation d'enquêtes statistiques sur l'utilisation des produits phytosanitaires, par exemple[307]). Pour l'heure, néanmoins, il faut s'intéresser aux réglementations rendant obligatoire la mise à disposition des données agricoles faisant l'objet d'une réservation privative (**A**). Toutefois, leur accessibilité reste limitée (**B**).

A. La mise à disposition obligatoire des données agricoles privées

85- Plusieurs réglementations contraignent les personnes morales de droit privé à mettre à disposition les données qu'elles détiennent dans un objectif de réalisation d'une mission de service public. En général, elles sont ouvertes dans le cadre de concessions ou dans le cadre de mission de service public et commercial[308], mais d'autres réglementations spécifiques contraignent les personnes morales de droit privé, sans concession ou mission de service public et commercial, à mettre à disposition leurs données que ce soit à des fins de contrôle (**1**), ou à des fins de statistiques publiques (**2**).

1. La mise à disposition obligatoire des données agricoles privées à des fins de contrôle

86- Certaines données agricoles doivent être mises à disposition à des fins de contrôle. C'est le cas notamment des « *données comportant des informations relatives aux détenteurs, aux exploitations, aux animaux qui y sont abattus et à leurs mouvements [qui] sont la propriété du ministre chargé de l'agriculture* », selon l'arrêté du 9 décembre 2009 fixant les modalités de gestion et de fonctionnement de la base nationale d'abattage des bovins[309]. Aussi, selon cet arrêté, les données, bien que de provenance privée, sont la propriété de l'administration. L'objectif est d'agrémenter la base de données nationale d'abattage de bovins.

« *Dans la catégorie des PME, une microentreprise est définie comme une entreprise qui occupe moins de 10 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 2 millions d'euros* ».

[307] Par ex., voir *infra*, n°159 et s.

[308] Voir *infra*, n°145.

[309] Arrêté du 9 déc. 2009 : *JORF* n°0294 du 19 déc. 2009.

2. La mise à disposition des données agricoles privées à des fins de statistiques publiques

87.- Certaines données sont mises à disposition à des fins de statistiques publiques. En effet, la LRN du 7 octobre 2016 a modifié la loi du 7 juin 1951 et a introduit l'article 3 bis instaurant la possibilité pour le ministre chargé de l'économie après avis du Conseil national de l'information et de la statistique (Cnis) d'exiger des « *personnes morales de droit privé sollicitées pour des enquêtes qu'elles transmettent par voie électronique sécurisée au SSP, à des fins exclusives d'établissement de statistiques, les informations présentes dans les bases de données qu'elles détiennent, lorsque ces informations sont recherchées pour les besoins d'enquêtes statistiques qui sont rendues obligatoires en application de l'article 1er bis* ». Cet article fait de ces données des données d'intérêt général au sens de la LRN. En outre, la loi prévoit des sanctions à l'encontre des personnes morales qui ne se conformeraient pas à cette obligation. C'est dans ce cadre que, par exemple, un arrêté du 13 avril 2017 a rendu obligatoire la transmission des données générées par des « *personnes morales dont un des établissements a une activité de commerce de détail en magasin non spécialisé à prédominance alimentaire de plus de 400 m2* ». La transmission des données devait permettre de réaliser les « *enquête(s) statistique(s) pour l'indice des prix à la consommation et l'enquête mensuelle sur l'activité des grandes surfaces alimentaires* ».

B. L'accès limité des données agricoles privées

88.- Bien que ces données soient mises à disposition des personnes publiques pour la réalisation de leur mission de service public, elles n'entrent malgré tout pas dans la catégorie des données d'intérêt général ou des données publiques. En effet, elles ont, au contraire, vocation à rester confidentielles soit en les anonymisant, soit en limitant l'accès à la base de données à un certain nombre d'utilisateurs autorisés. Par exemple, la base nationale d'abattage des bovins n'est accessible qu'aux comités régionaux interprofessionnels, au dernier détenteur du bovin abattu, à l'institut de l'élevage et enfin à l'Institut national de recherche agronomique (INRA)[310]. De plus, en l'espèce, les données doivent être détruites tous les cinq ans[311], ce qui réduit un peu plus leur disponibilité.

[310] Cahier des charges – Base de données nationale d'abattage de bovins.
[311] Arrêté du 9 déc. 2009, préc., art. 6.

89- **Conclusion de la section.** De nombreuses données produites par le secteur agricole au cours d'une mission de service public, que ce soit pour sa réalisation ou pour la recherche scientifique, sont soumises au régime d'ouverture des données publiques. Les agriculteurs ne sont pas soumis à une telle obligation, mais certaines données collectées sur leur champ ou dans leur ferme intéressent l'Administration et les chercheurs. C'est pourquoi certaines réglementations obligent à fournir ces données pour la réalisation de missions de service public comme pour la réalisation des statistiques agricoles, par exemple. D'autres, en revanche, ne font pas l'objet d'une obligation d'ouverture et restent difficilement accessibles. Le Règlement sur les données de 2022 pourrait bientôt contraindre les acteurs privés du secteur agricole à ouvrir certaines des données qu'ils collectent ou produisent, à condition toutefois que cette ouverture réponde à un besoin exceptionnel prévu dans le Règlement. Aussi, les agriculteurs ne devraient pas être trop inquiétés par cette obligation.

Section 2. La mise en œuvre de l'ouverture des données agricoles publiques

90- L'article 15 de la Déclaration des droits de l'homme et du citoyen de 1789 proclame que « *la Société a le droit de demander compte à tout Agent public de son administration* ». L'ouverture et l'accès aux données contribuent à la transparence de la vie publique ainsi exigée par le bloc de constitutionnalité. Depuis quelques années, la question de l'ouverture des données publiques, aussi appelées politique d'*Open Data*, est devenue un sujet brûlant[312]. Tout un processus juridique s'est amorcé depuis la fin des années 1970 afin de favoriser la transparence de la vie publique. Cette volonté d'ouverture des données a fait l'objet d'un encadrement juridique qui repose sur l'articulation de deux régimes cumulatifs[313]. Le premier est au centre du régime de l'accès aux documents administratifs — les données répondent aux conditions de la mise à disposition des informations par l'Administration, le second régime est celui de la réutilisation des données publiques[314]. L'objectif est de valoriser ces données, les moderniser, simplifier l'administration[315] et favoriser leur réutilisation. Il convient donc, dans un premier temps, d'envisager le principe du droit d'accès aux données agricoles publiques (**§1**) pour, dans un second temps, s'intéresser aux limites du droit d'accès aux données agricoles publiques (**§2**).

[312] YOLKA, P., « *Open Data* : L'ouverture c'est l'aventure », *AJDA*, 2016, p. 79.
[313] CLUZEL-METAYER, L., « La loi pour une république numérique : l'écosystème de la donnée saisi par le droit », *AJDA*, 2017, p. 340.
[314] Voir *infra*, n°410 et s.
[315] CDC, *Les données du ministère de l'agriculture et de l'alimentation : un potentiel à mieux explorer*, 2020, p. 153.

§1. *Le principe du droit d'accès aux données agricoles publiques*

91- Afin d'envisager la mise en œuvre de l'ouverture de l'accès aux données agricoles publiques, il convient d'envisager, dans un premier temps, le droit d'accès (**I**). Dans un second temps, il sera nécessaire de s'intéresser à la construction d'un service public de la donnée (**II**).

I. Le droit d'accès

92- Tout d'abord, il convient d'envisager la construction du droit d'accès aux données publiques (**A**). Ensuite, il faudra s'intéresser à la mise en œuvre du droit d'accès (**B**).

A. La construction du droit d'accès aux données publiques

93- Dans un premier temps, il est nécessaire d'analyser la théorie droit d'accès (**1**). Dans un second temps, il sera important d'étudier la reconnaissance du droit d'accès (**2**).

1. La théorie du droit d'accès

94- Il semble que la théorie du droit d'accès développée par M. J. Rifkin corresponde à l'organisation de l'accès aux données publiques par l'État. Il est question en effet d'octroyer aux personnes « *un droit individuel de ne pas être exclu de l'usage et de la jouissance des ressources productives accumulées par toute la société* »[316]. La « logique de l'accès est présentée comme le « *substitut postmoderne au modèle de la propriété privée* »[317]. Aussi, le droit d'accès étant une prérogative du droit du propriétaire, il serait ainsi laissé à d'autres usagers[318]. C'est donc une manière de « *réinterpréter le droit de propriété comme un droit d'administrer l'accès aux biens est, au fond, une traduction du droit que le propriétaire a de contrôler sa chose, droit vu comme une relation sociale plutôt que comme un simple droit de préserver son indépendance à l'égard des autres* »[319]. Appliqué aux données publiques, les administrés deviennent alors des créanciers de l'Administration en raison de leur droit d'accès

[316] RIFKIN, J., *L'âge de l'accès, La nouvelle culture du capitalisme*, La découverte, Poche, 2005, pp. 304 et s.
[317] ROCHFELD, J., « Penser autrement la propriété : la propriété s'oppose-t-elle aux "communs" ? », *RIDE*, 2014/3 (t. XXVIII), pp. 351 à 369.
[318] ROCHFELD, J., « Entre propriété et accès : La résurgence du commun », *op. cit.*, p. 86.
[319] RIFKIN, J., *L'âge de l'accès, op. cit.,* p. 304.

et de réutilisation[320]. Par conséquent, la propriété « *repensée par l'accès* »[321] permet d'inclure « *en offrant à tous l'accès à des biens déterminés* »[322]. Néanmoins, le droit d'accès présente plusieurs difficultés. La première réside dans la détermination des ressources, il s'agit alors de se demander quelles ressources doivent faire l'objet d'un droit d'accès et sur quels fondements. La seconde repose sur celle de définir les bénéficiaires de la ressource : s'agit-il de ceux qui ont participé à son avènement, ou bien de tous ceux qui en ont besoin ? La troisième difficulté concerne les débiteurs du droit d'accès à la ressource afin de savoir qui doit ouvrir l'accès à la ressource et comment[323]. Parfois encore, des enjeux contradictoires viennent perturber la mise en place des droits d'accès aux données. Il en va ainsi des données de la recherche scientifique[324].

2. La reconnaissance du droit d'accès

95- **Changement de paradigme.** Nous assistons à un changement de paradigme et au développement du droit d'accès. En effet, d'un circuit initialement fermé, avec une conception patrimoniale, se développe aujourd'hui un véritable droit d'accès et de diffusion des données *via* la politique d'ouverture des données publiques. Le principal objectif est de créer un marché européen de l'information[325]. À cette fin, l'information et la donnée ne font pas l'objet d'une propriété publique[326] et doivent pouvoir circuler.

96- **Droit d'accès et commun.** À la lecture de la définition de l'*Open Data* retenue dans « *The Open Data Institute* » de H. Verdier et M. Murciano[327], l'ouverture des données publiques a été conçue comme l'administration d'un commun. Le commun c'est « *[l'] ensemble de ressources en accès partagé et collectivement gouverné au moyen d'une structure de gouvernance assurant une distribution des droits et des obligations entre les participants au commun (commoners) et visant à l'exploitation ordonnée de la ressource, permettant sa reproduction*

---

[320] TARLET, F., *Les biens publics mobiliers*, *op. cit.*, n°749 et s., pp. 517 et s.
[321] CRETOIS, P., « La propriété repensée par l'accès », *RIDE*, 2014/3 t. XXVIII, pp. 319 à 334.
[322] ROCHFELD, J., « Entre propriété et accès : La résurgence du commun », *op. cit.*, p. 81.
[323] *Ibid.*, p. 86 ; selon certains auteurs, la meilleure solution pour exploiter des droits d'accès aux données publiques soit le *copyleft*, XIFARAS, M., « Le copyleft et la théorie de la propriété », Association Multitudes, *Multitudes*, 2010/2, n°41, pp. 50 à 64.
[324] Voir *supra*, n°59 et s.
[325] TERESI, L., « L'*Open Data* et le droit de l'Union européenne (1) », *AJDA*, 2016.
[326] Voir *supra*, n°53.
[327] VERDIER, H. et MURCIANO, C., « Les communs numériques, socle d'une nouvelle économie politique », *Esprit* 2017/5 (mai), pp. 132 à 145 : Selon *The Open Data Institute* « *Les données ouvertes (Open Data) sont des données accessibles, disponibles dans un format lisible par une machine et pourvues d'une licence qui universalise leur accès, leur partage et leur utilisation à des fins commerciales ou non* ».

dans le long terme »[328]. Aussi, pour organiser l'ouverture et le partage des données publiques, l'État administre le commun, les données publiques, et offre un droit d'accès aux administrés. La donnée comme « commun » permet d'offrir « *à tous l'accès à des biens déterminés* »[329]. À ce propos, M. P. Dardot et M. le Professeur C. Laval considèrent que les communs sont inappropriables[330].

B. La mise en œuvre du droit d'accès

97- S'il faut envisager, dans un premier temps, le contenu du droit d'accès (**1**), il faudra, dans un second temps, analyser ses conditions d'application (**2**).

1. Le contenu du droit d'accès

98- **Source du droit d'accès aux données publiques**. À la lecture de la loi pour une République Numérique et des articles L. 300-1 et suivants du CRPA, il apparaît que le régime des données publiques a été intégré dans celui des documents administratifs. Aussi, afin d'envisager le contenu du droit d'accès aux données publiques, faut-il avant toute chose s'intéresser à celui des documents administratifs. Or, le droit d'accès aux documents administratifs implique deux régimes simultanés. D'un côté, chacun dispose du droit d'obtenir la communication des documents publics détenus par l'Administration et d'un autre, celle-ci a l'obligation de publier les documents qu'elle a en sa possession. Par conséquent, l'information est à la fois quérable et portable. En effet, l'article L. 311-1 du CRPA oblige les « administrations » à publier en ligne ou à communiquer les documents qu'elles détiennent aux personnes qui en font la demande. La loi pour une République numérique est venue modifier la logique de l'accès aux documents administratifs en ajoutant une obligation pour les administrations consistant dans le fait de diffuser spontanément ces documents. En ce qui concerne le champ d'application de la communication et de la diffusion des données publiques, ainsi que leurs modalités, nous renvoyons aux ouvrages qui traitent de ces questions[331].

---

[328] CORIAT B., « Communs (approche économique) », in CORNU, M., ORSI, F. et ROCHFELD, J., ss. dir., *Dictionnaire des biens communs*, PUF, 08/2017, pp. 299 à 322, spéc. p. 300.
[329] ROCHFELD, J, « Entre propriété et accès : La résurgence du commun », in BELLIVIER, F., ss. dir., *La Bioéquité* Autrement, Frontières, 2009, pp. 69 à 87, spéc. p. 81.
[330] DARDOT, P. et LAVAL, C., *Commun. Essai sur la révolution au XXe siècle*, Paris, La Découverte, 2014.
[331] Voir BOURGEOIS, M., *Droit de la donnée, principes théoriques et approche pratique*, Lexis Nexis, 2017, pp. 300 et s.

99- **Titularité du droit**. Au titre de l'article L. 300-1 du CRPA « *le droit de toute personne à l'information est précisé et garanti par les dispositions des titres I°, III et IV du présent libre en ce qui concerne la liberté d'accès aux documents administratifs* ». Ce droit est donc reconnu à toute personne physique ou morale, sans autre considération. Néanmoins, la question s'est posée pour les personnes publiques de savoir si elles avaient accès au même titre que les personnes privées aux documents administratifs. La CADA estimait que la loi de 1978 ne s'appliquait qu'aux administrés, ce qui excluait de fait les personnes publiques. Elle considérait que la loi CADA n'avait pas vocation à régir les transmissions de documents entre autorités administratives[332]. La Cour d'appel Administrative de Nancy avait estimé le contraire dans un arrêt du 2 février 2009[333]. La loi pour une république numérique de 2016 est venue élargir l'interprétation du texte en considérant que les personnes publiques ont accès aux documents administratifs et donc aux données publiques de la même manière que les personnes privées. Pour cela, l'accès doit être donné à des fins d'accomplissement de mission de service public autres que celle pour les besoins de laquelle les documents ont été produits ou reçus[334]. De toute évidence, il existe désormais une véritable injonction d'ouverture de l'accès aux données publiques.

2. Les conditions de l'accès

100- **Diffusion des données publiques**. Le droit d'accès aux données publiques n'est plus seulement un simple accès sur demande, mais il s'agit bien d'imposer la mise à disposition des données par les personnes en charge d'une mission de service public. Ces personnes en charge d'une mission de service public, ici nommées « administrations », sont alors chargées d'une véritable mission qui est de diffuser les données de la manière « *la plus large possible* », dans « *une démarche proactive* »[335]. L'obligation de diffusion conditionne donc l'accès aux données publiques.

D'une part, le volet de diffusion contenu dans le CRPA permet aux administrations de diffuser les documents administratifs qu'elles produisent ou reçoivent[336]. D'autre part, il impose aux administrations, à certaines conditions, de diffuser : 1° les documents qu'elles

[332] CADA, avis n°20123064, 13 sept. 2012.
[333] CAA Nancy, 2 févr. 2009 : req. n°07NC00604, inédit ; Rec.
[334] BECET, J.-M., « Communication des documents des collectivités territoriales au public : Régime général », *op. cit.*, n°75 à 84.
[335] *Ibid.*, p. 13.
[336] CRPA, art. L. 312-1.

communiquent en application des procédures prévues par le CRPA, ainsi que leurs versions mises à jour ; 2° les documents qui figurent dans le répertoire des informations publiques ; 3° les bases de données, mises à jour de façon régulière, qu'elles produisent ou qu'elles reçoivent et qui ne font pas l'objet d'une diffusion publique par ailleurs ; 4° les données, mises à jour de façon régulière, dont la publication présente un intérêt économique, social, sanitaire ou environnemental. Ces dispositions ne devraient pas être modifiées par la directive PSI III puisque celle-ci ne vise que le volet réutilisation des données publiques.

101- **Conditions de mise à disposition des données publiques.** Sous réserve du secret, les administrations doivent publier les bases de données mises à jour de façon régulière et les données mises à jour de façon régulière, dont la publication présente un intérêt économique, social, sanitaire ou environnemental sous un format électronique[337]. Leur mise à disposition doit être effectuée en ligne dans des standards ouverts afin que les données puissent être réutilisées et exploitées librement[338]. Les standards ouverts sont définis comme des protocoles[339] « *de communication, d'interconnexion ou d'échange et tout format de données interopérables et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre* »[340]. Afin d'assurer l'interopérabilité[341] au sein des systèmes d'information de l'Administration, chaque protocole doit se conformer à la dernière version en vigueur du référentiel général d'interopérabilité (RGI)[342]. En revanche, les bases de données qui font déjà l'objet d'une diffusion par ailleurs sortent du cadre de cette obligation de diffusion puisqu'elles sont déjà accessibles. Cette obligation de diffusion n'est pas sans limites[343]. En outre, cette véritable mission de diffusion à la charge de l'Administration n'est pas sans conséquence, dans la mesure où elle repose sur un principe de gratuité[344].

---

[337] CRPA, art. L. 312-1-1.

[338] CRPA, art. L. 300-4 : « *Toute mise à disposition effectuée sous forme électronique en application du présent livre se fait dans un standard ouvert, aisément réutilisable et exploitable par un système de traitement automatisé* ».

[339] ROBIN, A., *Droit des données de la recherche, op. cit.*, n°221, p. 169.

[340] Loi n°2004-575, 21 juin 24 pour la confiance en l'économie numérique : *JORF*, 22 juin 2004, art. 4 ; LRN, art.4.

[341] Sur l'interopérabilité, voir *infra*, n°537 et 663 et s.

[342] Version 2.0 du RGI, arrêté du 20 avr. 2016 : *JORF* n°0095 du 22 avr. 2016 ; Ord. n°2005-1516, 8 déc. 2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, art. 11 : le « *RGI fixe les règles techniques permettant d'assurer l'interopérabilité des systèmes d'information. Il détermine notamment les répertoires de données, les normes et les standards qui doivent être utilisés par les autorités administratives. Les conditions d'élaboration, d'approbation, de modification et de publications de ce référentiel sont fixées par décret* ».

[343] Voir *infra*, n°112 et s.

[344] CLUZEL-METAYER, L., « L'ouverture des données publiques », in AFDA, ss. dir., *Le droit administratif au défi du numérique*, Dalloz, 2019, p. 13.

II. La construction d'un service public d'ouverture de la donnée

102- Tout d'abord, il est nécessaire de comprendre les effets de la création d'un service public de la donnée (**A**) pour, ensuite, envisager le prélude de l'État-plateforme (**B**).

A. Les effets de la création d'un service public de la donnée

103- Il est nécessaire de s'intéresser aux enjeux (**1**) et aux conséquences (**2**) de la création d'un service public de la donnée.

1. Les enjeux de la reconnaissance d'une mission de service public de la donnée

104- **Principe du service public de l'ouverture des données de référence.** Pour assurer la pérennité du service public et l'obtention d'une information claire pour les administrés, l'ouverture de l'accès aux données publiques ne doit pas s'opérer sans concession. Aussi, elle doit obligatoirement se faire de manière qualitative par la mise à disposition des données de référence. Ce n'est qu'à cette condition que l'on peut assurer la fiabilité des données et des informations et ainsi permettre d'en tirer toutes leurs utilités. C'est ce que relève Mme la Professeure L. Cluzel-Metayer : « *l'utilisation de données parfaitement fiables est à la fois un levier économique, mais aussi un outil d'amélioration de l'action publique et du service rendu au citoyen* »[345]. Donc, le service public de la donnée se manifeste par la mise à disposition des données publiques à titre gratuit et par le droit de réutilisation.

105- **Mise en œuvre de l'ouverture des données de référence.** Le meilleur moyen d'offrir ce niveau de qualité à l'échelle nationale est de construire un véritable service public de la donnée. Ceci permet de créer une injonction d'ouverture des données publiques de manière qualitative. La première impulsion en ce sens date de 2016 avec la loi pour une République numérique qui a créé un véritable service public de la donnée évolutif. S'il est aujourd'hui limité aux données de référence qui représentent seulement neuf jeux de données[346], l'objectif est d'en ouvrir à terme une cinquantaine, mais aussi de permettre une ouverture plus sélective dans une logique

[345] *Ibid.*, pp. 20 à 21.

[346] Base d'adresses nationales (BAN), Base Sirene des entreprises et de leurs établissements (SIREN, SIRET), Code officiel géographique (COG), Plan cadastrale informatisé (PCI), Registre parcellaire graphique (RPG), Référentiel de l'organisation administrative de l'État, Référentiel à grande échelle (RGE), Répertoire national des associations (RNA), Répertoire opérationnel des métiers et des emplois (ROME).

différente de l'*Open Data*. Il s'agirait d'ouvrir à la « *bonne* » personne. Aujourd'hui, il semble que le choix qui a été fait de limiter dans un premier temps le service public est dû à la crainte d'un échec en cas d'ouverture trop grande des données publiques comme cela a été le cas en Grande-Bretagne par exemple avec le projet National Information Infrastructure (NII)[347], qui par manque de structure et de priorisation n'a pas pu gérer les 233 jeux de données fournies. L'État français a donc pris le parti d'ouvrir les données publiques secteur par secteur plutôt que d'opérer en une ouverture généralisée. Également, il était plus simple pour les administrations de diffuser les données qu'elles produisaient elles-mêmes[348]. Par conséquent, même si « *l'ouverture des données publiques, telle que mise en œuvre depuis 2005, n'a jamais obtenu le "label service public" de la part du législateur, […] elle en a sans doute tous les attributs* »[349].

2. Les conséquences de la création d'un service public de la donnée sur le régime de l'ouverture des données publiques

106- Le fait de reconnaître l'ouverture des données publiques comme un service public aura d'importantes conséquences en termes de régime applicable à l'ouverture de ces données. En effet, un service public doit respecter plusieurs principes qui pour certains ont valeur constitutionnelle. Ainsi, le service public doit respecter les principes de continuité, d'égalité et de mutabilité. D'abord, le principe de continuité a valeur constitutionnelle depuis la décision 79-105 DC du 25 juillet 1979[350]. Ce principe repose sur le fait que le service public doit répondre aux besoins d'intérêt général sans interruption. Ensuite, le principe d'égalité procède du principe d'égalité de tous devant la loi proclamée par la Déclaration des droits de l'homme et du citoyen de 1789. Chacun doit pouvoir accéder de manière égale au service, participer de manière égale aux charges financières résultant du service et être traité de la même façon que les autres usagers. Enfin, le principe de mutabilité est un « *corollaire du principe de continuité* »[351]. Il s'agit d'assurer un service de manière qualitative. Ainsi, le service public doit pouvoir muter et s'adapter aux évolutions de la société, en suivant les besoins des usagers et les évolutions techniques. Par conséquent, le service public de la donnée doit respecter ces mêmes

[347] VERDIER H., *La donnée comme infrastructure essentielle*, Rapport au premier ministre sur la donnée dans les administrations 2016-2017 de l'administrateur général des données, La documentation française, p. 47.
[348] CLUZEL-METAYER, L. « La construction d'un service public de la donnée », *op. cit.*
[349] *Ibid.*
[350] C. const., Décision 79-105, 25 juill. 1979, loi modifiant les dispositions de la loi n°74-696 du 7 août 1974 relatives à la continuité du service public de la radio et de la télévision en cas de cessation concertée du travail : *JORF* du 27 juill. 1979.
[351] Fiche thématique : La notion de service public, 30 juin 2018 [www.servicepublic.fr].

principes. Comme le relève M. le Professeur G. Guglielmi, « *les jeux de données doivent être mis à jour, demeurer à toute époque sur un site* »[352] pour assurer le principe de continuité. Pour respecter le principe d'égalité, les jeux de données doivent également « *être accessibles sans rupture d'égalité en termes notamment d'accès (le filtrage par adresses IP étrangères ne serait pas admissible, le site doit être optimisé pour tout logiciel de navigation et n'exclure aucun usager)* »[353]. Ce qui implique donc l'interopérabilité des logiciels et applications de partage des données. Enfin, le service public de la donnée doit respecter le principe de mutabilité en s'adaptant aux changements des conditions technologiques (formats, standard, etc.). Mais encore, il faut relever l'existence d'autres principes comme la qualité, l'accessibilité, l'efficacité et la sécurité[354].

B. Le prélude de l'État-plateforme

107- Il faut envisager, tout d'abord, la mutation du service public (**1**) pour, ensuite, étudier la notion d'État-plateforme (**2**).

1. La mutation du service public

108- Afin d'ouvrir l'accès aux données, l'administration conserve la gouvernance de celles-ci dans l'intérêt général, mais aussi pour conserver « *sa souveraineté informationnelle* »[355]. À cette fin, la mission *Etalab* a été conçue en 2011 dans l'objectif de « *coordonner […] la politique des administrations en la matière et de concevoir un portail ministériel unique de mise à disposition des données : Data.gouv.fr* »[356]. Néanmoins, la politique d'*Open Data*, et plus particulièrement le service public de la donnée, ont été construits de manière à laisser la place à l'initiative privée. Ce qui nécessite une gouvernance ouverte du commun numérique. Par conséquent, l'idée « *d'un service public sans administration, gouverné par la multitude, commence à se dessiner* »[357]. L'administration a donné l'impulsion afin de montrer ce qui doit être fait avant de laisser la main aux entreprises privées. L'ouverture des données « *entraîne [alors] une mutation des*

[352] GUGLIELMI, G., « *Open Data* et service public : Les données publiques ouvertes sont-elles un service public ? », in BOURCIER, D. et FILIPPI (De), P., ss. dir., *Open Data & Big Data, Nouveaux défis pour la vie privée*, mare & martin, 2016, pp. 53 et s.
[353] *Ibid.*
[354] *Ibid.*
[355] VERDIER, H., « La donnée comme infrastructure essentielle », *op. cit.*, p. 16.
[356] CLUZEL-METAYER, L. « L'ouverture des données publiques », *op. cit.*, p. 12
[357] COLIN N. et VERDIER H., *L'âge de la multitude, Entreprendre et gouverner après la révolution numérique*, Armand Colin, 2015.

formes traditionnelles du service public, plus encore elle transforme l'architecture de l'État »[358]. Cette mutation tend donc vers l'État-plateforme.

2. La notion d'État-plateforme

109- Définition. L'État-plateforme est une notion inventée par M. T. O'Reilly, reprise par deux économistes en France, M. H. Verdier et M. N. Colin. Il s'agit d'une « *infrastructure propre à faciliter les échanges de données et la création par le biais d'API* (Interface de programmation d'application) *qui doivent conduire à l'émergence de nouveaux services numériques* »[359]. Autrement dit, « *les croisements de données effectuées dans le cadre des API vont déboucher sur la production de nouveaux services numériques, utilisant l'État comme plateforme d'échange* »[360]. C'est pour ces économistes « *[l'] incarnation d'une souveraineté retrouvée au centre du jeu numérique* »[361]. Ainsi, « *il ne s'agit plus seulement de rendre accessibles les données publiques, par une politique volontariste d'ouverture, mais de les faire circuler et de permettre leur réutilisation, en les intégrant à un vaste système d'échange de données "un écosystème" regroupant à la fois les producteurs de données, État, collectivités territoriales, acteurs privés, associations et réutilisateurs* »[362]. Cette plateformisation de l'État se manifeste notamment par l'obligation incombant aux administrations et aux opérateurs publics de publier un registre des informations publiques (RIP) qui répertorie toutes les bases de données détenues et ouvertes au public. Cette publication répond à l'obligation légale de la loi du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public, modifiée par l'ordonnance 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques[363].

110- Développement de l'État-plateforme. Le développement des API (*Application Programing Interfaces*), c'est-à-dire des interfaces d'échange de données entre logiciels qui « *assurent le croisement automatique de données hétérogènes, provenant de diverses sources, publiques et privées, sans intervention humaine* »[364], tout en regroupant dans un écosystème à la fois les producteurs de donnes et les réutilisateurs. Ainsi, « *il ne s'agit plus seulement de rendre*

---

[358] CHEVALLIER, J., « Vers l'État-plateforme ? », *RFAP*, n°167, 2018/3, pp. 627 à 637.
[359] COLIN, N. et VERDIER, H., *L'âge de la multitude*, *op. cit.* p. 33.
[360] CHEVALLIER, J., « Vers l'État-plateforme ? », *op. cit.*, p. 630.
[361] COLIN, N. et VERDIER, H., *op. cit.*, p. 33.
[362] CHEVALLIER, J., « Vers l'État-plateforme ? », *op. cit.*, p. 630.
[363] https://agriculture.gouv.fr/informations-publiques
[364] CHEVALLIER, J., « Transformation numérique. Les nouveaux développements de l'État plateforme », *JCP G*, n°19, 11 nov. 2020, doctr. 611.

accessibles les données publiques, par une politique volontaire d'ouverture, mais de les faire circuler et de permettre leur réutilisation, en les intégrant à un vaste système d'échange de données »[365]. Aussi, l'APIsation est à la fois « support et vecteur de l'édification de l'État-plateforme »[366].

111- **API-AGRO[367].** Dans le secteur agricole, la plateforme API-AGRO[368] est construite sur ce modèle et permet le partage et la réutilisation des données agricoles. En effet, API-AGRO est une plateforme ouverte sur laquelle est déposée de nombreuses bases de données provenant de sources multiples. Il peut s'agir d'instituts de recherche, d'entreprises privées ou bien encore des services de l'État. Ainsi, elle permet d'organiser l'ouverture et le partage des données au moyen d'API plus ou moins ouvertes selon le degré de sensibilité des données.

§2. *Les limites du droit d'accès aux données agricoles publiques*

112- Le droit d'accès comporte plusieurs limites qu'il convient d'envisager puisqu'elles peuvent avoir un impact sur l'accès aux données agricoles publiques. En effet, il existe une première limite relative aux exceptions à la communication des données (**I**). Une seconde limite impose la privatisation de certaines données (**II**).

I. Les exceptions à la communication des données

113- L'ouverture des données peut se faire tant que leur communication ne porte pas atteinte à un secret (**A**) ou à un droit de propriété intellectuelle (**B**).

A. Les données non communicables en raison d'un secret

114- La loi distingue deux types de données protégées par le secret. Il y a celles qui ne peuvent être communiquées au public (**1**) et celles qui ne peuvent être communiquées aux tiers (**2**).

[365] *Ibid.*
[366] *Ibid.*
[367] Pour des développements sur la plateforme API-AGRO, voir *infra*, n°282 et s., 470, 480 et s., 483, 495 et s.
[368] Voir *infra*, n°282.

1. Les données non communicables au public

115- Certaines données ne sont pas communicables soit en raison de leur nature[369] s'il s'agit de documents préalables à une décision, soit en raison des conséquences que leur divulgation pourrait avoir pour la sécurité publique ou dans l'intérêt public[370]. Il faut noter que la Loi pour une République Numérique de 2016 a eu pour conséquence de rétrécir le champ des données secrètes[371] puisque désormais les codes sources utilisés par les administrations sont des documents communicables[372]. De même, les règles définissant les traitements algorithmiques et leurs caractéristiques principales doivent être communiquées à l'intéressé qui en fait la demande[373], voire être publiées en ligne[374] dès lors que ces algorithmes fondent une décision individuelle[375]. L'article L. 213-2 du Code du patrimoine prévoit plusieurs délais à expiration desquels les documents sont communicables selon l'importance de ces informations en termes de sécurité publique et de protection de la vie privée.

Parmi les données publiques du secteur agricole, à savoir les données de la politique agricole commune (PAC), les données environnementales ou encore les données de la recherche scientifique, aucune n'entre dans cette catégorie des données non communicables au public. En effet, aucune n'est de nature à interdire sa communication au sens de l'article L. 311-5, al. 1er du CRPA. De même, leur divulgation n'aura pas pour effet de porter atteinte à la sécurité publique ou à l'intérêt public au sens de l'article L. 311-5, al. 2 du CRPA.

2. Les données non communicables aux tiers

116- Certaines données ne peuvent être communiquées qu'aux personnes intéressées. Aussi, les tiers sont exclus de la communication. La loi du 17 juillet 1978 prévoyait déjà une exclusion de communication aux tiers des documents relatifs au « secret en matière commerciale et industrielle ». La loi n°2018-670 du 30 juillet 2018 relative à la protection du secret des affaires

---

[369] CRPA, art. L. 300-5, al. 1° : « *Les avis du Conseil d'État et des juridictions administratives, les documents élaborés ou détenus par l'autorité de la concurrence, les documents élaborés ou détenus par la Haute Autorité pour la transparence de la vie publique, les documents préalables à l'élaboration du rapport d'accréditation des établissements de santé, les documents préalables à l'accréditation des personnels de santé, les rapports d'audit des établissements de santé, les documents réalisés en exécution d'un contrat de prestation de services exécuté pour le compte d'une ou de plusieurs personnes déterminées* ».

[370] CRPA, art. L. 300-5, al. 2° : secret défense, secrets professionnels, etc.

[371] CLUZEL-METAYER, L., « L'ouverture des données publiques », *op. cit.*, p. 19.

[372] CRPA, art. L. 300-2.

[373] CRPA, art. L. 311-3-1 et R. 311-1-1.

[374] CRPA, art. L. 312-1-3.

[375] BOURCIER, D. et FILIPPI (De), P., « Transparence des algorithmes face à l'*Open Data :* quel statut pour les données d'apprentissage ? » *RFAP*, 2018, pp. 525 à 538.

a rassemblé ces différents types de secret sous le terme de « secret des affaires »[376]. Les observateurs ne manquent pas de relever que les contours de cette exception sont difficiles à tracer[377]. L'objectif est de parvenir à un équilibre entre « *la circulation de l'information suffisante au bon fonctionnement des marchés* »[378] sans pour autant que cela ne porte atteinte à la concurrence. Le secret des affaires est aujourd'hui défini à l'article L. 151-1 du Code de commerce[379] issu de la loi n°2018-670 du 30 juillet 2018 relative à la protection du secret des affaires, transposant la directive 2016/943/UE du 8 juin 2016 sur le secret des affaires. Cette dernière est elle-même inspirée de l'article 39 de l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC). Aussi, le secret des affaires concerne « *toute information répondant aux critères suivants : 1° elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité ; 2° elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ; 3° elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret* »[380]. La CADA a eu l'occasion de reconnaître le secret des affaires comme un obstacle à la diffusion des données publiques dans un avis du 25 octobre 2018[381]. Le Conseil d'État en a conclu de même dans l'arrêt ARAFER[382].

Dans la mesure où des données agricoles répondraient aux conditions d'un secret des affaires, alors elles ne seraient pas communicables aux tiers au sens de l'article L. 311-6 du CRPA. Ce serait le cas notamment pour des données d'exploitation portant sur les doses de produits phytosanitaires utilisés ou sur les pratiques culturales qui feraient l'objet de protections adaptées pour conserver le secret par les exploitants agricoles. Ainsi, la collecte de ces données par les administrations pour des enquêtes statistiques ou afin de recherche scientifique ne pourraient faire l'objet d'une diffusion en l'état. Ces informations devraient alors préalablement

---

[376] Sur le secret des affaires, voir *infra*, n°346 et s.
[377] CE, *Rapport public annuel*, 1995 p. 102 ; CADA, conseil n°20071222, 3 mai 2007.
[378] LALLET, A. et NGUYEN DUY, P., « Communication des documents administratifs, Restrictions au droit à communication du régime général », *Rép. cont. adm*, n°231, juin 2019, n°231.
[379] CADA, avis n°20183478, 21 mai 2019 et CADA, avis n°20183650, 28 févr. 2019 ; voir *infra*, n°350.
[380] C. com., art. L. 151-1.
[381] CADA avis n°445, 25 oct. 2018 et CADA, conseil n°20193210, 23 avr. 2020, *Mairie de Versailles.*
[382] CE, 2ème et 7éme ch. réunies, 16 févr. 2018, ARAFER, 403 508 : « *La liste des informations demandées par l'ARAFER n'était pas de nature à porter atteinte au secret des affaires et qu'au demeurant une série de disposition destinées à imposer le respect des secrets protégés par la loi, constituaient en aval des garanties suffisantes pour assurer la préservation du secret des affaire sans faire obstacle en amont à la transmission d'information* » ; LOMBARD, M., « La régulation par la donnée », in AFDA, ss. dir., *Le droit administratif au défi du numérique*, Dalloz, 2019, p. 165.

à leur diffusion faire « l'*objet d'un traitement permettant d'occulter les éléments relevant du secret* »[383].

B. L'exception du droit de propriété intellectuelle sur les données agricoles publiques

117. Pour protéger les créations intellectuelles, des limites sont assignées au principe d'ouverture des données. Il peut arriver que la politique d'ouverture des données publiques rencontre la protection des œuvres par le droit de la propriété intellectuelle. À plusieurs reprises dans le Code des relations entre le public et l'administration, le législateur limite l'ouverture de l'accès aux données publiques dès lors qu'un tiers détient des droits de propriété intellectuelle dessus. L'article L. 311-4 dudit code précise que les documents administratifs sur lesquels des tiers détiennent des droits de propriété intellectuelle ne sont pas des informations communicables. Aussi, dès lors que les données contiennent des éléments protégeables par le droit d'auteur, il convient de faire la balance entre les intérêts en jeu. C'est pourquoi il est nécessaire d'envisager les conséquences d'un droit de propriété intellectuelle détenu par les tiers sur la communication des données publiques (**1**), avant de s'intéresser à l'inopposabilité des droits de propriété intellectuelle détenus par les administrations (**2**).

1. Le droit de propriété intellectuelle détenu par les tiers

118. **Quand la protection par le droit d'auteur rencontre l'accès des données publiques**. Le Code des relations entre le public et l'administration prévoit une première exception au libre accès des données publiques. En effet, l'article L. 311-4 dispose que « *les documents administratifs sont communiqués ou publiés sous réserve des droits de propriété intellectuelle* ». Il est alors nécessaire de faire la balance entre l'ouverture des données publiques et les droits de propriété intellectuelle sur les œuvres. Ce croisement entre deux droits fait naître certaines difficultés pour déterminer les informations publiques soumises à un droit de propriété intellectuelle. L'auteur d'une œuvre dispose d'un droit de propriété incorporelle du simple fait de sa création[384] et ce droit porte sur « *toutes les œuvres de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination* »[385]. La seule condition pour

[383] ROBIN, A., *Droit des données de la recherche*, *op. cit*, n°223, p. 170.
[384] CPI, art. L. 111-1.
[385] CPI, art. L. 112-1.

reconnaître une œuvre protégeable par le droit d'auteur, c'est son originalité. Par conséquent, toute œuvre exprimant l'empreinte de la personnalité de son auteur est protégée par le droit de la propriété intellectuelle. Or, la CADA a longtemps interprété les dispositions de l'article L. 311-4 du CRPA comme « *se bornant à rappeler que l'existence de droits de propriété littéraire ou artistique ne saurait légalement justifier le refus de communiquer un document administratif, mais a seulement des conséquences sur l'utilisation qui pourra en être faite par le demandeur* »[386]. Elle a alors retenu que les droits de propriété intellectuelle détenus par des tiers limitaient seulement les possibilités de réutilisation ultérieure d'un document administratif[387]. Il n'était en revanche pas possible de limiter la diffusion du document. La CADA ajoutait seulement l'obligation d'accompagner cette diffusion d'un rappel des restrictions qui s'attachent à son usage et les sanctions encourues. De la sorte, les usagers avaient connaissance de leur obligation de respecter les dispositions du Code de la propriété intellectuelle. Mais cette jurisprudence a évolué récemment.

119- **Condition de formalisme de la protection du droit d'auteur**. La position de la CADA sur la diffusion des œuvres a été infirmée par le Conseil d'État dans une décision du 8 novembre 2017[388]. En effet, dans cet arrêt, le Conseil d'État réinterprète l'article L. 311-4 du CRPA et l'article 9 de la loi du 17 juillet 1978 en retenant que « *ces dispositions impliquent […] au sens de l'article L. 121-2 du CPI, de recueillir l'accord de leur auteur* ». Le juge pour appuyer sa décision prend en compte le droit moral de l'auteur sur son œuvre. Aussi, si le droit patrimonial ne permet pas à l'auteur de s'opposer à la communication du document administratif, mais seulement à sa réutilisation par des tiers, le droit moral peut quant à lui être mis en œuvre. Effectivement, l'article L. 111-1 du CPI dispose que « *l'auteur d'une œuvre de l'esprit jouit sur cette œuvre […] d'un droit de propriété incorporel […] opposable à tous* ». Ce qui implique en principe que « *les tiers n'ont aucune possibilité, ne serait-ce que matérielle de s'opposer à la constitution du droit* »[389]. De ce fait, l'auteur a seul le droit de divulguer son œuvre[390], ce qui implique que la « *divulgation d'un document sans l'accord de son auteur, lorsque celui-ci n'a*

[386] CRPA, art. L. 311-4, Dalloz, Comm.
[387] CRPA, art. L. 321-2 ; CADA, conseil n°20061210, 16 mars 2006, *Président de la Cté urb. de Bordeaux* ; CADA, conseil n°20084340, 27 nov. 2008, *Maire de Maizières-lès-Metz*.
[388] CE, 10e et 9e ch. Réunies, 8 nov. 2017, *Association spirituelle de l'Église de scientologie Celebrity centre*, n°375704 ; note DELAUNAY, *AJDA* 2013. 1920 ; note COSTES L., *RLDI*. 2017 n°143 p. 30 ; note ROUSSEL S., *LGP*. 2017 n°44 p. 32 ; note CHIFFLOT N., *Procédures*. 2018 n°1 p. 37 ; note CARON C., *CCC* 2018 n°2 p. 34 ; comm. EVEILLARD G., *AJDA* 2018 n°3 p. 29 ; chron. EVEILLARD G., *JCP G* 2018 n°13 p. 621 ; note BRUGUIERE J.-M, *PI*. 2018 n°67 p. 38 ; chron. ROUAULT M.-Ch., *LPA*. 2018 n°81 p. 9 ; comm. BINCTIN N., FOULQUIER N., KALFLECHE G. et SORBARA J.-G., *PI*. 2018 n°68 p. 82 ; chron. MORAND-DEVILLER J., POULET F. et BOURDON P., *LPA* 2018 n°143 p. 12 ; note PETELIN T., *JCP E*. 2019 n°6 p. 40.
[389] PASSA, J., « L'opposition en droit de la propriété intellectuelle », *LPA*, 2007, n°68, p. 29.
[390] CPI, art. L. 121-2.

pas épuisé son droit d'opposition, porte atteinte à ce droit moral ». Ainsi, lorsqu'un document administratif est grevé d'un droit de propriété intellectuelle d'un tiers à l'Administration et que son auteur n'a pas épuisé son droit d'opposition, l'Administration doit demander son accord avant toute divulgation de l'œuvre lorsqu'elle n'a pas déjà fait l'objet d'une diffusion. Il est à noter que cette lecture du texte ne s'applique qu'aux tiers à l'Administration et que le Conseil d'État ne s'est pas prononcé pour les œuvres des agents publics régies à l'article L. 121-7-1 du CPI[391]. Il en va de même pour les bases de données détenues par des tiers. Quoi qu'il en soit, désormais « *l'Administration ne saurait diffuser des données protégées par le droit des tiers* »[392].

Aussi, dans le cas où des bases de données du secteur agricole seraient recouvertes d'un droit de propriété intellectuelle, elles ne pourraient donc être diffusées sans l'accord de leur auteur. Pour l'heure, il n'existe pas d'exemples de ce type dans le secteur agricole, les données produites par des acteurs privés ont vocation à rester privées. Aucune base de données produite par un acteur privé du secteur agricole et protégée par le droit d'auteur ne peut faire l'objet d'une communication publique sans son accord.

2. L'inopposabilité des droits de propriété intellectuelle détenus par les administrations

120- **Le principe d'un droit de propriété intellectuelle sur les bases des données publiques.** Si un véritable droit de propriété intellectuelle a d'abord été reconnu à l'Administration sur les bases de données qu'elle produisait[393], ce droit lui a ensuite été retiré. En effet, dans un premier temps, les administrations qui ont produit des bases de données ont revendiqué et obtenu la protection du droit *sui generis*[394] pour en contrôler l'extraction et la réutilisation[395]. Néanmoins, ce droit s'est rapidement heurté à la politique d'ouverture des données publiques[396]. Aussi, la

[391] « *Le droit de divulgation reconnu à l'agent mentionné au troisième alinéa de l'article L. 111-1, qui a créé une œuvre de l'esprit dans l'exercice de ses fonctions ou d'après les instructions reçues, s'exerce dans le respect des règles auxquelles il est soumis en sa qualité d'agent et de celles qui régissent l'organisation, le fonctionnement et l'activité de la personne publique qui l'emploie. L'agent ne peut : 1° S'opposer à la modification de l'œuvre décidée dans l'intérêt du service par l'autorité investie du pouvoir hiérarchique, lorsque cette modification ne porte pas atteinte à son honneur ou à sa réputation ; 2° Exercer son droit de repentir et de retrait, sauf accord de l'autorité investie du pouvoir hiérarchique* ».

[392] CLUZEL-METAYER, L., « L'ouverture des données publiques », *op. cit.*, p. 16.

[393] MAISL, H., « Régime de la protection juridique des bases de données publiques », *AJDA*, 1997, p. 189.

[394] Pour une étude détaillée du droit *sui generis*, voir *infra*, n°239 et s.

[395] BERNAULT C., LUCAS A. et LUCAS-SCHLOETTER A., *Traité de la propriété littéraire et artistique*, *op. cit.*, n°1430, p. 1104 ; MAISL, H., « Régime de la protection juridique des bases de données publiques », *op. cit.*, p. 189.

[396] Voir *supra*, n°92 et s.

« coexistence »[397] d'un droit sur les bases de données et de cette politique d'ouverture a fait l'objet d'une évolution jurisprudentielle et légale.

Tout d'abord, la circulaire du 14 février 1994 relative à la diffusion des données publiques[398] prévoyait que « *les données brutes élémentaires, sans mise en forme originale, ne sont en principe la propriété de personne ; en revanche, la valeur ajoutée par l'Administration est susceptible d'appropriation intellectuelle. Elle peut alors en céder l'usage dans les conditions prévues par la législation sur la propriété intellectuelle* ». À la lecture de ce texte, l'Administration pouvait donc se prévaloir d'un droit de propriété sur les bases de données qu'elle produisait. C'est d'ailleurs cette solution qui a été retenue dans l'arrêt *Direct mail promotion*[399] du Conseil d'État au sujet du répertoire S.I.R.E.N.E, reconnaissant un droit de propriété intellectuelle au profit de l'INSEE.

Cependant, une évolution textuelle et jurisprudentielle a modifié cette analyse. En effet, dans l'affaire *Notrefamille.com/Département de la Vienne*[400] du 8 février 2017, la société *Notrefamille.com* souhaitait réutiliser les données rassemblées dans les archives publiques concernant l'état civil du département de la Vienne. Or, le Conseil général avait délibéré contre l'extraction ou l'indexation systématiques des archives publiques[401] en reconnaissant le droit *sui generis* du département sur les bases de données d'état civil. La société avait alors saisi le tribunal administratif de Poitiers pour demander l'annulation de la décision du directeur général des services du département de la Vienne qui avait rejeté sa demande dans une décision du 31 janvier 2013[402]. La société avait interjeté appel de la décision devant la CAA de Bordeaux et par un arrêt du 26 février 2015, la CAA avait rejeté cet appel et confirmé la décision du tribunal administratif[403] sous l'empire des textes en vigueur. Un pourvoi a alors été formé devant le Conseil d'État pour demander l'annulation de l'arrêt. Or, entre temps, plusieurs textes avaient été modifiés par le législateur. En effet, les lois du 7 aout 2015 portant la nouvelle organisation territoriale de la République (loi NOTRe)[404], celle du 28 décembre 2015 relative

[397] CHERON, A., « La réutilisation des données publiques : Bases de données et *Open Data* (1) », *AJCT*, 2011.
[398] *JORF* n°42 du 19 févr. 1994.
[399] CE ass., 10 juill. 1996, *Sté Direct mail promotion*, n°168702.
[400] CE, 8 févr. 2017, nº 389806, *Sté NotreFamille.com*, préc.
[401] MOURIER, R., « *Open Data* vs droit de propriété intellectuelle » comm., ss. CE, 8 févr. 2017, nº 389806, *Sté NotreFamille.com*, Rec. CE, 27 févr. 2017, *Actualité du droit, Lamy*.
[402] TA Poitiers, 31 janv. 2013 : obs. L. C., *RLDI* 2013/92, 3059 ; note BRUGUIERE, J.-M., *JCP A* 2013, 2442.
[403] CAA Bordeaux, 4e ch., 26 févr. 2015, *Notrefamille.com* c/ *Département de la Vienne* : obs. BRUGUIERE J.-M., *PI*, 2015, p. 209.
[404] Loi n°2015-991 du 7 août 2015 portant la nouvelle organisation territoriale de la République (loi NOTRe) : *JORF* n°0182 du 8 août 2015.

à la gratuité et aux modalités de la réutilisation des informations du secteur public (loi Valter)[405] et celle du 7 octobre 2016 pour une République numérique (loi Lemaire)[406] prévoient désormais toutes un droit de réutilisation, même à des fins commerciales, des données de collectivités locales[407]. C'est ainsi que la loi Lemaire a modifié l'article L. 312-1-1, 3e du CRPA qui oblige désormais les administrations à publier « *les bases de données mises à jour de façon régulière qu'elles produisent ou qu'elles reçoivent, et qui ne font pas l'objet d'une diffusion publique par ailleurs* »[408]. Également, dorénavant l'article L. 321-3 du CRPA dispose que « *les droits des administrations ne peuvent faire obstacle à la réutilisation du contenu des bases de données que ces administrations publient en application de l'article précédemment cité* ». Par conséquent, en tenant compte de ces évolutions textuelles, le 8 février 2017, le Conseil d'État a censuré l'arrêt de la CAA de Bordeaux et a estimé que « *la loi du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'Administration et le public régit de manière complète les éventuels droits de propriété intellectuelle détenus par les personnes publiques sur les informations publiques, de telle sorte que le Code de propriété intellectuelle n'a pas lieu de s'appliquer* »[409]. Par cette décision, les droits de propriété intellectuelle applicables aux administrations sont neutralisés en présence de données publiques. C'est pourquoi « *en présence d'informations publiques, au sens de la loi du 17 juillet 1978 alors en vigueur, le département ne pouvait se fonder sur les droits tirés de sa qualité de producteur de base de données pour interdire l'extraction ou la réutilisation du contenu d'une telle base* »[410]. Désormais, donc, les administrations ne peuvent plus se prévaloir du droit de propriété intellectuelle sur les bases de données qu'elles produisent. Néanmoins, l'inapplicabilité du droit des producteurs de bases de données aux personnes publiques ne se limite qu'aux bases de données qui doivent être obligatoirement publiées par l'Administration[411]. Cette précision fait redouter une double atteinte à la diffusion et à la libre réutilisation des données publiques. D'une part, lorsque l'Administration détient des droits de propriété intellectuelle, comme un droit d'auteur sur des images contenues dans une base de données, elle peut s'opposer à la diffusion ou à la réutilisation de cette base. D'autre part, toutes les bases de données qui ne font pas

[405] Loi n°2015-1779 du 28 déc. 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public (loi Valter) : *JORF* n°0301 du 29 déc. 2015.
[406] Loi n°2016-1321 du 7 oct. 2016 pour une République Numérique : *JORF* n°0235 du 8 oct. 2016.
[407] VIVANT, M. et al., « Le droit *sui generis* du producteur d'une base de données ne peut s'opposer à la réutilisation des données publiques », *RLDI*, n°137, 1e mai 2017.
[408] CRPA, art. L. 312-1-1, 3e.
[409] FERAL-SCHUHL, C., ss. dir., *Cyberdroit, Le droit à l'épreuve de l'Internet*, Dalloz, 7e éd., 2018-2019, n°341.13.
[410] BERNAULT C., LUCAS A. et LUCAS-SCHLOETTER A., *Traité de la propriété littéraire et artistique*, *op. cit.*, n°1430, p. 1105.
[411] FERAL-SCHUHL, C., *id.*, n°341.49.

l'objet d'une publication obligatoire peuvent bénéficier du droit *sui generis*[412], c'est-à-dire lorsqu'elles ne répondent pas aux conditions de l'article L. 312-1-1, 3e du CRPA. En outre, la loi pour une République numérique de 2016 a prévu une exception dite « *Text and Data Mining* » qui permet « *aux chercheurs de fouiller des textes et des données incluses ou associées aux écrits scientifiques pour les besoins de la recherche publique à l'exclusion de toute finalité commerciale* »[413]. Cette exception démontre qu'un droit de propriété intellectuelle est possible sur les bases de données scientifiques.

II. La privatisation des données

121- La protection de la vie privée (**A**) constitue également un obstacle à la diffusion des données publiques (**B**).

A. La protection de la vie privée

122- Si la combinaison de deux régimes aussi diamétralement opposés, que ceux de l'ouverture des données publiques et de la protection de la vie privée, apparaît comme un véritable jeu d'équilibriste (**1**), il faut constater néanmoins que la protection de la vie privée prime sur l'ouverture de l'accès aux données publiques (**2**).

1. Le jeu d'équilibriste entre deux régimes initialement opposés

123- **Prise en compte des données privées dans la politique d'ouverture des données publiques.** La politique d'*Open Data* consiste en l'ouverture des données publiques afin, entre autres, de favoriser la transparence de la vie publique[414]. Néanmoins, il s'avère que parfois des données à caractère personnel sont intriquées dans des données ayant vocation à être mise à disposition, ce qui a pour conséquence de mettre en jeu l'exigence de protection de la vie privée[415]. Il est

---

[412] *Ibid.*

[413] ROBIN, A., « Les données scientifiques au prime du dispositif *Open Data* », *op. cit.*, n°222, p. 170 ; CPI, arts. L. 122-5, 10e et L. 3422-3, 5e.

[414] Loi n°2013-906, 11 nov. 2013 relative à la transparence de la vie publique et Loi n°2013-907, 11 oct. 2013 relative à la transparence de la vie publique.

[415] CEDH, art. 8 : « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* » ; Décret n°94-352 DC, 18 janv.1995 : « *La méconnaissance du droit au respect de la vie privée peut être de nature à porter atteinte à la liberté individuelle* » ; Loi n°70-643, 17 juill. 1970 : *JORF* 19 juill. 1970 ; C. civ., art. 9 : « *Chacun a droit au respect de sa vie privée* ».

alors question de rechercher un juste équilibre entre ces deux exigences démocratiques[416]. En 1995, le Conseil d'État préconisait dans son rapport public annuel de procéder à une harmonisation des lois régissant la transparence administrative[417] pour, notamment, intégrer l'aspect vie privée. Pourtant de prime abord, la politique d'ouverture des données publiques ne concernait pas les données personnelles, ce n'est que lors de la transposition de la directive 2003/98/CE[418] (PSI) par une ordonnance du 6 juin 2005[419] qu'elles ont fait leur entrée dans le texte. En effet, c'est au moment d'intégrer la possibilité de réutiliser des données publiques à d'autres fins que celles de la mission de service public pour laquelle les données ont été produites ou reçues[420] qu'il a fallu prévenir la réutilisation de données qui auraient un caractère personnel. Finalement, c'est la Loi pour une république numérique et le Règlement général sur la protection des données (RGPD) de 2016[421] qui ont modifié les règles relatives à l'ouverture des données publiques au regard des principes de la protection des données personnelles. Il apparaît ainsi que la « *protection de la vie privée prime sur l'exigence d'informations publiques* »[422].

2. La primauté de la protection des données personnelles et de la vie privée sur l'ouverture des données publiques

124- **Limites.** Si la protection des données personnelles paraît constituer un obstacle à la politique d'ouverture des données publiques, c'est en réalité une « *logique d'équilibre qui est aujourd'hui promue visant à faciliter la mise en œuvre du mouvement d'ouverture tout en permettant un meilleur encadrement des cas de réutilisation* »[423]. Deux réglementations forment une barrière à l'ouverture des données publiques. D'abord celle sur la protection des données personnelles qui ne concerne que les personnes physiques, ensuite, celle sur la protection de la vie privée qui s'applique aux personnes physiques et morales.

---

[416] BELORGEY, J.-M, « L'État entre transparence et secret », *Le Seuil*, Pouvoirs, n°97, 2001/2, pp. 25 à 32.
[417] GOUNIN, Y., « La réforme du droit d'accès aux documents administratifs », *AJDA*, 2000, p° 486 ; FERRARI, P., « Les droits des citoyens dans leurs relations entre les administrations, Commentaire générale de la loi n°2000-321 du 12 avril 2000 », *AJDA*, 2000, p. 471.
[418] Dir. 2003/98/CE du 17 nov. 2003 concernant la réutilisation des informations du secteur public : *JOUE* L 345/90 du 31 déc. 2003.
[419] Ord. 2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques : *JORF* n°131 du 7 juin 2005.
[420] LANNA, M., « Données publiques et protection des données personnelles : Le cadre européen », ENA, *RFAP*, n°167, 2018/3, pp. 501 à 511.
[421] Règl. n°2016/679 du 27 avr. 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données et abrogeant la directive 95/46/CE : *JOUE* L 119/1 du 4 mai 2016.
[422] CLUZEL-METAYER L., « L'ouverture des données publiques », *op. cit.*, pp. 7 à 23.
[423] LANNA, M., « Données publiques et protection des données personnelles : Le cadre européen », *op. cit.*

L'étude de la mise en œuvre de la protection des données personnelles dans la politique d'ouverture des données publiques suppose d'envisager, au préalable, la notion de données personnelles. Elles sont définies comme « *toute information se rapportant à une personne physique identifiée ou identifiable* »[424]. Cette identification peut être directe ou indirecte[425]. Concernant la mise en œuvre de la protection des données personnelles, si auparavant le responsable de traitement devait déposer une déclaration préalable des modalités de mise en œuvre du règlement, il doit, depuis l'adoption du RGPD, directement se conformer aux règles de protection et ce, tout au long du traitement[426]. Aussi, le droit de la protection des données personnelles est « *désormais construit sur une évolution logique de responsabilisation des opérateurs* »[427]. Les autorités publiques doivent donc désigner un délégué à la protection des données[428] chargé de veiller au contrôle de l'application du règlement (*Accountability*). De plus, l'article 25 exige « *l'intégration de mesures techniques protectrices des données personnelles en amont du traitement* »[429]. En effet, « *les bases de données créées par l'Administration devraient dès leur origine garantir le respect de la vie privée, ce que l'on désigne parfois par l'expression anglaise de privacy by design* »[430]. À savoir, il peut s'agir de la pseudonymisation ou de l'anonymisation des données. Les données anonymisées n'auront ainsi plus vocation à être protégées par le règlement. Mais, l'article 25 prévoit également l'adoption « *par défaut des mesures permettant de réduire l'usage des données au strict nécessaire eu égard à la finalité du traitement, ce qui est nommé privacy by default* »[431].

125- **Exceptions à l'interdiction de communication.** Il existe trois exceptions à l'interdiction de communication à des tiers : l'intéressé consent expressément à la diffusion de ses données ; il existe une obligation légale de publication ; les documents entrent dans une catégorie de documents pouvant être rendue publique sans anonymisation[432].

---

[424] RGPD, art. 4.
[425] Voir *infra*, n°689 et s.
[426] LANNA, M., *op. cit*.
[427] CLUZEL METAYER, L. et DEBAETS E., « Le droit de la protection des données personnelles, la loi du 20 juin 2018 », *RFDA*, 2018.
[428] RGPD, art. 37-1e, a.
[429] LANNA, M., *op. cit.*
[430] GORCE G. et 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 (2013-2014), 16 avr. 2014.
[431] CLUZEL-METAYER, L. et DEBAETS, E., « Le droit de la protection des données personnelles, la loi du 20 juin 2018 », *op. cit.*
[432] CRPA, art. D. 312-1-3.

B. L'obstacle à la diffusion des données publiques

126- La présence de données relevant de la sphère privée dans les bases de données de l'Administration interdit leur diffusion (**1**). Aussi, afin de protéger les données privées, la jurisprudence a posé des conditions d'accès (**2**).

1. L'interdiction de diffusion

127- En principe, la politique d'ouverture des données publiques exclut toute diffusion aux tiers des données relevant de la sphère privée[433]. Cependant, s'il y a un traitement préalable rendant impossible l'identification des personnes concernées alors elles peuvent être diffusées[434]. Mais cette condition semble difficile à mettre en œuvre du fait du risque de réidentification. En effet, les procédés visant à empêcher la réidentification ne semblent pas infaillibles[435]. La CNIL suggère d'indexer les documents n'ayant pas fait l'objet d'anonymisation préalable afin de faciliter le travail de recherche des internautes dans les bases de données, mais souhaite rendre impossible l'indexation des données identifiantes sur des moteurs de recherches externes[436].

L'objectif est donc de trouver un équilibre entre la transparence de la vie publique et la protection de la vie privée. C'est la tendance des réformes législatives, de la doctrine, de la CADA et de la jurisprudence administrative. Néanmoins, à l'heure du développement des technologies de l'information et des activités économiques des personnes publiques, la privatisation des données et leur ouverture à la concurrence « *tend à prédominer […] la préoccupation de protéger davantage la confidentialité de certaines informations, qu'il s'agisse de secrets privés ou de secrets administratifs* »[437]. Or cela peut paraître paradoxale[438] puisque la législation tend vers plus de transparence par l'ouverture de l'accès aux documents administratifs[439] et par la libre réutilisation des informations publiques[440]. Par exemple, dans

---

[433] CRPA, art. L. 311-6 : « *Ne sont communicables qu'à l'intéressé les documents administratifs : 1° Dont la communication porterait atteinte à la protection de la vie privée…* » ; CRPA, art. L. 312-1-1.
[434] CRPA, art. L. 312-1-2.
[435] CLUZEL-METAYER, L., « Les limites de l'*Open Data* », *AJDA*, 2016, n°102 à 107.
[436] CNIL, délib. n°2018-101, 15 mars 2018.
[437] DELAUNAY B., « Nouvelles limitations à l'accès aux documents administratifs », *AJDA*, 2013.
[438] *Ibid.*
[439] Loi n°78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés : *JORF* du 7 janv. 1978.
[440] Ord. n°2005-650 du 6 juin 2005 relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques : *JORF* n°131 du 7 juin 2005.

l'arrêt *Commune de Sète*[441], le Conseil d'État a admis l'ouverture de documents administratifs contenant des informations de nature privée à condition, toutefois, que les mentions nominatives soient occultées.

2. Les conditions d'accès limitées

128- La jurisprudence du Conseil d'État pose les conditions pour l'accès aux documents administratifs contenant des informations dont la diffusion pourrait porter atteinte à la vie privée. D'abord, il faut rechercher un lien suffisamment direct entre les missions de service public et les documents litigieux. Ensuite, il faut rechercher si leur communication peut porter atteinte au secret, notamment au secret commercial et industriel d'un organisme privé chargé d'une mission de service public. C'est ce qui a été retenu dans l'affaire *La Poste c/M. Bigi*[442]. Une solution similaire a été adoptée pour un établissement public industriel et commercial (EPIC)[443]. De plus, cette interdiction de diffusion d'informations protégées concerne tout autant celles concernant les personnes physiques que les personnes morales[444]. En témoigne la décision *ministre du travail, de l'emploi et de la santé c/cabinet de La Taille*[445] dans laquelle les documents litigieux étaient selon le Conseil « *de nature à révéler des orientations, notamment syndicales, susceptibles de méconnaître la protection de la vie privée que l'article 6 de la loi du 17 juillet 1978 garantit à toute personne, tant physique que morale, ou de divulguer des choix révélateurs des actions et des projets d'entreprises de nature à porter atteinte au secret en matière commerciale et industrielle protégé par les mêmes dispositions* ».

Ainsi, les données personnelles ou celles portant atteinte à la vie privée dans les bases de données agricoles publiques doivent faire l'objet d'une occultation avant toute publication.

129- **Conclusion de la section.** Les données publiques doivent être obligatoirement communiquées et diffusées par les administrations, pour qui il s'agit d'une véritable mission, une fois seulement qu'elles ont fait l'objet d'un traitement. La tendance est aujourd'hui à la création

---

[441] CE, 10e et 9e ch. réunies, 10 mars 2010, *Commune de Sète*, n°303814 ; Rec. 70 ; note PELLISSIER G., *JCP A.* 2010 n°16 p. 23 ; note MELLERAY F., *AJDA.* 2010, n°5 p. 25 ; GLASER E., *RLCT.* 2010 n°58 p. 18 ; obs. DUBREIL *JCP A.* 2010. 221.

[442] CE, 17 avril 2013, *La Poste c/ M. Bigi*, n°342372, t. pp. 601-602 ; comm. KOUBI G., *JCP A.* 2013 n°28 p. 25 ; note DELAUNAY B., *AJDA.* 2013 n°33 p. 1920, t. pp. 601 à 602.

[443] CE, 10ème et 9ème ch. réunies, 21 avr. 2017, *Régie autonome des transports parisiens*, n°395952 ; *Rec.* ; concl. CREPEY E., *AJDA* 2017. 1206 ; comm. VIROT-LANDAIS A., *JCP A.* 2017 n°27 p. 15 ; note CHIFFLOT N., *Procédures* 2017 n°10 p. 27.

[444] CE, 10ème et 9ème ch. Réunies, 17 avr. 2013, *Ministre du travail, de l'emploi et de la santé c/ Cabinet de la Taille*, req. n°344924 ; *Rec.* ; comm. DELAUNAY B., *AJDA.* 2013 n°33 p. 1920.

[445] CE, 10ème et 9èmé ch. réunies, 17 avr. 2013, n°344924, préc.

d'un véritable État-plateforme. Aussi, leur intégration dans une base de données ne constitue plus une limite à cette obligation. C'est pourquoi les personnes agissant dans le cadre d'une mission de service public qui constituent des bases de données contenant des données agricoles publiques ne peuvent plus revendiquer un droit de propriété sur ces bases. Nous assistons donc au recul de la réservation des bases de données face à celui de l'ouverture des données publiques. De même, avant toute diffusion l'Administration et les chercheurs sont tenus d'assurer le respect de la vie privée et de la réglementation sur les données à caractère personnel en faisant disparaître toute information susceptible d'identifier une personne physique ou une personne morale.

130- **Conclusion du chapitre.** Les données agricoles publiques sont, aujourd'hui, rendues largement accessibles grâce à la politique d'ouverture des données publiques. Les obligations nées de ce régime à la charge des administrations, mais aussi, dans une autre mesure, des chercheurs, réduisent les possibilités de réservation de certaines données. Dans l'objectif d'une ouverture généralisée des données agricoles publiques, les initiatives des acteurs du secteur agricole telles que la création de la plateforme API-AGRO doivent tendre vers une accessibilité accrue des données en faveur de la création d'un État-plateforme. Mais cette ouverture généralisée reste néanmoins limitée aux données publiques qui ne correspondent, en définitive, qu'à une infime part des données produites et collectées dans le secteur agricole.

Chapitre 2. L'accessibilité des données agricoles privées

131- Dans le secteur agricole, de nombreuses entreprises gravitent autour de l'exploitation des données issues des exploitations. En effet, ces entreprises se positionnent sur le marché des données agricoles afin de proposer des services et des outils toujours plus innovants et sophistiqués aux agriculteurs. À cette fin, de très nombreuses données sont collectées et produites sur les exploitations pouvant porter sur la qualité des sols, la quantité et la qualité du lait produit, l'utilisation des produits phytosanitaires, au moyen d'objets connectés, c'est-à-dire des machines-outils, des satellites ou bien encore, des drones. Or, celui qui détient les données en détermine bien souvent les conditions d'accès et d'usage, contrairement aux données collectées ou produites au cours d'une mission de service public qui doivent être librement accessibles. Par conséquent, il se peut que parfois l'utilisateur de l'objet connecté n'ait pas accès aux données produites par son utilisation. Les questions autour de l'accès concernent également les tiers. En effet, les consommateurs, le public en général ou encore les concurrents peuvent vouloir, à certaines conditions, accéder aux données que ce soit pour des raisons d'intérêt général ou pour parvenir à un équilibre sur le marché. Également, afin de favoriser l'innovation et la recherche, les données doivent être accessibles techniquement et juridiquement[446]. Ainsi, après avoir circonscrit l'objet soumis au droit d'accès à travers les données faisant l'objet d'une réservation privative (**Section 1**), il conviendra d'envisager la mise en œuvre de leur accès (**Section 2**).

Section 1. L'objet du droit d'accès : les données faisant l'objet d'une réservation privative

132- En premier lieu, il convient de qualifier les données agricoles privées (**§1**). En second lieu, il faudra envisager leur hétérogénéité (**§2**).

§1. *La qualification des données agricoles privées*

133- La qualification des données agricoles privées suppose de les définir (**I**) et d'en étudier la provenance (**II**).

[446] ROBIN, A., *Droit des données de la recherche, Science ouverte, innovation, données publiques*, Larcier, 2022, n°129, p. 107.

I. La définition des données agricoles privées

134- Il est remarquable de noter que la notion de données s'arrête à celle de données publiques. Ainsi, les données qui font l'objet d'une réservation privative ne sont pas définies (**A**), il faut donc expliciter le concept même de données privées (**B**).

A. L'absence de définition des données privées

135- À la lecture des réglementations applicables aux données, ainsi que de la jurisprudence et de la doctrine, il faut faire le constat qu'aucune définition n'a été proposée pour les données faisant l'objet d'une réservation privative. Seule la notion de données publiques a fait l'objet d'une définition. En effet, les données publiques devaient être définies afin d'identifier spécifiquement les données sur lesquelles s'applique le régime de l'ouverture des données. *A contrario*, les données faisant l'objet d'une réservation privative répondent à plusieurs régimes selon leur contenu, leur objet, leur intérêt, etc. Il serait alors trop restrictif de donner une définition précise pour une catégorie si étendue recouvrant une très grande diversité de données. Aucun amalgame ne doit en outre être fait entre données privatives et données à caractère personnel[447] qui recouvrent deux réalités bien différentes. L'une concerne les données produites et collectées par les personnes privées dans le cadre de leurs activités et qui font l'objet d'une réservation privative, l'autre s'applique aux données qui identifient ou rendent identifiables une personne privée. Par conséquent, si la notion de données privées n'a pas véritablement de réalité juridique, elle a néanmoins le mérite de la simplification afin de les distinguer des données publiques.

B. Le concept de données privées

136- Dès lors que les données ne sont pas soumises à la politique d'ouverture des données publiques, elles peuvent faire l'objet d'une réservation que ce soit par le droit de la propriété intellectuelle[448] ou par la mise en œuvre de mesures techniques et/ou juridiques de protection. L'objectif d'une telle réservation est ainsi d'en limiter l'accès[449]. Par conséquent, les personnes

[447] Sur la notion de données à caractère personnel, voir *infra*, n°684 et s.
[448] Voir *infra*, n°218 et s.
[449] ROBIN, A., *Droit des données de la recherche, op. cit.*, n°130, p. 108.

qui détiennent les données adoptent des comportements réservataires et déterminent les conditions d'accès et d'usage. C'est le cas notamment des données industrielles collectées et produites au moyen d'outils sur les exploitations agricoles détenues en grande majorité par les entreprises qui ont créé la machine et le logiciel lié.

II. La provenance des données agricoles privées

137- Les données agricoles privées proviennent des entreprises de l'agriculture numérique (**A**) généralement produites ou collectées dans le cadre d'un contrat de prestation de services ou d'un contrat de vente (**B**).

A. La collecte et la production des données par les sociétés de l'agriculture numérique

138- Toute personne morale ou physique est susceptible de produire ou de collecter des données agricoles. De nombreuses sociétés se sont spécialisées dans le secteur de l'agriculture numérique afin d'apporter des solutions numériques et techniques aux agriculteurs. Au vu de l'immense écosystème que représente ce secteur, il serait vain de tenter d'être exhaustif. Il est possible toutefois de fournir quelques exemples. Plusieurs corps de métiers se sont développés autour de l'agriculture numérique, ainsi pour les principaux intéressant directement le traitement des données agricoles, il faut évoquer les éditeurs de logiciels et les fournisseurs de matériels.

En ce qui concerne les éditeurs de logiciels, certains comme Isagri proposent des solutions logicielles et matérielles à l'usage des agriculteurs et des viticulteurs[450]. Au moyen de ces outils, les céréaliers, les éleveurs ou encore les viticulteurs peuvent visualiser les zones à traiter, la fertilité des animaux, les risques sanitaires, les traitements réalisés, le traçage des différentes étapes du vin, etc. Ces logiciels permettent également aux exploitants agricoles de rester dans le cadre des obligations réglementaires et administratives. Afin d'améliorer les services qu'Isagri propose, la société doit pouvoir récupérer les données techniques de l'utilisation du service par l'agriculteur. De même, les données collectées *via* les outils doivent pouvoir être partagées dans les applications collaboratives au profit de la collectivité. En outre,

[450] Logiciel de gestion, logiciel technique, logiciel collaboratif pour la compatibilité, mais aussi des solutions informatiques comme des stations météo et des ordinateurs.

la société propose de traiter des données telles que des images satellitaires afin de fournir des cartes satellites pour les besoins des cultures dans le but d'obtenir des informations parcellaires. Ces logiciels de gestion technico-économique permettent donc de visualiser et de faciliter l'activité sur l'exploitation agricole. Ils nécessitent une certaine accessibilité des données afin, d'une part, de permettre aux entreprises d'améliorer leurs services, d'autre part, d'ouvrir certaines données à la communauté dans le cadre d'applications collaboratives (partage de données avec le comptable de l'agriculteur par exemple).

D'autres entreprises proposent des outils d'aide à décision. La société SMAG, par exemple, propose des logiciels et des applications pour l'optimisation et la valorisation des pratiques agricoles. Ces solutions permettent d'enregistrer, de structurer et de partager des données hétérogènes de l'exploitation entre les différentes solutions que propose SMAG au moyen d'une API. Également, la société ITK fournit des analyses afin de mesurer et d'améliorer la rentabilité, la performance de la production et de la chaîne logistique aux producteurs agricoles et à leurs conseillers. Tant SMAG qu'ITK sont des fournisseurs de services qui interviennent directement dans l'analyse des données afin d'offrir de l'aide à la décision aux agriculteurs en apportant leur expertise. Leurs analyses permettent d'optimiser l'itinéraire cultural, de prédire les risques de maladie, d'optimiser les traitements phytosanitaires, de piloter l'irrigation ou encore d'anticiper le risque de gel. À cette fin, des données brutes sont collectées *via* des outils d'imagerie et des capteurs puis sont transformées au moyen d'algorithmes qui peuvent faire l'objet d'une protection ou d'une réservation[451]. Ainsi, afin de fournir de l'aide à la décision, les analyses issues de ce travail sont restituées aux agriculteurs sous la forme de tableaux de bord, de graphiques ou encore de cartes. Ces créations se trouvent protégées par le droit d'auteur, dès lors qu'elles présentent un caractère original.

Certaines entreprises sont, enfin, spécialisées dans la fourniture de matériel. C'est le cas notamment de la société Weenat qui fournit du matériel de collecte de données à l'usage des agriculteurs. Les capteurs ainsi disposés sur les exploitations permettent de collecter des données. Aussi, la société Weenat propose des applications liées à ces capteurs afin de fournir ici encore de l'aide à la décision concernant l'irrigation, la protection des cultures, le suivi de la météo, l'anticipation et le suivi du gel, etc. La société Sencrop propose également des stations météos connectées et des capteurs associés *via* une application météo collaborative afin d'anticiper les aléas climatiques, la gestion des maladies et des ravageurs, le pilotage de l'irrigation au moyen d'outil d'aide à la décision, de bilans, etc. Farmstar est une solution

[451] Voir *infra*, n°303 et s.

agronomique qui permet de gérer l'azote sur les exploitations en continu au moyen des satellites. Wiuz est une plateforme ouverte qui permet d'interconnecter les outils internes et externes afin de fluidifier les données et faciliter l'accès à ces données, aux techniciens, aux conseillers, aux agriculteurs, à leurs prestataires, etc. Ekylibre propose un logiciel de gestion global de l'exploitation qui permet d'interconnecter tous les outils dont l'agriculteur dispose *via* des solutions *Open source*.

Ainsi, toutes ces entreprises collectent et produisent des données agricoles qui ont généralement vocation à rester privées dans le cadre de leur relation avec les agriculteurs, à moins qu'elles soient diffusées sur des plateformes collaboratives. Aussi, les agriculteurs produisent eux-mêmes des données lors de leurs activités agricoles au moyen du matériel qu'ils utilisent sur leurs exploitations.

B. L'origine des données agricoles privées

139- Comme il vient d'être vu, si les données agricoles sont produites ou collectées au moyen d'outils de collecte, comme des capteurs ou des satellites, elles peuvent également être saisies directement par l'agriculteur dans les logiciels de gestion de son exploitation. Par conséquent, l'agriculteur est considéré comme le générateur des données. En effet, c'est par son activité et par son utilisation des produits et services à sa disposition que les données sont générées. En outre, les données naissent au cours d'une relation contractuelle de prestation de services ou après la vente d'un objet connecté associé à un abonnement. Ces données sont donc produites ou collectées par l'entreprise de l'agriculture numérique afin de créer des outils d'aide à la décision, de nouveaux objets connectés, pour améliorer les machines agricoles, etc. Dans un tel cas, l'entreprise détient les données qu'il collecte dans le cadre de son activité de prestation de services, elle dispose alors des moyens de les réserver *via* le secret en les rendant confidentielles, ou par le droit de propriété intellectuelle en les intégrant dans des bases de données. Ici déjà se révèle toute l'ambigüité de telles relations puisqu'il s'agit de savoir qui du générateur des données ou de leur détenteur dispose effectivement les droits sur ces données et dans quelles mesures.

§2. *L'hétérogénéité des données agricoles privées*

140- Sur l'échelle de l'accès, les données faisant l'objet d'une réservation privative, collectées dans le cadre d'une relation contractuelle, par exemple entre l'agriculteur et son prestataire de services, se trouvent tout en bas. En principe, ces données ne sont accessibles que par les parties au contrat. Elles sont collectées par les objets connectés sur les exploitations (semoir, capteurs, robot de traite, etc.) ou reportées directement par l'agriculteur dans son logiciel de gestion. L'agriculture est alors l'utilisateur des produits et services liés qui génèrent des données agricoles. Ces données peuvent avoir pour objet la quantité de produits utilisés, la température, l'humidité du sol, le rayonnement solaire, etc. Une fois qu'elles sont collectées, les entreprises prestataires de services vont traiter ces données et les stocker dans des bases de données. En tant que détenteurs des données collectées, les entreprises du secteur agricole seront alors dans la capacité de réserver l'accès à ces données[452].

D'autres données se situent *a contrario* à l'autre extrémité de l'échelle de l'accès et doivent être ouvertes. C'est le cas notamment de celles dont l'intérêt dépasse les seules parties au contrat. C'est pourquoi plusieurs catégories de données ont été créées par le législateur afin de les rendre accessibles selon leur intérêt. Il faut relever d'abord, les données d'intérêt général (**I**), puis les futures catégories de données privées ouvertes (**II**).

I. Les données d'intérêt général

141- Afin d'étudier la catégorie de données d'intérêt général, il faudra constater, tout d'abord, l'absence de définition des données d'intérêt général (**A**), pour ensuite envisager l'étendue de la catégorie (**B**).

A. L'absence de définition des données d'intérêt général

142- **Tentatives de définition.** La notion d'intérêt général est difficile à définir. Depuis plusieurs décennies, cette notion est très commentée et débattue. Pour la doctrine, c'est une « *notion fuyante, insaisissable, floue, qui ne se laisse pas enfermer dans les classifications normatives traditionnelles* »[453]. Cela vient du fait notamment que « *selon les temps, les lieux et les opinions,*

[452] *Ibid.*
[453] MERLAND, G., « L'intérêt général dans la jurisprudence du Conseil constitutionnel », *LGDJ*, 2004, p. 2.

elle reçoit des contenus forts variables »[454]. Pourtant, elle est au cœur même de l'action publique[455]. D'ailleurs, elle est mainte fois citée dans la jurisprudence du Conseil d'État et du Conseil constitutionnel. En 1999, le Conseil d'État définissait la notion d'intérêt général comme « *centrale de la pensée politique du système juridique français* » tout en affirmant que c'est à « *la loi, expression de la volonté générale, de définir l'intérêt général, au nom duquel les services de l'État, sous le contrôle du juge, édictent les normes réglementaires, prennent les décisions individuelles et gèrent les services publics* »[456]. De même, l'intérêt général est « *le dépassement des intérêts particuliers [qui] est, d'abord, dans cette perspective, l'expression de la volonté générale, ce qui confère à l'État la mission de poursuivre des fins qui s'imposent à l'ensemble des individus, par-delà leurs intérêts particuliers* »[457]. Cette définition est néanmoins contestée par certains auteurs[458].

143- **Instrument de contrôle de constitutionnalité.** Dans le contentieux constitutionnel français, il est très souvent fait référence à l'intérêt général depuis une décision du 12 juillet 1979[459]. Cette notion a offert au juge constitutionnel « *un précieux instrument du contrôle de la loi* »[460]. Elle est la « *condition de constitutionnalité destinée à autoriser les restrictions législatives à un certain nombre de droits et de libertés* »[461]. À cette fin, le législateur doit formuler les objectifs poursuivis par la loi qui sera, par conséquent, d'intérêt général.

144- **Définition inexistante.** Le constat est qu'il n'existe pas, pour l'heure, de consensus sur la définition de l'intérêt général. Il est, néanmoins, généralement admis qu'il reflète « *l'ordre public, l'intérêt du peuple ou bien la priorité des décisions administratives sur les intérêts privés, sectoriels, les droits individuels et les contrats entre particuliers* »[462]. Mais le législateur n'a pas formulé de définition à ce jour. Il en va de même dans la loi pour une République Numérique de 2016 qui a intégré la notion d'intérêt général pour des données issues d'une

---

[454] VEDEL, G., préf. RANGEON, F., *L'idéologie de l'intérêt général*, Economica, 1986 (dernière version 1999), p. 3.
[455] MAZEAUD, P., « Qui se soucie de l'intérêt général ? », *Comm. à l'Académie des sciences morales et politiques*, Canal académie audio, 7 févr. 2011.
[456] CE, *Réflexions sur l'intérêt général*, Rapport public 1999, EDCE n°50, La Documentation française, 30 nov. 1998.
[457] *Ibid.*
[458] FOUCART T., « La définition contestable de l'intérêt général par le Conseil d'État », art. Iref-Europe, Contrepoints, [en ligne], consulté le 10 oct. 2018, https://www.contrepoints.org/2018/10/10/327228-la-definition-contestable-de-linteret-general-par-le-conseil-detat.
[459] Cons. const., 12 juill. 1979, n°79-107 DC, *Ponts à péage*: Rec. p. 31 ; RJC, I, 73 ; FAVOREU, L., *Rec. de jur. constit*., 1959-1993, p. 73 ; *RDP*, 1979, 1691.
[460] MERLAND, G., « L'intérêt général dans la jurisprudence du Conseil constitutionnel », *op. cit*., p. 2.
[461] *Ibid.*
[462] CRETOIS, P. et ROZA S., « De l'intérêt général : introduction », Astérion [en ligne], 17/2017, mis en ligne le 20 novembre 2017, consulté le 27 février 2020. URL : http://journals.openedition.org/asterion/2996.

concession de service public[463] ou dans le cadre de mission de service public et commercial[464], sans qu'aucune définition n'en soit donnée.

B. L'étendue de la catégorie des données d'intérêt général

145- La loi retient pour l'heure, comme entrant dans la catégorie des données d'intérêt général, celles produites dans le cadre de concession ou dans le cadre de mission de service public et commercial. Mais le législateur n'a pas développé de régime entourant largement toutes les données qui intéresseraient l'intérêt général en dehors des simples concessions et mission de service public et commercial. Or, « *en raison de leur intérêt pour améliorer les politiques publiques* »[465], ces données ne peuvent plus être couvertes par le secret et devraient faire l'objet d'une large ouverture.

II. La création de nouvelles catégories de données par le législateur européen

Le législateur européen a prévu plusieurs situations dans lesquelles les données devront être accessibles. Il a déjà acté la mise à disposition des données de forte valeur (**A**) et envisage celle des données devant être ouvertes en raison d'un besoin exceptionnel (**B**).

A. La future catégorie des données de forte valeur

146- Le législateur européen semble avoir abandonné les notions d'intérêt général et de commun au profit des ensembles de données de forte valeur dans la directive 2019/1024 du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public[466]. Pour analyser cette nouvelle catégorie de données, il convient, tout d'abord, d'en envisager la définition (**1**) pour, ensuite, analyser ses conditions d'ouverture (**2**).

[463]Art. 17 de la LRN a modifié ord. n°2016-65 du 29 janv. 2016 relative aux contrats de concession : *JORF* n°0025 du 30 janv. 2016.
[464]Art. 18 a modifié l'article 10 de la loi n°2000-321 du 12 avr. 2000 relative aux droits des citoyens dans leurs relations avec les administrations : *JORF* n°0088 du 13 avr. 2000.
[465]https://www.vie-publique.fr/eclairage/20301-loi-republique-numerique-7-octobre-2016-loi-lemaire-quels-changements
[466] *JOUE* L 172/56 du 26 juin 2019.

1. La définition des ensembles de données de forte valeur

147.- L'article 2 de la directive 2019/1024 définit les « ensembles de données de forte valeur » comme « « *des documents dont la réutilisation est associée à d'importantes retombées positives au niveau de la société, de l'environnement et de l'économie, en particulier parce qu'ils se prêtent à la création de services possédant une valeur ajoutée, d'applications et de nouveaux emplois décents et de grande qualité, ainsi qu'en raison du nombre de bénéficiaires potentiels des services et applications à valeur ajoutée fondés sur ces ensembles de données* ».

Ces données ont selon le législateur un intérêt supérieur à celui de leur détenteur en raison « *des avantages socioéconomiques d'une valeur particulièrement élevée pour l'économie et la société* »[467] qu'elles représentent. Et voilà pourquoi elles doivent être mises à disposition et réutilisables.

2. Les conditions d'ouverture des ensembles de données à forte valeur

148.- L'article 14 de la directive expose les conditions de mise à disposition des ensembles de données à forte valeur. Elles doivent être mises à disposition gratuitement, de sorte qu'elles soient lisibles par machine en recourant à des API et sous la forme d'un téléchargement de masse le cas échéant. La Commission européenne a pour mission d'identifier ces ensembles de données de forte valeur selon plusieurs éléments d'évaluation. En effet, ces ensembles sont évalués selon leur aptitude potentielle à "*a) générer des avantages socioéconomiques ou environnementaux importants et des services innovants ; b) bénéficier à un grand nombre d'utilisateurs, notamment des PME ; c) contribuer à générer des recettes ; et d) être associés à d'autres ensembles de données"*. Pour les identifier, la commission doit évaluer ces ensembles de données et opérer une analyse du coût-avantage de la mise à disposition de ces données afin qu'elle ne représente pas un coût trop important pour les organismes publics chargés de cette mise à disposition. La Commission a déterminé six premières catégories thématiques d'ensembles de données de forte valeur[468] : géospatiales, observation de la terre et environnement, météorologiques, statistiques, entreprises et propriété d'entreprises, mobilité.

---

[467] Dir. préc., cons. 66.

[468] *Ibid.* : « *Les ensembles de données et la tarification pour la réutilisation des documents, les catégories thématiques pourraient notamment couvrir les codes postaux, les cartes nationales et locales (catégorie "géospatiales"), la consommation d'énergie et les images satellitaires (catégorie "observation de la terre et environnement"), les données in situ provenant d'instruments et de prévisions météorologiques (catégorie "météorologiques"), les indicateurs démographiques et économiques (catégorie "statistiques"), les registres du commerce et les identifiants d'enregistrement (catégorie "entreprises et propriété d'entreprises"), ainsi que la signalisation routière et les voies de navigation intérieures (catégorie "mobilité")* ».

Trois ensembles de données de forte valeur font exception, il s'agit de ceux détenus par des entreprises publiques lorsque leur mise à disposition entraînerait une distorsion de concurrence sur les marchés pertinents, ainsi que les ensembles de données détenus par les bibliothèques. Enfin, les ensembles de données de forte valeur seront exemptés de l'obligation de mise à disposition pendant une période n'excédant pas deux ans, lorsque leur mise à disposition par les organismes publics aurait de trop lourdes conséquences sur leur budget. Une fois la mise à disposition assurée par ces organismes, la directive prévoit la gratuité de la réutilisation de ces données par les utilisateurs[469].

La transposition de la directive qui date de 2019[470] n'ayant pas encore eu lieu, elle n'est pas pour l'heure applicable. Néanmoins, il semble que son applicabilité soit limitée dans le secteur agricole hormis les données portant sur l'observation de la terre et l'environnement qui concernent par exemple les images satellitaires. Mais une grande partie de ces images est déjà mise à disposition, notamment, dans le projet Equipex-Geosud localisé à la maison de la télédétection à Montpellier, porté par un consortium composé notamment de INRAE, AgroParisTech, CIRAD, IGN, CEREMA et IRD, dont l'objectif était jusqu'en 2020 de développer une infrastructure nationale de données et de services autour de l'imagerie spatiale au service de la communauté scientifique, de l'action publique et de l'innovation. Il produit des images satellitaires à très haute résolution spatiale actualisée du territoire national et compte jusqu'à 1200 comptes utilisateurs.

En conséquence, cette nouvelle catégorie créée par le législateur n'aura pas de réel impact sur le secteur agricole.

B. La proposition de mise à disposition des données privées en raison d'un besoin exceptionnel

149. Comme il l'a été vu plus haut, la proposition de Règlement sur les données du 23 février 2022[471] prévoit la création d'une obligation de mise à disposition de certaines données[472]. Cette mise à disposition devra être conditionnée par l'existence d'un besoin exceptionnel déterminé par le Règlement, à la demande d'un organisme du secteur public ou d'une institution, d'un organe

[469] *Ibid.*, art. 6.
[470] Voir *infra*, n°415.
[471] Proposition règl. du 23 févr. 2022 fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (Règl. sur les données), COM (2022) 68 final.
[472] Voir *supra*, n°84 et s.

ou d'un organisme de l'Union. Néanmoins, cette obligation ne s'applique pas aux petites et moyennes entreprises, ainsi, elle ne devrait pas inquiéter les exploitants agricoles français.

150- **Conclusion de la section.** La grande majorité des données collectées dans le secteur agricole l'est au cours d'activités de prestation de services réalisées par les entreprises de l'agriculture numérique auprès des exploitants agricoles. Ces données sont donc soumises à la liberté contractuelle. Au vu de la très grande hétérogénéité de la catégorie des données privées, il serait vain de tenter d'en donner une définition en une seule acception. Pourtant, afin d'organiser l'accès à certaines données, encore faut-il pouvoir en délimiter les contours, ce qui implique de les définir. Pour l'heure cependant l'organisation de l'accessibilité des données privées reste marginale. L'accessibilité des données privées est, en effet, limitée à des situations exceptionnelles dans le cadre de concession ou pour la réalisation de mission de service public et commercial. Le législateur européen a prévu néanmoins de rendre accessibles les données qui représentent une forte valeur économique. Il prévoit également de permettre l'accessibilité à certaines données pour un besoin exceptionnel. Les limites de ces obligations excluent généralement les agriculteurs et la plupart des acteurs du secteur agricole.

Section 2. La mise en œuvre de l'ouverture de l'accès aux données agricoles privées

151- L'accès aux données agricoles privées n'est pas la règle. Pourtant, il arrive que la question de l'accès à certaines de ces données se pose en raison soit de leur objet (**§1**), soit de leur intérêt concurrentiel (**§2**).

§1. *La reconnaissance de l'accès aux données privées selon leur objet*

152- Certaines données faisant l'objet d'une réservation privative peuvent contenir des informations d'intérêt général ou d'intérêt commun. Par conséquent, la question se pose de savoir si l'ouverture de l'accès aux données agricoles d'intérêt général doit être organisée par la loi. Mais aussi, les multiples possibilités de réservation des données privées engendrent parfois des difficultés pour les agriculteurs à qui l'accès aux données de leur exploitation n'est pas garanti. De ce fait, une seconde question se pose qui est de savoir s'il faut désormais reconnaître un droit d'accès de principe en faveur de l'exploitant agricole sur les données de son exploitation à l'image de ce qui existe pour les données personnelles.

Dans un premier temps, il convient d'envisager la consécration de l'accès aux données d'intérêt général (**I**). Dans un second temps, il sera nécessaire de s'intéresser à la reconnaissance du droit d'accès de principe aux données privées pour le générateur des données (**II**).

I. L'accès aux données d'intérêt général : une future consécration légale ?

153- Aujourd'hui, la question se pose de savoir si le législateur doit reconnaître l'ouverture de l'accès aux données privées d'intérêt général (**A**). Afin d'illustrer l'intérêt de l'ouverture de ces données, l'exemple le plus significatif dans le secteur agricole est assurément celui des données phytosanitaires (**B**).

A. La création d'un régime d'ouverture des données privées d'intérêt général

154- Plusieurs propositions d'ouverture de données considérées comme d'intérêt général ont été faites au cours des dernières années sans qu'aucune aboutisse jusqu'alors (**1**), pourtant la création d'un régime d'ouverture des données d'intérêt général semble, aujourd'hui, particulièrement opportune (**2**).

1. Les tentatives échouées de création d'un régime d'ouverture des données d'intérêt général

155- **L'extension de la catégorie des données d'intérêt général.** Certains auteurs s'interrogent sur l'opportunité de l'élargissement de la notion de données d'intérêt général en ouvrant des données de nature privée d'entreprises ne réalisant pas de mission de service public. L'objectif, ici, est de favoriser le partage de données qui auraient un intérêt général même si elles sont détenues par des entreprises privées sans concession publique. Cela permettrait d'endiguer la rétention d'information d'intérêt général opérée par les entreprises privées. Cependant, la détermination de ces données semble bien difficile à établir. La grande diversité des données empêche de les catégoriser et rend difficile la détermination des données d'intérêt général détenues par des entreprises privées.

156- **Injonction réglementaire de partage des données privées d'intérêt général.** Il existe, aujourd'hui, une véritable injonction au partage qui se traduit par de nombreuses initiatives avortées. Plusieurs rapports se sont prêtés à l'exercice d'imposer l'ouverture de données

d'intérêt général depuis 2015. Certains de ces rapports ont conclu à la difficulté de mise en œuvre d'un régime d'ouverture des données d'intérêt général, voire sur son impossibilité.

D'abord, le premier rapport, plutôt optimiste, avait été réalisé par M. F. Jutand sur les données de transport en mars 2015. Une définition était avancée pour les « *informations d'intérêt général* » comme « *toutes données (ou classe de données) des services de mobilité dont l'ouverture serait jugée opportune* »[473]. Ce rapport préconisait la création d'un nouveau statut pour les données d'intérêt général[474] et plus particulièrement pour les données ou classes de données très spécifiques : celles « *nécessaires à l'information du voyageur* »[475].

Trois mois plus tard, le gouvernement[476] mettait la création de la notion de données d'intérêt général dans les mesures du plan numérique en incluant les données des entreprises privées. Dans le même temps, le Conseil National du Numérique (CNNum) rendait, au contraire, un avis défavorable dans un rapport « *ambition numérique* »[477]. Il estimait « *qu'une nouvelle catégorie juridique dite de "données d'intérêt général"* » [478] ne devait pas être créée. Les raisons tenaient au fait que cette catégorie serait « *de portée trop large et floue et la qualification juridique des dites données trop complexes pour être mobilisable simplement* ». Il ajoute « *[qu'] elle risque par ailleurs de créer une insécurité juridique chez les acteurs privés fragilisant la construction de services et de modèles d'affaires intégrant la donnée* »[479]. Il encourage, néanmoins, l'ouverture des données « *au cas par cas* », « *en veillant au respect des droits fondamentaux et à l'équilibre des intérêts des partis prenantes* »[480].

Par la suite, le ministère de l'Économie et des Finances a commandé un rapport relatif aux données d'intérêt général à M. L. Cytermann publié en septembre 2015. Cette mission à spectre plus large avait une approche similaire au CNNum et précisait « *qu'un régime juridique unique des données d'intérêt général n'est ni souhaitable ni possible juridiquement, et qu'il convient de retenir une approche sectorielle dans la démarche d'ouverture de ces données* »[481].

---

[473] JUTAND F., *Ouverture des données de transport*, Rapport remis au secrétaire d'État chargé des transports, de la Mer de la Pêche, mars 2015, p. 72.
[474] *Ibid.*, pp. 75 à 76 : « *Le comité recommande d'examiner la possibilité de créer un statut "d'information d'intérêt général", qui permettrait d'élargir le périmètre des informations réutilisables au-delà de celles produites dans le cadre d'une mission de service public* ».
[475] *Ibid.*, p. 63.
[476] GOUVERNEMENT VALLS II, *Stratégie numérique du gouvernement*, publié du 26 Août 2014 au 11 Février 2016, Dossier de presse Gaité Lyrique du 18 juin 2015, p. 12.
[477] CNNum, *Ambition numérique, Pour une politique française et européenne de la transition numérique*, Rapport remis au premier ministre, juin 2015.
[478] *Ibid.*, p. 154.
[479] *Ibid.*
[480] *Ibid.*, p. 153.
[481] CYTERMANN L., Maître des requêtes au CE, *Rapport relatif aux données d'intérêt général*, Rapport d'étape CE / CGE / IGF, 2015, p. 3.

L'année suivante, la loi pour une république numérique du 7 octobre 2016[482] reprenait certaines des propositions de la mission consacrée aux données d'intérêt général menée par M. L. Cytermann et modifiait plusieurs textes de loi[483].

Enfin, le rapport Villani « *Donner un sens à l'intelligence artificielle : pour une stratégie nationale et européenne* », mission confiée par le ministre Édouard Philippe, porté par M. C. Villani et publié le 28 mars 2018, constate l'ouverture déjà réalisée de certaines données d'intérêt général tout en préconisant « *d'aller plus loin* » et de favoriser l'ouverture d'autres données d'intérêt général, l'objectif étant de favoriser « *le développement des usages de l'intelligence artificielle* »[484].

Il apparaît que la doctrine n'a pas trouvé d'accord sur la création d'un statut des données d'intérêt général d'origine privée. Pourtant, il semble qu'il y ait un véritable intérêt à l'ouverture de ces données.

2. L'opportunité de la création d'un régime d'ouverture des données d'intérêt général

157- **Principe de l'ouverture.** La création d'un régime d'ouverture des données privées d'intérêt général permettrait d'améliorer la confiance entre les acteurs du monde agricole. En effet, pour répondre au plus près des besoins du secteur, il faudrait établir au cas par cas les données devant bénéficier d'un tel statut. L'idée n'est plus de réfléchir en termes de détention des données par des personnes publiques ou privées, mais bien de changer de paradigme et de penser en termes d'opportunité d'ouverture de l'information portée par la donnée en fonction de son intérêt intrinsèque[485]. Par conséquent, les données d'intérêt général devraient être ouvertes à tous, par

---

[482] Loi n°2016-1321, 7 oct. 2016, pour une République Numérique (LRN), préc.

[483] Loi préc., art. 17 mod. art. 53-1 ord. n°2016-65, 29 jan. 2016, relative aux contrats de concession : ouverture des données et des bases de données collectées ou produites à l'occasion de l'exploitation du service public lors de la délégation d'un service public ; art. 18 mod. art. 10, loi n°2000-321, 12 avr. 2000 relative aux droits des citoyens dans leurs relations avec les administrations : données relatives aux subventions publiques au-delà d'un certain seuil ; art. 19 mod. art. 3 bis, loi n°57-711, 7 juill. 1951 relative à l'obligation, la coordination et le secret en matière de statistique : données transmises par les personnes morales lorsque ces informations sont recherchées pour les besoins d'enquêtes statistiques ; art. 20 et 21 mod. CJA, art. L. 110 et L. 111-13 : données de jurisprudence ; art. 22 mod. art. L. 119-1-1 du Code de la voirie routière et prévoit une base de données nationale des vitesses maximales autorisées sur le domaine public routier ; art. 23 ajoute art. L. 111-73-1 au code de l'énergie : données de consommation d'énergie ; art. 24 mod. art. L. 135 B du LPF : communication des informations sur les valeurs foncières déclarées à l'occasion des mutations.

[484] VILLANI C., *Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne,* Rapport AI for Humanity, Mission confiée, par le Premier Ministre Philippe E., Mission parlementaire du 8 sept. 2017 au 8 mars 2018, publié en mars 2018 : « *Les données d'intérêt général sont définies comme une "forme d'Open Data privé" ayant vocation à s'appliquer aux données qui revêtent une importance particulière pour le fonctionnement du marché ou des politiques d'intérêt général* », pp. 33 à 34.

[485] ROCHFELD, J., CORNU, M. et MARTIN, G., J., ss. dir., *L'échelle de communalité. Propositions de réforme pour intégrer les biens communs en droit,* Rapport final de recherche, avr. 2021, n°17 à 34, p. 350 : « *L'ouverture des*

exemple, « *en raison de leur intérêt pour améliorer les politiques publiques* »[486]. Certains auteurs proposent d'aller plus loin en reconnaissant une communalité de certaines catégories de données telles que les données environnementales[487]. C'est pourquoi il faudrait désormais réfléchir en termes de finalité[488], que ce soit dans un objectif de sécurité, de salubrité, de réalisation d'une mission de service public ou encore de santé publique. Cette ouverture au cas par cas irait dans une logique inverse de celle de la privatisation des données de santé ou des données personnelles dans un objectif de respect de la vie privée. Il pourrait en être ainsi des données contenant des informations relatives à la sécurité alimentaire.

158- **Ouverture des données agricoles d'intérêt général.** Le secteur agricole se prête parfaitement à l'établissement d'une catégorie de données d'intérêt général. En effet, de nombreuses données liées aux produits utilisés sur les plantations ou dans l'alimentation des animaux peuvent être considérées comme d'intérêt général puisqu'elles ont un impact direct sur la santé des consommateurs ou sur l'environnement. Également, certaines données permettent la réalisation de mission de service public, et à ce titre, doivent être accessibles. Il serait opportun qu'un comité réunissant les acteurs du secteur agricole établisse une liste de données qui devront être diffusées au moyen de plateformes prévues à cet effet. Toutefois, il faudra nécessairement préciser « *la notion de données d'intérêt général et le domaine des données concernée*s »[489]. Par exemple, les risques liés à l'alimentation pour la santé animale et humaine ne sont plus à démontrer après l'épisode de la crise de la vache folle ou encore celui de la grippe aviaire. Aussi, l'épidémiosurveillance apparaît comme absolument nécessaire afin d'éviter qu'apparaissent de nouvelles pandémies mondiales. C'est pourquoi les données sur la santé animale ont fait l'objet du Règlement n°2016/429 du 9 mars 2016 relatif aux maladies animales transmissibles[490] d'ordre épidémiologique concernant les dangers exposés à l'article L. 201-1 du Code rural. Ces données sont rendues accessibles grâce à l'obligation qui repose sur les propriétaires ou détenteurs d'animaux de tenir un registre d'élevage dans lequel ils doivent recenser les données sanitaires, zootechniques et médicales relatives aux animaux élevés.

---

données d'intérêt général se justifierait en considération, non [plus] de la nature publique de la personne qui les a produites ou qui les détient, mais de l'objet de ces informations et de l'importance que la collectivité leur reconnaît ».

[486] *Ibid.*

[487] *Ibid.*

[488] CNNum, *Synthèse de la consultation sur la régulation des contenus illicites,* États généraux des nouvelles régulations numériques, mai 2020, p. 301.

[489] *Ibid.*, p. 322.

[490] Règl. n°2016/429 du 9 mars 2016 relatif aux maladies animales transmissibles et modifiant et abrogeant certains actes dans le domaine de la santé animale (« législation sur la santé animale ») : *JOUE* L 84/1 du 31 mars 2016 ; Ord. n°2021-1317 du 20 oct. 2021 relatives aux mesures de surveillance, de prévention et de lutte contre les maladies animales transmissibles : *JORF* n°0246 du 21 oct. 2021.

Également, les vétérinaires doivent y mentionner leurs interventions sur les élevages[491]. Ces données ne sont accessibles qu'une fois que l'autorité administrative a collecté et traité les données et informations épidémiologiques concernant les dangers pour la santé humaine et animale cités à l'article L. 201-1 du Code rural[492]. À cette fin, les chambres d'agriculture ont notamment pour mission de collecter et de traiter les données relatives aux exploitations qui sont requises dans le cadre de la législation sur la santé animale[493]. Elles assurent, notamment, la collecte et le traitement de données relatives à l'identification et à la traçabilité des animaux. Ainsi, les données de santé animale font l'objet d'une intermédiation pour leur accessibilité. L'intérêt pour ces données est tel que l'Organisation internationale pour la santé animale (OIE) a créé un système mondial d'information zoosanitaire OIE-WAHIS qui doit devenir la plateforme de référence consacrée aux données sur les maladies animales et les capacités vétérinaires. Cette plateforme doit permettre un accès libre et gratuit à ces données pour les institutions, les partenaires commerciaux, les organisations internationales, les entreprises, les chercheurs, les universitaires, les journalistes, mais aussi les membres de la société civile[494].

B. L'exemple de l'ouverture des données phytosanitaires

159- Pour illustrer la nécessité de créer un régime d'ouverture des données d'intérêt général, les données phytosanitaires fournissent un bon exemple. En effet, la question de la mise à disposition des données produites par les agriculteurs se pose aujourd'hui pour les statisticiens, mais aussi pour les chercheurs et plus largement pour toutes les personnes qui souhaiteraient y accéder. Deux axes doivent être envisagés, le premier concerne la mise à disposition des données pour la réalisation d'une mission de service public (**1**). Le second est celui de l'ouverture des données phytosanitaires dans l'intérêt général (**2**).

[491] C. rur., art. L. 234-1.
[492] C. rur., art. L. 203-1.
[493] Règl. n°2016/429 du 9 mars 2016, préc.
[494] Communiqué de presse, OIE-WAHIS : une nouvelle ère pour les données de santé animale, 12 avr. 2021, https://www.woah.org/fr/oie-wahis-une-nouvelle-ere-pour-les-donnees-de-sante-animale/

1. La mise à disposition des données phytosanitaires pour la réalisation d'une mission de service public

160- **Notion.** Les données phytosanitaires sont celles qui communiquent des informations sur l'utilisation des pesticides[495]. Les pesticides sont les produits issus de synthèse chimique, de produits d'origine naturelle (extraits végétaux, animaux ou minéraux) et de micro-organismes (champignons, bactéries, virus et leurs extraits), d'herbicides, de fongicides, d'insecticides, d'acaricide, etc., ainsi que des stimulateurs de défenses des plantes et des médiateurs chimiques[496]. Pour pouvoir être commercialisés, ces produits doivent posséder une autorisation de mise à disposition sur le marché (AMM produit phytosanitaire), qui définit les conditions d'utilisation et les usages pour lesquels le produit est autorisé et chaque agriculteur doit posséder un certificat individuel phytosanitaire pour les utiliser.

161- **Contrôles et statistiques.** La mise sur le marché des produits phytosanitaires fait l'objet d'un contrôle par les États membres au titre de l'article 67 du Règlement n°1107/2009 concernant la mise sur le marché des produits phytopharmaceutiques du 21 octobre 2009[497], au moyen d'un rapport qu'ils doivent transmettre à la Communauté européenne dans les six mois. À cette fin, toutes les personnes qui mettent sur le marché les produits phytosanitaires ainsi que leurs utilisateurs doivent tenir des registres. C'est pourquoi les agriculteurs consignent dans ces registres le nom des produits utilisés, le moment de leur utilisation, la dose utilisée ainsi que la zone et la culture traitées. Ces informations sont communiquées sur demande à l'autorité compétente qui peut être une autorité de contrôle[498], en l'occurrence la Direction régionale de l'Alimentation, de l'Agriculture et de la Forêt (DRAAF)[499] en France est chargée de contrôler

---

[495] Dir. 2009/128/CE, art. 3, repris à l'article L. 253-1du Code rural : D'une part, les pesticides sont les produits pharmaceutiques au sens du règlement CE n°1107/2009, d'autre part, les produits biocides au sens du règlement (CE) 528/2012. Les produits pharmaceutiques sont désignés comme : « *substances actives ou préparations contenant une ou plusieurs substances actives qui sont présentées sous la forme de laquelle elles sont livrées à l'utilisateur et qui sont destinées à protéger les végétaux ou les produits végétaux contres tous les organismes nuisibles ou à prévenir leur action ; exercer une action sur les processus vitaux des végétaux, pour autant qu'il ne s'agisse pas de substances nutritives, assurer la conservation des produits végétaux, détruire les végétaux indésirables, détruire les parties de végétaux, freiner ou prévenir une croissance indésirable des végétaux* ».

[496]https://www.ecophyto-pro.fr/fiches/fiche/23/les_produits_phytopharmaceutiques_statut_et_mise_en_marche/n:304

[497] Règl. n°1107/2009 du 21 oct. 2009, concernant la mise sur le marché des produits phytopharmaceutiques et abrogeant les directives 79/117/CEE et 91/414/CEE du Conseil : *JOUE* L.309/1 du 24 nov. 2009.

[498] *Ibid.*, art. 67.

[499] Les directions régionales de l'alimentation, de l'agriculture et de la forêt sont des services déconcentrés du ministère de l'Agriculture et de l'Alimentation. Elles ont pour mission de mettre en œuvre au niveau de la région la politique nationale en matière d'alimentation, d'agriculture et de forêt. Elles ont notamment pour missions de coordonner les contrôles sanitaires sur l'ensemble de la chaîne alimentaire (animale et végétale). Ces missions visent à garantir au consommateur des produits alimentaires sûrs et à permettre les échanges internationaux. Elles ont aussi, une mission d'information statistique, économique et géographique pour laquelle elles produisent et diffusent des informations économiques sur les exploitations, les industries agroalimentaires et les marchés

le bon usage des produits phytosanitaires par les exploitants. Les statisticiens du Service de la Statistique et de la Prospective (SSP) du Conseil national de l'information statistique (CNIS)[500] ont également pour mission de collecter les données phytosanitaires à travers une enquête quinquennale[501].

162- **Ouverture des données pour la réalisation d'une enquête statistique.** Le Règlement n°1185/2009 du 25 novembre 2009 relatif aux statistiques sur les pesticides[502] contraint les États membres à produire des données statistiques sur la mise sur le marché et l'utilisation des pesticides. À cette fin, aux termes de la loi n°51-711 de 1951 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques[503], les statisticiens peuvent procéder par des enquêtes, récupérer les informations relatives à la mise sur le marché et à l'utilisation des pesticides grâce aux registres de l'article 67 du Règlement n°1107/2009 du 21 octobre 2009, emprunter des sources administratives ou encore utiliser toute combinaison de ces moyens. Toutefois, le règlement ne prévoit pas d'accès direct aux données des agriculteurs. La question se pose alors de savoir si le SSP du CNIS peut accéder directement aux bases de données des agriculteurs détenues par les éditeurs de logiciels dans lesquelles les données liées aux pratiques culturales sont enregistrées et notamment celles concernant l'utilisation des produits phytosanitaires.

163- **Limites de la mise à disposition légale des données phytosanitaires contenues dans les bases de données.** La loi n°51-711 du 7 juin 1951 prévoit, en son article 1er, que les statistiques publiques regroupent l'ensemble des productions issues des enquêtes statistiques dont la liste est arrêtée chaque année par un arrêté du ministre chargé de l'économie. Cet article prévoit également l'exploitation, à des fins d'information générale, des données collectées par des administrations, des organismes publics ou des organismes privés chargés d'une mission de service public. C'est à ce titre que le SSP du CNIS mène tous les cinq ans une enquête sur l'utilisation des produits phytopharmaceutiques (PPP) sur 1 % des agriculteurs. En outre, cet article laisse entendre que le Règlement n°1185/2009 relatif aux statistiques sur les pesticides

alimentaires. Ces données constituent des références notamment pour le pilotage et l'évaluation des politiques publiques du ministère chargé de l'agriculture. C'est pourquoi elles surveillent l'évolution des pratiques et statistiques d'utilisation des produits phytosanitaires par les agriculteurs.

[500] Le Conseil national de l'information statistique est un organisme français créé en 1984, chargé de la concertation entre les producteurs et les utilisateurs de la statistique publique. Dans une démarche prospective, il a pour mission de mettre en lumière les nouveaux besoins des acteurs pour comprendre la société dans le domaine social et économique. Chaque année, il établit un programme de travaux et d'enquêtes statistiques pour répondre à ces besoins.

[501] Par exemple, l'enquête sur les pratiques culturales en grandes cultures en 2021 (PK GC 2021).

[502] *JOUE* L 324/1 du 10 déc. 2009.

[503] *JORF* du 8 juin 1951.

du 21 octobre 2009, précédemment évoqué, ne permet pas d'accéder directement aux données détenues par des personnes privées exerçant dans un cadre privé, les données doivent être récupérées *via* des enquêtes statistiques arrêtées chaque année par le ministre chargé de l'économie ou tout autre moyen prévu par la loi. Néanmoins, la Loi pour une république numérique de 2016 est venue apporter une modification à la loi sur l'obligation, la coordination et le secret en matière de statistiques de 1951 en intégrant un nouvel article 3 bis. Cet article instaure désormais la possibilité pour le ministre chargé de l'économie après avis du CNIS d'exiger des « *personnes morales de droit privé sollicitées pour des enquêtes qu'elles transmettent par voie électronique sécurisée au SSP, à des fins exclusives d'établissement de statistiques, les informations présentes dans les bases de données qu'elles détiennent, lorsque ces informations sont recherchées pour les besoins d'enquêtes statistiques qui sont rendues obligatoires en application de l'article 1er bis* ».

Par conséquent, désormais à la lecture de ce texte, les personnes morales peuvent être contraintes de transmettre les données qu'elles détiennent dans leurs bases de données lorsqu'elles sont sollicitées par une enquête. Néanmoins, cette hypothèse laisse planer un doute sur sa portée. En effet, la question se pose de savoir si la personne morale doit mettre à disposition toutes les données visées par une enquête qu'elle détient, même celles produites ou collectées par d'autres personnes ou seulement les données qu'elle produit elle-même par son activité. Par exemple, un arrêté du 13 avril 2017 prévoit une obligation pour « *les personnes morales dont un des établissements [ayant] une activité de commerce de détail en magasin non spécialisé à prédominance alimentaire de plus de 400 m2 [de transmettre] par voie électronique à l'INSEE les données nécessaires à la réalisation de l'enquête statistique pour l'indice des prix à la consommation et l'enquête mensuelle sur l'activité de grande surface alimentaire […]* »[504]. Dans cet exemple, les données mobilisées dans le cadre des enquêtes auprès des personnes morales sont des données que les personnes morales produisent ou collectent elles-mêmes, c'est-à-dire, en lien direct avec leur activité. En revanche, dans le cas des données phytosanitaires, ces données sont liées à l'activité des agriculteurs utilisant les objets connectés et les services informatiques. L'enquête portant sur les pratiques culturales en grandes cultures qui permet de collecter les données sur les usages des produits phytosanitaires vise les exploitants agricoles et non pas les entreprises qui fournissent les logiciels de saisie ou de collecte des données. Par conséquent, il faut s'interroger sur la possibilité d'accéder aux données concernant l'activité des clients d'une personne morale à des fins statistiques.

[504] Arrêté du 13 avr. 2017 rendant obligatoire la transmission de données par voie électronique à des fins de statistique publique : *JORF* n°0103 du 2 mai 2017, art. 1er.

Néanmoins, là où la loi ne distingue pas, il n'y a pas lieu de distinguer, donc en l'absence de précision, les personnes morales sont tenues par ce dispositif de mettre à disposition les données qu'elles détiennent sans distinction de leur origine. De plus, en attendant la promulgation du règlement sur les données, le *Data Act* proposé le 23 février 2022, le Droit ne prévoit pas pour l'heure, de maîtrise des données non personnelles pour celui qui les produit. Par conséquent, les agriculteurs ne peuvent pas en l'état actuel du droit positif revendiquer une quelconque maîtrise juridique sur l'accès à ces données. De même, les données à caractère personnel, éventuellement collectées à cette fin, pourront être traitées à des fins statistiques puisque le RGPD prévoit que tout traitement ultérieur à des fins statistiques est considéré comme compatible avec les finalités initiales de la collecte des données[505]. Ce traitement peut se réaliser à condition, toutefois, de respecter les conditions prévues par le RGPD et qu'il ne soit pas utilisé pour prendre des décisions à l'égard des personnes concernées[506].

Cela étant dit, la mise en œuvre d'un tel dispositif d'accès aux données contenues dans les bases des personnes morales doit au préalable faire l'objet d'une concertation entre le ministre en charge de l'Économie et les personnes morales sollicitées par ces enquêtes[507]. Également, une étude de faisabilité et d'opportunité doit être réalisée et rendue publique[508]. Or, certaines entreprises pourront refuser la mise à disposition des données phytosanitaires qu'elles détiennent afin de conserver la confiance des agriculteurs en ne divulguant pas leurs données. Le juge ou le législateur devrait préciser la portée de ce dispositif d'accès à des données générées lors d'une activité privée.

Pour l'heure, il est donc assez difficile d'accéder aux données agricoles privées générées dans le cadre d'activités privées pour l'Administration. En outre, l'accès aux données privées d'intérêt général des agriculteurs reste limité pour le service de la statistique et de la prospective (SSP).

164- **Évolution législative.** La proposition de règlement relatif aux statistiques sur les intrants et les produits agricoles (SAIO)[509] envisage la possibilité pour les Instituts Nationaux de Statistiques

---

[505] RGPD, art. 5, 1e, b) : « *Le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités)* » ; voir RGPD, art. 89 sur les Garanties et dérogations applicables au traitement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

[506] Voir *infra*, n°711 et s.

[507] Loi n°51-711 de 1951 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistiques : *JORF* du 8 juin 1951, art. 3 bis.

[508] *Ibid.*

[509] Proposition de règlement relatif aux statistiques sur les intrants et les produits agricoles et abrogeant les règlements n°1165/2008, n°543/2009, n°1185/2009 et la directive 96/16/CE du Conseil, COM/2021/37 final, 2 févr. 2021.

(INS) et les autres autorités nationales d'accéder directement et immédiatement à toutes les données administratives collectées à des fins publiques, qu'elles soient détenues par des organismes publics ou privés, de même qu'un droit d'utilisation de ces données. Les INS devraient pouvoir intégrer ces données administratives aux statistiques. Mais cette proposition porte sur les données administratives collectées à des fins publiques, ce qui laisse entendre qu'il s'agit là encore de données collectées au cours d'une mission de service public. Par conséquent, seront exclues, une fois de plus, les entreprises privées exerçant une activité privée et de surcroît les exploitants agricoles. De manière plus élargie, le règlement sur la gouvernance européenne des données (DGA)[510] prévoit le partage altruiste de données qui peut, de prime à bord, répondre aux attentes concernant l'ouverture des données d'intérêt général. Cependant, ce dispositif fondé sur le volontariat ne semble pas en adéquation avec la collecte de données aussi sensibles que celles portant sur l'utilisation des produits phytosanitaires. Néanmoins, il est à noter que le règlement sur les données (*Data Act*)[511], pourrait faciliter la mise à disposition de ces données puisque les moyennes et grandes entreprises seront tenues de transmettre les données privées qu'elles détiennent aux administrations qui doivent « *s'acquitter d'une mission de service public prévue par la loi* »[512] dans des conditions déterminées par le règlement. Aussi, les entreprises de l'agriculture numérique qui détiennent des données phytosanitaires pourraient, à ce titre, être tenues de les mettre à disposition.

Cet exemple permet de se rendre compte que, pour l'heure, l'accès aux données privées d'intérêt général des agriculteurs est fortement limité à la fois pour le service de la statistique et de la prospective (SSP) et, au-delà, pour toute personne qui souhaiterait accéder à ces données.

2. La reconnaissance de l'ouverture des données phytosanitaires pour l'intérêt général ou commun

165- **Problématique.** Si l'accès aux données phytosanitaires contenues dans des bases de données privées est encore compliqué pour l'Administration, il devient quasiment impossible pour toutes les autres personnes qui souhaiteraient accéder à ces données. Dans le cadre du dispositif de l'article 3 bis de la loi n°51-711 du 7 juin 1951, ce n'est qu'une fois que les données sont

[510] Règl. n°2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement n°2018/1724 (règlement sur la gouvernance des données) : *JOUE* L 152/1 du 3 juin 2022.
[511] Proposition règl. fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (Règl. sur les données), 23 févr. 2022, COM (2022) 68 final.
[512] Règlement sur les données, préc., art. 15.

reçues par les autorités administratives qu'elles deviennent publiques et communicables au tiers. Également, l'article 67 du Règlement n°1109/2009 du 21 octobre 2009 prévoit la mise à disposition des informations sur l'utilisation des produits phytosanitaires par un système d'intermédiation. Les habitants peuvent, en effet, faire la demande auprès de l'autorité publique qui peut, ensuite, demander la communication des registres contenant les informations sur l'utilisation des produits phytosanitaires. Il y a donc un principe d'intermédiation entre le producteur de données et les tiers qui souhaitent accéder à ces informations. Dans les faits, les données phytosanitaires sont très peu accessibles. En ce qui concerne l'enquête sur les pratiques culturales en grandes cultures, seulement une infime partie des 28 000 agriculteurs (1 %) utilisant ces produits sont contrôlés tous les cinq ans[513] et donc très peu de ces données sont communiquées. En dehors des obligations de communication aux autorités compétentes pour collecter ces données phytosanitaires, aucune obligation de communication aux tiers ne repose sur les agriculteurs. De toute évidence, l'accès aux données phytosanitaires est somme toute restreint.

Par ailleurs, les documents, y compris les données, produits ou reçus par toute personne physique ou morale et par tout service ou organisme public ou privé dans l'exercice de leur activité deviennent des archives, et ce quel que soient leur date, leur lieu de conservation, leur forme et leur support, au sens de l'article L. 211-1 du Code du patrimoine. Aussi, l'article L. 211-4 du Code du patrimoine précise que les archives publiques sont, entre autres, « *les documents qui procèdent de l'activité de l'État, des collectivités territoriales, des établissements publics et des autres personnes morales de droit public* », ainsi que « *les documents qui procèdent de la gestion d'un service public de l'exercice d'une mission de service public par des personnes de droit privé* ». Ces archives publiques sont conservées dans l'intérêt public pour les besoins de la gestion et de la justification des droits des personnes physiques ou morales, publiques ou privées et pour la documentation historique de la recherche[514]. Par conséquent, les données phytosanitaires qui ont été collectées par les administrations pour la réalisation d'une mission de service public deviennent des archives publiques communicables de plein droit aux termes de l'article L. 213-1 du Code du patrimoine une fois seulement qu'elles ont été agrégées et anonymisées[515].

[513] Par exemple, enquête sur les pratiques culturales en grandes cultures en 2021 (PK GC 2021).
[514] C. patr., art. L. 211-2.
[515] CRPA, art. L. 312-1-2 : Les données phytosanitaires ne font pas partis des exceptions comprises dans le D. n°2018-1117 du 10 déc. 2018 relatif aux catégories de documents administratifs pouvant être rendus publics sans faire l'objet d'un processus d'anonymisation préalable : *JORF* n°0287, du 12 déc. 2018.

166- **Données phytosanitaires et données environnementales.** Il existe un principe d'accès aux informations relatives à l'environnement inscrit à l'article 7 de la Charte de l'environnement. Cet article reprend les principes de l'article 1er de la Convention d'Aarhus[516] et prévoit le principe de communication des informations environnementales. Celles-ci portent notamment sur « *les substances [...] qui ont ou risquent d'avoir des incidences sur les éléments de l'environnement tels que l'air et l'atmosphère, l'eau, le sol, les terres, le paysage et les sites naturels* ». Deux arrêts de la CJUE du 23 novembre 2016 ont retenu que les informations relatives à des émissions dans l'environnement des produits phytosanitaires, des biocides et sur les substances qu'ils contiennent sont des données communicables même en présence d'un secret des affaires[517]. La CJUE en a conclu que le droit à l'information portant sur la nature, la composition, la quantité, la date et le lieu de ces émissions, ainsi que les données relatives aux effets des produits émis, ne saurait être limité par la liberté d'entreprise ou le « droit de propriété » garantissant la confidentialité des données non divulguées dans le cadre d'une autorisation de mise sur la marché de produits phytopharmaceutiques. Cependant, cette obligation de communication des données environnementales ne contraint que les autorités publiques[518]. Celles-ci sont déterminées par l'article L. 124-3 du Code de l'environnement comme « *l'État, les collectivités territoriales et leurs groupements, les établissements publics* » ainsi que « *les personnes chargées d'une mission de service public en rapport avec l'environnement, dans la mesure où ces informations concernent l'exercice de cette mission* ». Par conséquent, parmi les personnes morales détenant des données environnementales, seules celles qui exercent une mission de service public et dont l'activité a un rapport avec l'environnement sont soumises à l'obligation de communication des données environnementales qu'elles détiennent. C'est le cas notamment des entreprises qui par leur activité exposent les personnes et les biens à des risques significatifs tels que le nucléaire[519], les

[516] Convention sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement, (conv. d'Aarhus), 25 juin 1998.
[517] CJUE, 5e ch., 23 nov. 2016, aff. C-442/14, *Bayer CropScience SA-NV, Stichling De Bijenstichling* c/*College Voor de Toeliating van quasbeschermingsmiddelen en biociden* : JurisData n°2016-027449 ; obs. EMMANOUILIDOU, *RJ envir*. 2017. 179 ; note JAMAY, *EEI* 2017, n°23 ; note THEVENOT, *Dr. envir*. 2017. 67 ; obs. CAZET S., *Europe* 2017, n°2 et CJUE, 5e ch., 23 nov. 2016, aff. C-673/13, P., *comm.* c/*Stichling Greenpeace Nederland et PAN Europe* : *RJ envir*. 2017.180, obs. EMMANOUILIDOU; *EEI* 2017, no 23, note JAMAY; *Dr. envir.* 2017. 67, note THEVENOT.
[518] Conv. d'Aarhus, préc., art. 4 ; Règl. n°1367/2006 du 6 sept. 2006 concernant l'application aux institutions et organes de l' « Union » européenne des dispositions de la convention d'Aarhus sur l'accès à l'information, la participation du public au processus décisionnel et l'accès à la justice en matière d'environnement : *JOUE* L 264 du 25 sept. 2006, art. 4 ; C. env., art. L.124-1 et s. ; Dir. n°2003/4/CE du 28 janv. 2003 concernant l'accès du public à l'information en matière d'environnement : *JOUE* L 41/26 du 14 févr. 2003 ; Charte de l'environnement, art. 7.
[519] C. env., art. L. 125-10.

déchets[520] ou à d'autres risques majeurs[521]. Certaines entreprises[522] ont également des obligations de rapportage extrafinancier[523] qui consistent à communiquer les implications sociales, environnementales, sociétales de leurs activités ainsi que sur leur mode de gouvernance[524]. Ainsi, les agriculteurs et les entreprises privées qui détiennent les données environnementales dans des logiciels de gestion de parcelle ne sont pas soumis à cette obligation. Donc, seules les personnes exerçant une mission de service public ont l'obligation de communiquer les données environnementales agricoles. La DRAAF[525], par exemple, publie les données de l'agriculture qu'elle détient, qui sont issues pour l'essentiel des enquêtes statistiques (statistiques agricoles annuelles, recensement agricole décennal…) et des données de la PAC.

167.- **Future ouverture généralisée des données environnementales ?** Les données environnementales sont encore loin d'être ouvertes à tous. Toute personne qui souhaite accéder à ces données doit, d'abord, faire sa demande auprès d'une personne publique. Or, il semble qu'il faille désormais rompre avec ce système d'intermédiation dans l'accès aux données environnementales pour parvenir à une ouverture généralisée des données environnementales agricoles. Certains auteurs plaident pour une « *désintermédiation dans la mise en œuvre du droit à l'information du public* »[526]. En effet, « *si les informations environnementales ont à être divulguées, c'est en raison de leur objet davantage qu'en raison du caractère public ou privé de la personne qui les détient* »[527]. Or, l'objet de ces données est l'environnement reconnu comme bien commun au sens du préambule de la Charte de l'environnement. Ce caractère commun de l'environnement a été rappelé dans la décision n°2019-823 du Conseil constitutionnel du 31 janvier 2020[528]. Dans cette décision, une question prioritaire de

[520] C. env., art. L. 125-1.
[521] C. env., art. L. 252-2.
[522] Une déclaration de performance extrafinancière doit être élaborée par une entreprise, lorsque son total du bilan ou son chiffre d'affaires et son nombre de salariés dépassent les seuils suivants : pour toute société cotée, 20 millions d'euros pour le total du bilan ou 40 millions d'euros pour le montant net du chiffre d'affaires et 500 pour le nombre moyen de salariés employés au cours de l'exercice. Pour toute société non cotée : 100 millions d'euros pour le total du bilan ou le montant net du chiffre d'affaires et 500 pour le nombre moyen de salariés.
[523] Dir. 2014/95/UE, 22 oct. 2014 modifiant la directive 2013/34/UE en ce qui concerne la publication d'informations non financières et d'informations relatives à la diversité par certaines grandes entreprises et certains groupes : *JOUE* L 330/1 du 15 nov. 2014.
[524] *Ibid.*, codif. C. com., arts. L. 225-102-1 et R. 225-104 à R. 225-105-2.
[525] https://draaf.occitanie.agriculture.gouv.fr/Donnees-detaillees.
[526] EPSTEIN, A.-S., « La compatibilité du droit d'accès aux informations environnementales de source privée avec la protection du secret des affaires : Prélude à la consécration d'un droit d'accès aux données d'intérêt général de source privée », *RJE*, 2020/HS20 n° Spécial, pp. 137-149 ; ROCHFELD, J., CORNU, M. et MARTIN, G., J., ss. dir., *L'échelle de communalité*, *op. cit*.
[527] EPSTEIN, A.-S., *Ibid.*
[528] Cons. const., déc. n°2019-823, QPC, 31 janv. 2020, *Union des industries de la protection des plantes* : Pan. DEBAETS E. et JACQUINOT, N., *D.S.*, 2021. 24 ; chron. VERPEAUX M., MACAYA A., *JCP G* 2021. 39 ; chron.

constitutionnalité (QPC) avait été posée par l'association *Union des industries de la protection des plantes*, il s'agissait de se demander si la liberté d'entreprendre pouvait être limitée par la poursuite des objectifs de valeur constitutionnelle de protection de l'environnement et de la santé. Cette demande concernait l'interdiction à compter du 1er janvier 2022, de la production, du stockage et de la circulation des produits phytopharmaceutiques contenant des substances actives non approuvées pour des raisons liées à la protection de la santé humaine ou animale ou de l'environnement prévue à l'article L. 253-8 du Code rural. L'association considérait cette interdiction comme portant atteinte à la liberté d'entreprendre. Le Conseil d'État avait alors saisi le Conseil constitutionnel le 7 novembre 2019 d'une QPC, qui avait décidé que ces dispositions étaient conformes à la Constitution et a donné une portée significative à la formule présente dans le préambule de la Charte de l'environnement qui décrit l'environnement comme « *un patrimoine commun des êtres humains* ». Aussi, dans une proposition de réforme pour intégrer les biens communs[529] en Droit, dirigée par Mme la Professeure J. Rochfeld, les auteurs proposent de considérer une échelle de communalité[530]. Ainsi, comme le synthétise Mme A-S. Epstein « *certaines catégories d'informations revêtent une communalité renforcée et sont ainsi destinées à triompher systématiquement du secret des affaires : c'est le cas des informations relatives à des émissions de substances dans l'environnement (art. 4 Convention Aarhus)*[531] ».

168- **Ouverture méthodique des données d'intérêt général ou d'intérêt commun.** Par conséquent, au regard de ces éléments, les données phytosanitaires devraient être ouvertes largement par les personnes qui les produisent ou les détiennent, afin de respecter le droit à l'information et pour la réalisation de mission de service public. Plus largement, s'agissant des données agricoles privées, il faudra faire une balance entre le droit à l'information et le secret

---

VIDELIN J.-C., *JCP A*, 2021. 21 ; chron. FONBAUSTIER L., *Energie – Environnement – Infrastructures*, 2021, 4 ; pan. HOURSON S., *Rev. Du Centre Michel de l'Hospital,* 2021, 22 ; chron. PEGLION-ZIKA C.-M., *RLDC*, 2021, 190 ; Comm. TORRE-SCHAUB M., *AJFP*, 2020, 43 ; KAMAL-GIRARD M., *LGP*, 2020, 25 ; chron. ROBLOT-TROIZIER A., *RFDA*, 2020, 501 ; comm. ATTARD J., *LPA*, 2020, 10 ; note BRAMERET S., RLC, 2020, 26 ; chron., MARTINEZ J., *Concurrences*, 2020, 211 ; Pan., CLAVEL S. et JAULT-SESEKE F., *D.S.*, 2020, 951 ; MONTEILLET V. et LERAY G., *D.S.*, 2020, 1012 ; Ét. BILLET P., *JCP A*, 2020, 44 ; chron. AUDUBERT V., *RDH*. 2020. 14 ; note PARANCE B et MABILE S., *DS*. 2020. 20 ; SALLES S., *LGP*. 2020. 24 ; Pan. REBOUL-MAUPIN N. et STRICKLER Y., *D.S*. 2020. 31 ; Pan. AVOUT L. BOLLE S. et FAMOUX É., *D.S*. 2020. 35.(Interdiction de la production, du stockage et de la circulation de certains produits phytopharmaceutiques).

[529] ROCHFELD, J., CORNU, M. et MARTIN, G., J., ss. dir., *L'échelle de communalité*, *op. cit.*

[530] *Ibid.* : La communalité peut « *se définir sur le fondement de deux critères. D'une part, elle porte une affectation à un type d'intérêt particulier, soit à un intérêt commun socialement et juridiquement reconnu, tels l'usage commun d'une ressource, un impératif de conservation, une volonté de s'organiser pour participer au gouvernement d'une chose, le tout au bénéfice d'une communauté large (nationale, régionale ou mondiale ; présente, future, transgénérationnelle) ou plus restreinte (de malades, d'habitants, de personnes intéressées et organisées, etc.). D'autre part, elle implique une inclusivité, soit l'impossibilité d'exclure les autres […]* ».

[531] Conv. d'Aarhus, préc., art. 4 ; dir. 2003/4 du 28 janv. 2003 concernant l'accès du public à l'information en matière d'environnement et abrogeant la directive 90/313/CEE du Conseil : *JOUE* L 41/26 du 4 févr. 2003, art. 4 ; C. env., art. L. 124-5.

des affaires afin d'identifier les données d'intérêt général ou d'intérêt commun devant être ouvertes.

II. La consécration du droit d'accès du générateur de la donnée

169- Si l'exploitant agricole peut toujours avoir accès à ses données à caractère personnel[532], l'accès aux données à caractère non personnel de son exploitation n'est jamais garanti. Bien que la plupart des prestataires de services reconnaissent l'accès aux données de l'exploitation aux agriculteurs, l'arrivée sur le marché d'industriels étrangers fait craindre que les exploitants agricoles n'aient pas toujours accès à leurs données. En effet, par exemple, certains groupes américains créent une dépendance pour les agriculteurs qui souhaitent réparer leurs machines, par exemple, en baguant les logiciels embarqués afin que seuls les réparateurs agréés de la machine puissent faire les réparations[533]. Ceci a de lourdes conséquences pour les agriculteurs qui sont soumis aux délais parfois très longs des réparateurs pour leurs interventions pratiquées à des coûts exorbitants. Ils sont alors parfois obligés de hacker les logiciels de leurs machines afin d'intervenir eux-mêmes. La reconnaissance d'un droit d'accès de principe aurait donc vocation à limiter ces comportements prédateurs. Par ailleurs, l'harmonisation des régimes d'accès aux données personnelles et non personnelles offrirait une simplification louable. Par conséquent, avant d'envisager l'éventualité de la création d'un droit d'accès de principe pour les données à caractère non personnel (**B**), il est nécessaire d'analyser, d'abord, le régime de l'accès aux données à caractère personnel (**A**).

A. L'accès entériné aux données à caractère personnel de l'agriculteur

170- Il convient d'envisager le principe du droit d'accès (**1**), puis d'en rappeler les limites (**2**).

[532] Voir *infra*, n°730 et s.

[533] EUDES, Y., « Les agriculteurs hackeurs du Nebraska », *in Le Monde,* https://www.lemonde.fr/pixels/visuel/2017/08/08/agro-hackeurs-du-nebraska_5170156_4408996.html.

1. Le principe du droit d'accès aux données à caractère personnel

171- L'article 15 du Règlement général sur la protection des données (RGPD)[534] prévoit un droit d'accès aux données à caractère personnel pour la personne physique concernée. Cette dernière peut faire la demande d'accès directement auprès du responsable de traitement, autrement dit, l'entreprise qui collecte et traite les données de l'agriculteur. L'accès aux données à caractère personnel est limité à la seule personne concernée. Ce droit d'accès est en principe gratuit, sauf « *si les demandes sont manifestement infondées ou excessives* »[535]. La CNIL est compétente pour traiter tous conflits relatifs aux demandes d'accès aux données à caractère personnel.

2. Les limites du droit d'accès aux données à caractère personnel

172- Les exploitants agricoles ont en principe le droit d'exiger l'accès aux données qui les concernent parmi celles que collectent et traitent les éditeurs de logiciels ou d'autres prestataires de services. Mais, pour cela, encore faut-il déterminer quelles sont les données collectées sur les exploitations qui permettent effectivement d'identifier une personne physique[536]. En effet, dès lors que le traitement de la donnée permet d'identifier ou de rendre identifiable la personne physique, il est soumis aux règles du RGPD. Il est, cependant, très compliqué de délimiter les données qui sont effectivement personnelles de celles qui ne le sont pas parmi les très nombreuses données collectées sur les exploitations agricoles. Aussi, les acteurs n'ont pas toujours conscience du caractère personnel des données qu'ils collectent et traitent. Par conséquent, afin d'exiger un accès aux données à caractère personnel, encore faut-il avoir connaissance que l'entreprise traite ce type de données. Ainsi, l'agriculteur n'aura, également, pas toujours conscience des données qui sont effectivement collectées dans son champ. Ainsi, cette réglementation a surtout vocation à s'appliquer aux données que l'agriculteur fournit pour créer son compte d'utilisateur afin d'accéder au contenu du logiciel ou de l'application ou bien encore pour la souscription à l'abonnement permettant l'utilisation des outils informatiques mis à disposition.

---

[534] Règl. n°2016/679 du 27 avr. 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données et abrogeant la directive 95/46/CE : *JOUE* L 119/1 du 4 mai 2016.
[535] RGPD, art. 12, 5e.
[536] Voir *infra*, n°702 et s.

B. La consécration du droit d'accès de principe aux données non personnelles du générateur de données

173- S'agissant de l'accès aux données à caractère non personnel, il convient d'envisager, tout d'abord, le fondement du droit d'accès (**1**), puis son contenu (**2**).

1. Le fondement du droit d'accès

174- **Fondements non retenus.** En premier lieu, Portalis écrivait que « *l'homme n'eut jamais bâti, semé ni planté, s'il n'eut été sûr de conserver la propriété de ce qu'il acquérait par le travail* »[537]. L'article 546 du Code civil prévoit en ce sens que « *la propriété d'une chose, soit mobilière, soit immobilière, donne droit sur ce qu'elle produit, et sur ce qui s'y unit accessoirement, soit naturellement, soit artificiellement. Ce droit s'appelle droit d'accession* ». Le droit d'accession permet au propriétaire de la chose principale frugifère d'obtenir automatiquement la propriété de l'accessoire. C'est ainsi que *l'accessoire suit le principal*. Appliqué à l'agriculture numérique, le droit d'accession supposerait que l'objet connecté permette de matérialiser des éléments de fait préexistants dans le fonds informationnel que constitue l'exploitation agricole. Les données brutes de l'exploitation collectées par le biais de ces objets connectés seraient donc rattachées à l'activité de l'exploitant agricole sur son fonds. La cause éminente de ces données serait le fonds agricole. De manière analogique, un arrêt de la Cour de cassation du 10 octobre 2019 a retenu que « *si les fruits générés par l'exploitation viticole sont certes des fruits industriels, ils n'en sont pas moins restituables au propriétaire puisque leur cause éminente reste la terre et que le Code civil envisage l'accession, et non, l'industrie, en cause de propriété* »[538]. Il s'agissait, ici, de déterminer qui du propriétaire du fonds ou de l'exploitant, possesseur de mauvaise foi, devait obtenir les fruits de l'exploitation. Les juges ont décidé que le raisin, fruit des vignes, devait revenir au propriétaire du sol du fait de l'accession. L'accession prime, donc, la force de travail et l'industrie personnelle. Ainsi, cet arrêt appliqué aux données agricoles laisserait supposer que lorsqu'il est propriétaire du fonds, l'exploitant agricole doit obtenir tout ce qui s'unit au sol. Les données seraient donc attachées

---

[537] PORTALIS, F. et PORTALIS, J.-E.-M., *Discours et rapports sur le Code civil*, PUC, 06/2010.

[538] Civ. 3e ch., 10 oct. 2019, n°16-21.177 : Juris-Data n°2019-017692 Inédit ; comm. MEILLER E., *Rev. droit rural*. 2020. 480 ; pan. ROUX J.-M. *Annales des loyers*. 2019. 12 : Dans cet arrêt les demandeurs, des exploitants viticoles, reconnus comme possesseurs de mauvaise foi, demandaient à conserver les fruits industriels, les raisins, issus de leur force de travail et de leur industrie personnelle. Les juges du fond ont rejeté leur pourvoi au motif que « *le possesseur de mauvaise foi est tenu de restituer au propriétaire non seulement les fruits naturels ou industriels de la terre perçus, mais encore ceux qu'il a négligé de percevoir, et relevé* ».

au sol. Or, l'entreprise de l'agriculture numérique, en tant que fournisseur de services, ne fait que collecter les données brutes au nom et pour le compte de l'exploitant agricole en échange d'une contrepartie financière.

Néanmoins, la théorie du droit d'accession appliquée aux données semble bancale du fait que le droit d'accession emporte l'appropriation de l'accessoire. Or les données ne peuvent pas être objet de propriété[539].

M. le Professeur J.-C. Galloux s'est penché sur la question de l'accès aux données et a proposé de s'appuyer sur le *jus fundi* du Droit civil[540]. En effet, le droit du fonds ou *jus fundi* permet de reconnaître la propriété de la chose découverte au propriétaire du fonds ou à concurrence de la moitié avec la personne qui a découvert la chose, autrement dit l'inventeur. En revanche, lorsqu'un contrat est conclu justement pour la découverte de cette chose, le propriétaire du fonds reste seul propriétaire de la chose découverte. Appliqué aux données agricoles, le *jus fundi* permettrait de reconnaître l'exploitant agricole comme propriétaire des données issues de son exploitation. En effet, son fonds agricole constituerait un fonds informationnel privé sur lequel il détiendrait la maîtrise juridique de la chose découverte, c'est-à-dire, la donnée. Autrement dit, en tant que propriétaire du fonds informationnel, l'agriculteur devrait nécessairement détenir les droits sur les données issues de son exploitation. Ainsi, il n'entrerait plus en concurrence avec l'entreprise qui collecte les données puisque cette dernière ne serait qu'un simple prestataire de services agissant au nom et pour le compte de l'exploitant agricole par le biais d'un contrat de prestation de services. Cette entreprise n'aurait donc plus la maîtrise de l'accès aux données. Au contraire, l'exploitant agricole bénéficierait des prérogatives d'un propriétaire sur les données issues de son fonds, parmi lesquelles figure l'accès. Pour ainsi dire, il disposerait d'un droit exclusif sur les données brutes collectées ou produites lors de son activité agricole. Selon ce même auteur, la télédétection fournit un bon exemple de l'application du *jus fundi* en faveur du propriétaire du fonds. En effet, afin de résoudre un conflit entre l'État observé et le détenteur des données l'Assemblée générale de l'ONU a décidé dans sa résolution 41/65 du 3 décembre 1986 que l'État observé aura dorénavant accès aux données concernant le territoire relevant de sa juridiction, sans discrimination et à des conditions de prix raisonnables. L'objectif serait donc de redonner une maîtrise sur les données issues de leur exploitation aux agriculteurs et de leur redonner du pouvoir face à la puissance économique des entreprises de l'*AgTech*. Mais ce fondement, comme le précise également M. le Professeur J.-C. Galloux, ne devrait pas permettre de

[539] Voir *infra*, n°504 et s.
[540] GALLOUX, J.-C., « Libres propos sur le droit d'accès aux données », *op. cit.*

reconnaître un droit réel sur les données. Mme H. Juillet-Régis[541] considère également qu'il serait délétère de reconnaître un tel droit sur les données, puisque ceci aurait pour conséquence de considérer la valeur intrinsèque de la donnée alors que c'est par son usage que la donnée crée de la valeur. En outre, évoquer le droit du fond permet simplement de trouver des arguments permettant de justifier un droit d'accès et de contrôle sur l'accès aux données en faveur du co-contractant générateur de la donnée[542]. En outre, cette démonstration ne peut servir que d'élément de définition, elle n'a pas pour effet ou pour objet d'organiser une prérogative patrimoniale sur les données brutes pour l'exploitant agricole. Il s'agit simplement de démontrer le lien entre le fonds agricole et les données qui y sont produites ou collectées. C'est un appui théorique à la fondamentalisation de la maîtrise juridique sur les données brutes d'exploitation. Il ne s'agit en aucun cas de la preuve d'un droit de propriété sur les données industrielles.

175- **Fondements retenus.** Le fondement du droit d'accès doit reposer sur son intérêt économique. Effectivement, les exploitants agricoles s'inquiètent de la perte de maîtrise des données qu'ils génèrent sur leur exploitation. Or, pour obtenir la maîtrise des données, encore faut-il y avoir accès. Cette question de l'accès en faveur de l'agriculteur peut sembler anecdotique si l'on considère comme M. le Professeur G. Pillet que l'accès se confond avec le service[543]. Tant et si bien que la question de l'accès ne se poserait pas dans les relations entre l'agriculteur et le fournisseur de services ou d'équipements agricoles, mais seulement dans les relations avec les tiers[544]. D'autant que les entreprises de l'*AgTech* sont plutôt enclines à donner l'accès aux données brutes pour les exploitants agricoles, dès lors qu'ils paient leur abonnement. En effet, elles prévoient dans leur contrat une clause de réversibilité permettant aux agriculteurs de récupérer les données brutes générées sur leur exploitation à l'issue de la relation contractuelle. Mais cet accès semble, néanmoins, précaire puisqu'il est conditionné au paiement de l'abonnement et que la demande de réversibilité est à la charge de l'exploitant agricole. Aussi, parce que « ce qui va de soi va mieux en le disant », la question de l'accès aux données doit aujourd'hui être prise en considération par le législateur. Si l'agriculteur a un droit d'accès aux données, l'entreprise en conserve la maîtrise. Rien n'interdit les entreprises à autoriser l'accès aux données non personnelles collectées à des tiers au contrat. Ceci fait craindre pour les agriculteurs que les données produites ou collectées dans leur exploitation soient utilisées à des

[541] JUILLET-REGIS, H., « Quelle régulation pour les données agricoles ? », *Droit rural*, n°479, janv. 2020, coll. 5.
[542] Sur la notion de co-contractant générateur de la donnée, voir *infra*, n°611 et s.
[543] PILLET, G., « L'efficacité du droit français des contrats face aux géants de l'internet », *RTD com.* 2018, p. 273.
[544] Voir DOUVILLE, T., « Contrat et données agricoles », *Droit rural* n°469, janv. 2019, dossier 3.

fins contraires à leurs propres intérêts. Par exemple, les entreprises peuvent accorder l'accès aux données à d'autres professionnels ou revendre les données à des agriculteurs concurrents, ce qui aurait pour effet de fausser le libre jeu de la concurrence.

De plus, les entreprises ont tout intérêt à retenir les données brutes afin de se constituer un monopole et d'éviter que les exploitants agricoles ne transmettent lesdites données à la concurrence. Pour cela, d'un point de vue technique, les entreprises ne rendent pas toujours interopérable leur système informatique, ce qui a pour conséquence de restreindre l'accès aux données. L'absence d'interopérabilité contribue, en outre, à la limitation de la circulation des données. Ces constatations soulèvent des interrogations au sujet de la légitimité des entreprises à détenir un tel pouvoir de contrôle sur l'accès aux données brutes des exploitations. Or, comme la question de l'exploitation de l'image des biens en son temps[545], l'exploitation des données agricoles interroge sur les enjeux économiques de la maîtrise de l'accès aux données. La « *forte valeur économique* »[546] qu'a acquise l'exploitation des données justifie l'intervention juridique puisque, comme pour l'exploitation de l'image des biens, « *cette valeur économique est essentiellement due aux possibilités de circulation de la richesse elle-même favorisée par les nouvelles technologies, hier la photographie, le cinéma ou la télévision, aujourd'hui nos autoroutes de l'information* »[547]. La valeur d'usage des données collectées sur les exploitations représente un tel enjeu économique qu'il est désormais primordial de régir leur accès et d'assurer un accès de principe au fournisseur, générateur, de données — l'agriculteur — afin d'éviter d'éventuelles restrictions injustifiées. Ainsi, la fonction de ce nouveau droit d'accès serait, dans un premier temps, économique dans la mesure où il permettrait de replacer l'agriculteur au centre de l'économie de la donnée et de lui offrir un accès permanent aux données brutes générées sur son exploitation. Ce droit devrait permettre, dans un second temps, d'assurer la maîtrise des données brutes par l'exploitant agricole en lui permettant de faire circuler les données selon ses besoins technologiques tout en contribuant à la recherche et à l'innovation. Ce droit d'accès devrait donc rester un droit personnel régi par le contrat entre l'agriculteur et l'entreprise qui détient les données. Mais il doit devenir un principe légal et non plus l'exception d'un régime réservataire.

[545] BRUGUIERE, J.-M., « L'exploitation de l'image des biens », *Légicom*, 2005/2, n°34, pp. 13 à 34.
[546] Termes repris de BRUGUIERE, J.-M., *ibid.*
[547] BRUGUIERE, J.-M., « L'exploitation de l'image des biens », *ibid*.

2. Les contours du principe légal de l'accès

176- **Objet du droit d'accès.** Le droit d'accès ne doit porter que sur les données brutes de l'exploitation, c'est-à-dire, celles qui sont collectées telles quelles *via* les objets connectés. Il faut donc exclure les données enrichies par les entreprises de l'*AgTech*. Cependant, tout enrichissement ne doit pas permettre de limiter le droit d'accès, sans quoi les entreprises pourraient revendiquer la maîtrise sur les données au moindre apport, même minime. Il conviendra, par conséquent, de délimiter les conditions de l'enrichissement[548].

177- **Titulaire du droit d'accès.** Celui qui détient le droit d'accès est celui qui a généré les données par son activité. Dans le même sens, le Code de conduite de l'Union européenne sur le partage des données agricoles par accord contractuel octroie la maîtrise de l'accès au créateur de la donnée, c'est-à-dire « *la personne ou l'entité qui peut prétendre disposer d'un droit exclusif d'accorder l'accès aux données et de contrôler leur utilisation […]* ». Ainsi, l'accès est le préambule des droits d'usage du titulaire des droits sur les données. Autrement dit, le droit d'accès constitue un droit préliminaire à la maîtrise des données par l'exploitant agricole. Sans possibilités d'obtenir l'accès aux données brutes, l'exploitant agricole ne pourra pas faire valoir son droit de contrôle sur les données issues de son exploitation. Or, les données agricoles sont avant tout générées par l'activité de l'agriculteur. C'est en utilisant le matériel agricole ou le logiciel lors de son activité que les données sont générées. Par conséquent, ces données sont rattachées à l'activité d'exploitation du champ ou de la ferme.

Afin d'assurer un droit d'accès en toutes circonstances aux données brutes générées par l'activité agricole, l'entreprise de l'*AgTech* devrait être débitrice de l'obligation de mise à disposition de ces données en faveur du générateur. Cette obligation positive supposerait de mettre à disposition *via* une plateforme, un logiciel ou encore une application, les données brutes de l'exploitant agricole afin qu'il puisse y avoir accès à n'importe quel moment. Le droit d'accès se traduirait dans les contrats par une clause de mise à disposition des données brutes en faveur des agriculteurs, générateur des données, durant toute la durée de la relation contractuelle. Afin de mettre à disposition les données brutes des exploitations agricoles, les plateformes d'intermédiation auraient un rôle à jouer en créant des « ponts » entre les détenteurs des données brutes et ceux qui génèrent ces données grâce aux API. L'accès aux données par leur mise à disposition en faveur des exploitants agricoles est la prémisse de la maîtrise juridique sur les données qui doit passer notamment par la portabilité des données[549].

[548] Voir *infra*, n°622.
[549] Voir *infra*, n°598 et s.

178- **Future consécration réglementaire.** Le législateur européen s'est positionné sur cette question très récemment dans sa proposition de règlement sur les données (*Data Act*), du 23 février 2022[550]. Il a proposé de reconnaître un droit d'accès aux utilisateurs d'objets connectés ou de services liés. Il pose, notamment, comme principe que les utilisateurs ont le droit « *d'accéder aux données générées par l'utilisation du produit ou du service lié et à les utiliser* »[551]. Si l'accès n'est pas direct, une simple demande devrait suffire pour obtenir l'accès lorsque c'est techniquement possible. En échange, l'utilisateur n'aurait pas le droit de servir des données obtenues « *pour mettre au point un produit concurrençant le produit dont proviennent les données* »[552]. Aussi, la proposition de règlement engrange un changement de paradigme en instaurant un accès de principe pour l'utilisateur d'objets ou de services sur les données qu'il génère. Si jusqu'alors, l'utilisateur obtenait l'accès aux données au moyen d'un contrat, ce serait bientôt au détenteur de données d'obtenir l'autorisation de l'utilisateur dans le cadre d'un accord contractuel pour accéder aux « *données à caractère non personnel générées par l'utilisation du produit ou d'un service lié […]* »[553].

§2. *L'éventuelle consécration de l'accès aux données selon leur intérêt concurrentiel*

179- Les données sont de plus en plus au cœur des enjeux concurrentiels. La détention de certains jeux de données peut conférer un avantage concurrentiel conséquent pour l'entreprise qui les détient et engendrer des comportements anticoncurrentiels. Mme V. Bellon-Maurel[554], directrice de l'institut *#Digitag* à Montpellier, a exprimé ses inquiétudes à ce sujet en expliquant que « *de gros industriels ont la mainmise sur les données, ce qui peut créer des situations de monopoles et fausser le jeu de la concurrence* ». L'accès aux données agricoles est, donc, un nouvel enjeu du droit de la concurrence (**I**), plusieurs atteintes à l'accès aux données peuvent, ainsi, être relevées (**II**).

[550] Commission européenne, proposition de règlement du 23 fèvr. 2022 fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données — *Data Act*), COM (2022) 68 final, 2022/0047 (COD).
[551] Règlement sur les données, préc., art.4.
[552] *Ibid.*, art.4 § 4
[553] *Ibid.* art. 4 § 5.
[554] BELLON-MAUREL, V., « Le numérique est dans le pré », On n'arrête pas l'éco, *France Inter*, 29 févr. 2020.

I. L'accès aux données agricoles : le nouvel enjeu du droit de la concurrence

180- De nombreuses entreprises ont vu le jour ces dernières années surfant sur le phénomène du *Big Data* agricole dont l'objectif est notamment de fournir de nouveaux services aux agriculteurs. Selon le rapport « *Droit de la concurrence et données* » de l'Autorité de la concurrence du 10 mai 2016[555], « *la collecte et l'utilisation des données* » contribuent au pouvoir de marché en procurant un avantage concurrentiel aux entreprises et « *en particulier à celles qui sont mieux positionnées pour procéder à leur collecte massive* »[556]. Aussi, certains acteurs détiennent des données qu'ils n'exploitent pas nécessairement parce qu'ils ne savent ou ne peuvent pas encore les exploiter pour en tirer profit. Ils les conservent dans l'attente d'un usage potentiel futur, appelé « *valeur d'option des données* » par les économistes[557]. Les entreprises sont donc les seules à avoir accès aux données qu'elles obtiennent directement par le biais du matériel agricole utilisé par les exploitants agricoles. De cette façon, elles se créent un monopole sur les données qu'elles détiennent et courent le risque d'abuser de leur situation de position dominante sur le marché dans la mesure où la détention des données peut conférer à l'entreprise qui les détient un pouvoir de marché conséquent. Ainsi, un refus d'accès ou l'adoption d'une stratégie visant à s'approprier de manière excessive un gisement de données pourraient être constitutif d'un comportement anticoncurrentiel. Un certain nombre de ces comportements concernant directement les données, a été listé par l'Autorité de la concurrence.

En premier lieu, l'analyse concurrentielle d'un secteur nécessite l'identification du marché en cause (**A**). En second lieu, il faut déterminer la répression des atteintes aux données sur le marché des données agricoles (**B**).

A. L'identification du marché en cause

181- Afin d'identifier le marché en cause, il est nécessaire, avant tout, de le définir (**1**) pour ensuite envisager la détention des données comme source de pouvoir de marché (**2**).

[555] Aut. conc. et Bundeskartellamt, Avis, *Droit de la concurrence et données*, 10 mai 2016.
[556] *Ibid*, p. 29.
[557] CHIGNARD, S. et BENYAYER, L.-D., *Datanomics, Les nouveaux business models des données*, FYP, éd., 2015.

1. La définition du marché en cause

182- **Définition du marché en cause.** La jurisprudence en droit de la concurrence définit habituellement le marché en cause avant toute analyse du jeu concurrentiel. La première étape réside donc dans la définition de la notion même de marché. Celle-ci revêt en réalité deux acceptions. D'abord, dans une première acception, il peut s'agir de « *l'espace à l'intérieur duquel s'échangent les marchandises et les services de toute nature* ». Ensuite, dans une seconde acception, la notion de marché en cause peut englober « *le périmètre à l'intérieur duquel s'exerce la concurrence entre les entreprises* »[558]. C'est donc à partir du marché ainsi déterminé que l'Autorité de la concurrence va pouvoir analyser le jeu de la concurrence. C'est en ce sens que les juges du Tribunal de première instance des Communautés européennes ont retenu, dans un arrêt du 6 juillet 2000, que « *le cadre de l'application de marché en cause est une condition nécessaire et préalable du jugement porté sur un comportement prétendument anticoncurrentiel, puisque, avant d'établir l'existence d'un abus de position dominante, il faut établir l'existence d'une position dominante sur un marché donné, ce qui suppose que ce marché ait été préalablement délimité* »[559].

183- **Définition de marché de produits.** Le « *formulaire simplifié de notification d'une concentration conformément au règlement CE n°139/2004* » qui forme l'annexe II du règlement (CE) de la commission du 7 avril 2004 concernant la mise en œuvre du règlement (CE) n°139/2004 du Conseil relatif au contrôle des concentrations entre entreprises, donne la définition suivante du marché de produits : « *un marché de produits en cause comprend tous les produits et/ou services que le consommateur considère comme interchangeables ou substituables en raison de leurs caractéristiques, de leur prix et de l'usage auquel ils sont destinés. Un marché de produits en cause peut, dans certains cas, se composer de plusieurs produits et/ou services qui présentent des caractéristiques physiques ou techniques en grande partie identiques et sont interchangeables* »[560]. Ainsi, le marché en cause est celui dans lequel les partenaires ont le choix entre plusieurs opérateurs. Afin de déterminer si un marché existe, les spécialistes recherchent la substituabilité du produit en cause et la substituabilité

---

[558] DECOCQ A. et DECOCQ G., *Droit de la concurrence, droit interne et droit de l'Union européenne*, LGDJ, 7e éd., 2016, n°64, p. 93.

[559] TPICE 6 juill. 2000, aff. T-62/98, *Volkswagen AG c/Comm. CE* ; comm. IDOT L., *Rev. Eur*. 2000 n°10 p. 21 ; chron. VALLERY A. et LOUIS F., *Cah. Dr. eur*. 2000 n°5-6 p. 719 ; note POILLOT-PERUZZETTO S., *CCC* 2000 n°12 p. 15 ; chron. KRAMER P., *LGP* 2000 n°357 p. 50 ; note PIRETO C., *JDI* (Clunet) 2001 n°2 p. 656 ; chron. SUDRE F., *RTDH* 2001 n°47 p. 797 ; chron. BLAISE J.-B. et IDOT L., *RTDE* 2002 n°3 p. 555 ; comm. VALIGNY C., *RLC* 2005 n°5 p. 139, Cité in *ibid.*, n°65, p. 94.

[560] *Ibid.*, n°67, p. 97.

géographique. Dans le premier cas, l'idée est de rechercher l'interchangeabilité d'un produit sur un marché. Il s'agit de se demander, d'abord, si un produit est substituable du point de vue de l'utilisateur (substituabilité subjective) et ensuite selon les caractéristiques physiques du produit (substituabilité objective). Pour voir si un bien est subjectivement substituable, les autorités de la concurrence utilisent le « *test du monopoleur hypothétique* » qui revient à simuler un changement de prix sur un produit dans l'objectif de voir si les consommateurs s'en détournent, dans ce cas il est substituable. S'il ne s'en détourne pas, c'est que le produit n'est pas substituable. Concernant, la substituabilité géographique, il est question d'analyser si dans un secteur donné (mondial, national, régional ou local) le produit est substituable.

184- **Le marché des données agricoles.** Dans le domaine de l'agriculture numérique, le marché en cause est celui sur lequel les entreprises vont collecter des données agricoles par le biais d'objets connectés ou lorsqu'elles sont saisies dans les logiciels d'exploitation. Ces données sont susceptibles d'intéresser un grand nombre d'opérateurs sur différents marchés. Par exemple, les entreprises SMAG et ITK[561] collectent les données des exploitations et les traitent afin de fournir de l'aide à la décision aux agriculteurs. Elles sont donc positionnées sur le marché de la collecte et du traitement des données. D'autres sociétés sont plutôt positionnées sur le marché du partage des données, telles que WIUZ qui propose une plateforme agronomique de partage ouverte de données agricoles, ou Farmleap qui est une plateforme numérique fermée pour échanger des données dans des groupes d'agriculteurs afin de leur permettre de se comparer de manière anonyme. Aussi, les données géographiques pourraient intéresser des groupes d'agriculteurs positionnés dans le même secteur géographique et beaucoup moins ceux qui en sont éloignés. D'autres données auront de l'intérêt à plus grande échelle, notamment celles concernant les prix de revente par culture, par exemple.

2. La détention des données comme source de pouvoir de marché

185- **Définition.** Le pouvoir de marché peut être défini comme « *l'aptitude d'une entreprise à l'emporter sur ses concurrents ainsi qu'à contracter de manière rentable avec ses partenaires* »[562], ou encore, « *le pouvoir dont dispose une entreprise pour faire obstacle à une concurrence effective* »[563]. C'est dans l'arrêt *Hoffman-La Roche* du 13 février 1979[564] que les

[561] Voir *supra*, n°138.
[562] *Ibid.*, n°86, p. 123.
[563] MAINGUY, D. et DEPINCE, M., *Droit de la concurrence*, LexisNexis, 2e éd., 2015, n°327, p. 322.
[564] CJCE, 13 févr. 1979, aff. 85/76, *Hoffmann-La Roche & Co. AG c/ Comm.* CE : Rec. 461.

juges communautaires ont défini les « *facteurs de la position dominante, qui se transposent à celle de tout pouvoir de marché* »[565]. En premier lieu, le facteur principal est celui de la part de marché de l'entreprise sur le marché en cause. Il s'agit là d'un facteur quantitatif[566]. En second lieu, il existe, également, des facteurs qualitatifs, comme la « *capacité technologique* » et le « *réseau commercial* ». Il peut également s'agir d'aptitudes comme des aptitudes technologiques, industrielles, commerciales, ou encore financières et sociales[567].

186- **Avantages de la détention des données.** Comme le rappelle M. M. Bourgois, le fait pour une entreprise de détenir des données, qu'elles soient de nature qualitative comme les *Smart Data* ou quantitative avec les *Big Data*, lui confère de nombreux avantages. En effet, l'entreprise connaît mieux son écosystème, elle est plus en mesure de détecter d'éventuelles tendances, elle pilote sa stratégie, notamment en réduisant sa zone de risque, elle optimise la gestion de ses ressources internes et externes et tout ceci lui confère la possibilité de se lancer sur de nouveaux marchés[568]. Les données représentent, ainsi, un véritable pouvoir de marché pour l'entreprise qui les détient.

187- **Influences de la détention des données sur de nouveaux marchés.** Un marché biface ou multiface est défini par le Conseil d'État, comme « *un type de marché dont l'agencement entretient — voire nécessite — l'existence de deux clientèles différentes, mais interdépendantes en ce qui concerne les produits qui y sont échangés* »[569]**.** Les économistes J.-C. Rochet et J. Tirole ont développé la théorie des marchés multifaces en 2003[570]. Pour M. le Professeur C. Benavent, il s'agit avant tout « *[d'] un mécanisme propre à l'économie des plateformes* ». Ainsi, les « *firmes qui exploitent plusieurs versants du marché peuvent maximiser les profits, en acceptant un prix inférieur au coût marginal sur l'un des versants si le profit sur un autre est suffisant* »[571]. Dès lors que plusieurs groupes d'utilisateurs et de consommateurs opèrent sur un marché, il est dit « multiface »[572]. La Commission européenne a, dans ce sens, retenu qu'une plateforme en ligne correspond à « *une entreprise active sur des marchés bifaces ou multifaces, qui utilise internet pour permettre des interactions entre au moins deux groupes distincts, mais*

[565] DECOCQ A. et DECOCQ G., *Droit de la concurrence, droit interne et droit de l'Union européenne, op. cit*., n°87, p. 125.
[566] *Ibid*., n°88, p. 125.
[567] *Ibid*., n°93 et 94, p. 128.
[568] BOURGEOIS M., *Droit de la donnée, op. cit.*, n°1245, p. 279.
[569] CE, *Puissance publique et plateformes numériques : accompagner l'« ubérisation »*, EDCE, 29 sept. 2017.
[570] ROCHET, J.-C. et TIROLE, J., « Platform Competition in Two-sided Markets », *JEEA*, vol. 1, n°4, June 2003.
[571] BENAVENT C., *Plateformes, sites collaboratifs, marketplaces, réseaux sociaux…. Comment ils influencent nos choix*, FYP, 2016, p. 79.
[572] Aut. conc. et Bundeskartellamt, Avis, *Droit de la concurrence et données*, 10 mai 2016, p. 31.

interdépendants, d'utilisateurs, de façon à créer de la valeur pour au moins un des groupes »[573]. Les données peuvent avoir des effets sur un marché biface ou multiface, mais également la détention des données peut avoir des effets sur un marché connexe.

188. **Effets du *Big Data* sur les marchés multifaces.** En analysant le marché des données, il s'avère que lorsqu'elles procurent un avantage concurrentiel, cela peut conférer des effets sur un autre marché. D'abord, sur le premier marché, en amont, la donnée est collectée de manière gratuite (le plus souvent), en échange d'un service. Ensuite, ces données collectées seront commercialisées sur un second marché aval, qui sera cette fois-ci payant (le plus souvent). Elles prennent alors la forme de nouveaux services vendus auprès d'autres clients/consommateurs[574]. C'est ce qu'a, notamment, retenu l'autorité de la concurrence dans sa décision du 21 avril 2015, au sujet de Booking.com qui est « *un marché qui comprend deux faces, en mettant en relation deux catégories de clients distinctes : les hôteliers et les consommateurs de nuitées* »[575].

189. **Effets du *Big Data* sur les marchés connexes**. La connexité entre deux marchés permet de repérer les comportements sur un marché qui engendreraient des effets sur un second marché non dominé[576]. Aussi, lorsqu'une entreprise détient un pouvoir de marché et se retrouve en situation de domination, elle peut, par son comportement, « *emporter des pratiques illicites sur un marché connexe qu'elle ne domine pas* »[577]. Plusieurs critères ont été dégagés pour évaluer la connexité d'un marché. L'avocat général, M. Dámaso Ruiz-Jalamo Colomer a présenté ces critères dans ses conclusions du 27 juin 1996[578] : « *Les autorités compétentes [doivent] tenir compte des circonstances suivantes : la structure de la demande et de l'offre sur les marchés ; les caractéristiques des produits ; l'utilisation par l'entreprise dominante de son pouvoir sur le marché dominé pour pénétrer sur le marché connexe ; la part de marché de l'entreprise dominante sur le marché non dominé et l'étendue du contrôle du marché dominé par l'entreprise en question* ». Or, la collecte d'un grand nombre de données grâce au *Big Data* permet d'imaginer le potentiel que leur usage procure sur des marchés différents jusque-là cloisonnés. Ce potentiel permet, selon M. M. Bourgeois, « *d'y voir l'apparition d'une forme de*

---

[573] Commission européenne, *Consultation publique sur l'environnement réglementaire concernant les plateformes, les intermédiaires en ligne, les données et l'informatique en nuage, ainsi que l'économie collaborative*, 15 déc. 2015.
[574] BOURGEOIS M., *Droit de la donnée, op. cit.*, n°1247, p. 280.
[575] Aut. conc., déc. n°15-D-06, 21 avr. 2015, *Booking.com* ; note BEHAR-TOUCHAIS, M., *Rev. des contrats*, 2015, pp. 931-937 ; comm., SELINSKY, V., *RLC* 2015, pp. 28 à 31.
[576] BOURGEOIS M., *op. cit.*, n°1250, p. 281.
[577] MAINGUY D. et DEPINCE M., *Droit de la concurrence, op. cit.*, n°255, p. 322.
[578]CJCE 14 nov. 1996, *Tetra Pak c/ Commission*, aff. C-333/94 P : Rec. I. 5951 : note S., Y., *Gaz. Pal*., 1998, 184. p. 38 ; comm. KORAH V., *ECLR* 1997, n°3 pp. 98 à 192 ; concl. Av. gén. M. Damazo Ruiz-Jalamo Colomer, voir pt 57.

"connexité" entre ces marchés »[579]. L'affaire *Booking.com*[580] en est un bon exemple puisque la société touchait deux marchés connexes par le biais des données qu'elles détenaient, à la fois celui des clients qui souhaitaient réserver des nuitées dans des chambres d'hôtel et celui des annonceurs qui souhaitaient contracter avec booking.com en raison de sa bonne audience.

190- **Avantage concurrentiel**. La détention des données crée un véritable avantage concurrentiel. Les barrières imposées pour l'accès à ces données permettent à l'entreprise qui les détient de garder un avantage sur ses concurrents. C'est ce qu'a retenu l'Autorité de la concurrence dans son avis de 2016. Elle relève qu'il existe « *plusieurs affaires dans lesquelles les autorités de concurrence ont considéré que bien que les données soient non rivales, l'accès à celles-ci se faisait à un coût prohibitif, de telle sorte qu'y avoir accès était considéré comme un avantage concurrentiel significatif* »[581].

191- **Objet du marché.** Certains auteurs soutiennent que la donnée est devenue elle-même l'objet d'un marché. En effet, elle est, aujourd'hui, qualifiée de nouvel « or noir ». Il y a un véritable changement de paradigme, il ne s'agit plus de prélever certaines données dans un objectif précis, mais bien de prélever toutes les données possibles et imaginables pour ensuite voir ce qu'il est possible d'en faire. C'est à partir de ces gisements de données que les idées de traitements s'organisent. Aussi, de nouveaux métiers apparaissent pour le traitement, l'analyse de ces données, mais également des courtiers de données ou *Data broker* dont le cœur de métier est d'acheter, d'agréger et de revendre des données. Il s'agit donc d'un produit à part entière qui peut faire l'objet de commercialisation. Certains auteurs, sur ces constatations, évoquent même l'idée de créer une fiscalité sur les données[582]. M. M. Bourgeois s'est exercé dans la délimitation du marché de la donnée[583]. Ainsi, c'est bien sur l'interchangeabilité du produit qu'il faut se référer pour opérer le travail de délimitation du marché en cause. Comme il a été vu plus haut, il faut rechercher la substituabilité du produit et la substituabilité géographique. En ce qui concerne la substituabilité du produit, il est nécessaire de rechercher la substituabilité de la demande en analysant le côté objectif, autrement dit celui de la vente, puis le côté subjectif, autrement dit celui des consommateurs. En effet, au sujet de la **substituabilité objective**, les données peuvent entrer dans différentes catégories qui s'avèrent non substituables. Les données géographiques ne répondent pas aux mêmes besoins que les données de rendements par

[579] BOURGEOIS M., *op. cit.*, n°1259, p. 284.
[580] Aut. conc., déc. n°15-D-06, 21 avr. 2015, *Booking.com*, préc.
[581] Aut. conc. et Bundeskartellamt, *Droit de la concurrence et données*, *op. cit.*, p. 43.
[582] BINCTIN N., *Droit de la propriété intellectuelle : droit d'auteur, brevet, droits voisins, marque, dessins et modèles*, LGDJ, 4e éd., 2016, p. 296.
[583] BOURGEOIS M., *op. cit.*, n°1301 et s, pp. 295 et s.

exemple. Pour des catégories plus larges et, comme le relève M. M. Bourgeois, les différents niveaux de protection des données délimitent des catégories différentes. Le marché ne sera pas le même selon qu'il s'agit de données nominatives, de données pseudonymées, ou encore de données chiffrées. Ensuite, au sujet de la **substituabilité subjective**, il s'agit de s'interroger sur l'usage des données. Des marchés différents de données voient le jour selon le cœur de métier de ceux qui les utilisent. Aussi, les données agricoles n'intéresseront probablement pas les réseaux sociaux ou les plateformes de mise en ligne pour l'échange de services entre particuliers. Dans le sens inverse, les données des utilisateurs des réseaux sociaux n'intéresseront pas les entreprises créant des objets connectés à destination des agriculteurs. En appliquant le test du monopoleur hypothétique consistant à simuler une variation du prix d'un produit sur un marché, il est possible de voir si les consommateurs s'en détournent ou non. En cas de détournement, il y a substituabilité, et dans le cas contraire, le produit est leader, il n'y a pas de substituabilité. Il s'avère que généralement la collecte des données est gratuite, c'est le traitement et l'usage qui en est fait par la suite qui est payant. De ce constat, ce n'est pas le prix qui doit être déterminant, mais d'autres critères. Par exemple, le respect de la vie privée peut être un critère déterminant pour les utilisateurs des réseaux sociaux qui se détourneront de ceux qui ne respectent pas la réglementation de l'Union européenne. Ou encore, dans le cadre agricole, les agriculteurs pourraient se détourner des entreprises qui ne leur fournissent pas de garanties suffisantes sur les droits qu'ils détiennent sur les données collectées sur leurs champs. Ou bien encore, dans le cas où l'entreprise de traitement des données agricoles échangerait les données non personnelles avec d'autres entreprises sans l'accord préalable de l'exploitant agricole. Du côté de l'offre de données, il s'agit « *d'une offre substituable* » correspondant à « *une offre "réorientable", c'est-à-dire vers laquelle un fournisseur peut réorienter sa production rapidement et moyennant de faibles coûts* »[584]. Enfin, en ce qui concerne le marché géographique, il s'agit du « *territoire sur lequel les entreprises offrent et demandent les biens et les services en cause, sur lequel les conditions de concurrence sont suffisamment homogènes et qui peut être distingué de zones géographiques voisines parce qu'en particulier, les conditions de concurrence y diffèrent de manière appréciable* »[585]. Aussi, le marché géographique peut être mondial, régional, national ou local. Il semble néanmoins difficile d'admettre une position dominante pour les acteurs de l'agriculture numérique. En effet, de très nombreux acteurs se positionnent sur le marché et utilisent leur propre technologie pour collecter ou obtenir les données dont ils ont besoin afin de développer des services et des

[584] *Ibid.*
[585] DECOCQ A. et DECOCQ G., *Droit de la concurrence, droit interne et droit de l'Union Européenne, op. cit.*

technologies utiles pour les agriculteurs. Par exemple, les sociétés *SMAG*, *ITK* ou encore *Ekylibre* proposent des services similaires, mais la concurrence se fait plutôt sur les technologies et les services proposés selon les besoins des exploitants agricoles.

B. La répression des atteintes à l'accès aux données sur le marché des données agricoles

192- Les données ont un véritable poids en droit de la concurrence. Des marchés se forment autour des données et elles peuvent offrir un pouvoir de marché important aux entreprises qui les détiennent. Ceci peut influencer les comportements de ces entreprises sur d'autres marchés. Aussi, il semblerait que les données aient de plus en plus d'influence dans l'analyse concurrentielle. L'autorité française de la concurrence et son homologue allemand ont, ainsi, relevé les comportements anticoncurrentiels liés aux données dans leur avis commun du 10 mai 2016[586]. Cette étude s'est faite au travers des fusions-acquisitions et des pratiques d'éviction. Il faut dans un premier temps envisager les comportements anticoncurrentiels quant à l'accès aux données (**1**) pour dans un second temps s'intéresser aux sanctions des atteintes à la concurrence (**2**).

1. Les comportements anticoncurrentiels quant à l'accès aux données

193- Définitions. Les articles L. 430-1 du Code de commerce et 3 du règlement CE sur les concentrations[587] englobent les deux cas de concentrations que sont les fusions et les acquisitions. Les concentrations sont des opérations « *de fusion ou de cession de contrôle, au sens large, c'est-à-dire comme une prise de participation en capital, quelle qu'en soit la forme, acquisition de droits sociaux par contrat unique, par OPA ou OPE, augmentation de capital… mais aussi de façon indirecte par l'acquisition d'éléments d'actif* »[588]. Mais également lors de la « *constitution d'une filiale commune* ».

194- Fusions. Pour commencer, il faut déterminer ce que sont les fusions. Il s'agit d'abord d'une opération économique[589]. Il peut être question d'une fusion par création d'une entité nouvelle

---

[586] Aut. conc. et Bundeskartellamt, *Droit de la concurrence et données*, *op. cit.*, pp. 18 et s.
[587] Règl. n°139/2004 relatif au contrôle de concentration entre entreprises (« le règlement CE sur les concentrations ») : *JOUE* L 24/1, 29 janv. 2004, art. 3.
[588] MAINGUY D. et DEPINCE M., *Droit de la concurrence*, *op. cit.*, n°381, p. 353.
[589] DECOCQ A. et DECOCQ G., *Droit de la concurrence, droit interne et droit de l'Union européenne, op. cit.*, n°133, p. 173 ; La communication du 21 février 2009 énonce : « *(9) au sens de l'article 3, paragraphe 1, point &),*

ou par absorption. Dans le premier cas, « *une personne morale nouvelle [apparaît], à laquelle sont transférées les entreprises qui appartenaient à des entités anciennes, lesquelles disparaissent alors comme personnes morales* »[590]. Dans le second cas, « *l'une des entités disparait après avoir apporté son patrimoine à l'autre, qui survit seule comme personne morale* »[591]. Mais également lorsque cette opération entraîne la création d'une unité économique.

195- **Acquisitions.** Les acquisitions sont quant à elles des prises de contrôle. Pour cela, il doit y avoir au moins une entreprise du côté de l'acquéreur du contrôle, un contrôle effectif et un procédé d'acquisition dudit contrôle[592]. Il s'agit de « *la possibilité d'exercer une influence déterminante sur l'activité d'une autre entreprise qu'un droit ou une situation juridique ouvre à une personne ou à une autre entreprise* »[593]. Les procédés d'acquisitions du contrôle se font par, l'acquisition, directe ou indirecte, que ce soit par prise de participations au capital ou par l'achat d'éléments actifs (contrat ou tout autre moyen) ou par le contrôle de l'ensemble ou de parties d'une ou de plusieurs autres entreprises[594].

196- **Influence des données dans le contrôle des concentrations.** Parfois, les entreprises acquièrent d'autres entreprises ou fusionnent dans l'objectif d'obtenir de grands jeux de données. Cette pratique a d'ailleurs bien augmenté selon l'OCDE (2015)[595]. Elle va avoir un réel effet dès lors qu'il s'agit de bases de données importantes. Dans le cas où la concentration conduirait à l'obtention de jeux de données auxquels les concurrents ne pourraient pas avoir accès, alors il y a un risque d'atteinte à la concurrence. Cela pourrait également « *générer des gains d'efficience* ». Cette question, bien que pour l'heure prospective, a le mérite d'être évoquée ici à propos des données agricoles. Un acteur économique majeur sur le marché des données issues des exploitations agricoles pourrait collecter des masses de données importantes *via* les objets connectés. Or, « *ces données générées par le comportement des utilisateurs, source précieuse*

---

du règlement sur les concentrations, une concentration est réalisée lorsque deux ou plusieurs entreprises indépendantes fusionnent en créant une nouvelle entreprise et disparaissent en tant que personnes morales distinctes. Une fusion peut également avoir lieu lorsqu'une entreprise est absorbée par une autre et perd la personnalité morale ».

[590] DECOCQ, A. et DECOCQ, G., *ibid.*, n°135, p. 174.

[591] *Ibid.*, n°136, p. 175.

[592] Selon le règlement CE sur les concentrations, article 3 paragraphe 2, « *le contrôle découle des droits, contrats ou autres moyens qui confèrent, seuls ou conjointement et compte tenu des circonstances, de fait ou de droit, la possibilité d'exercer une influence déterminante sur l'activité d'une entreprise, et notamment : a) des droits de propriété ou de jouissance sur tout ou partie des biens d'une entreprise ; b) des droits ou des contrats qui confèrent une influence déterminante sur la composition, les délibérations ou les décisions des organes d'une entreprise* ». L'article L. 430-1 du Code de commerce, §3 reprend ce texte.

[593] DECOCQ A. et DECOCQ G., *op. cit*., n°142, p. 179.

[594] Règl. CE sur les concentrations, art. 3 et C. com., art. L. 430-1, §I, 2e.

[595] OECD, « Data-driven Innovation : Big Data for Growth and Well-Being », *OECD Publishing*, Paris, 2015.

d'innovation, peuvent, si elles sont concentrées entre les mains de ce seul acteur, entraver la libre concurrence en empêchant tout tiers de rivaliser face à ce capital informationnel »[596]. Aussi, en se créant des monopoles sur les données que les entreprises détiennent au moyen de l'Internet des objets (*Internet of Things*), *« bien souvent à l'occasion et sous le prétexte d'un service distinct, exploitant le caractère "biface" propre au marché numérique »*[597], ces entreprises peuvent contrôler l'ouverture de l'accès à leurs concurrents en situation de domination. La complexité et les coûts du droit de la concurrence rendent dissuasive toute action en droit de la concurrence pour certains acteurs[598].

197- **Contrôle des concentrations.** L'ensemble des opérations issues des concentrations doivent être « *notifiées aux autorités de concurrence, qui procèdent à un bilan économique et concurrentiel, au regard du marché pertinent, pour refuser ou autoriser (le cas échéant sous réserve du respect de certains engagements) l'opération envisagée* »[599]. Le règlement CE sur les concentrations et le Code du commerce offrent à l'autorité de la concurrence « *le pouvoir de s'opposer aux concentrations qui risquent de porter atteinte à la concurrence, "notamment" par la création ou le renforcement d'une position dominante* »[600]. Elle apprécie, ainsi, le bilan économique de l'opération et au regard des prohibitions de comportements anticoncurrentiels. Pour ce faire, l'autorité de la concurrence prend en compte, entre autres, les risques que représente la concentration par rapport à l'agrégation d'un très grand nombre de données.

198- **Critères jurisprudentiels.** La jurisprudence a déterminé trois critères selon lesquels une situation de concentration ne porte pas atteinte à la concurrence. Tout d'abord, le premier critère consiste en l'existence de concurrents crédibles. Dans deux affaires, la Commission européenne a eu l'occasion de se prononcer sur cette question. D'abord, dans l'affaire *Google/DoubleClick* du 11 mars 2008[601], elle a décidé que même si la fusion des sociétés *Google* et *DoubleClick* engendrait un accroissement des données, cet accroissement ne représentait pas une atteinte à la concurrence. Elle justifie cette décision du fait que des sociétés concurrentes « crédibles » (Microsoft, Yahoo, AOL) avaient déjà accès à ces données. Dans la seconde affaire,

---

[596] BOURGEOIS, M. et MOINE, M., « Internet des objets (IOT) : quand l'inerte s'anime », *Rev. pratique de la prospective et de l'innovation n°2*, Oct. 2019, doss. 15.
[597] *Ibid.*
[598] *Ibid.*
[599] BOURGEOIS M., *Droit des données, op. cit.*, n°1274, p. 288.
[600] DECOCQ A. et DECOCQ G., *op. cit*., n°159, p. 195 ; TPICE, 25 mars 1999, aff. T-102/96, *Gencor Ltd/Comm. CE* : Rec. II. p. 753 ; note PRIETO C., 2005, *JDI* 2005 n°2 p. 446 ; chron. PILCZER J.-S., *Cah. Dr. eur.* 2014 n°3 p. 597 ; IDOT L., *Eur.* 1999, p. 7, pt. 163 : « *Analyse prospective du marché en cause* ».
[601] Commission européenne, déc., 11 mars 2008, aff. COMP/M.4731, *Google c/ DoubleClick*, C(2008) 927 final ; note PHILIPPE J. et TRABUCCHI M., *LGP* 2010 n°281 p. 10 ; comm. BURE F., LAPREVOTE F.-C et DUPREY J.-S, *RLC* 2008 n°16 p. 11.

microsoft/yahoo/search business du 18 février 2010[602], la Commission allait plus loin en retenant que la fusion des sociétés Microsoft et Yahoo pouvait même avoir un effet bénéfique sur la concurrence en exerçant une pression concurrentielle sur Google. Pour confirmer cette décision, il a été retenu, dans l'affaire *telefónica/vodafone/everything everywhere* du 4 septembre 2012[603], que la fusion de ces sociétés engendrait certes la possibilité de collecter une grande variété d'informations relatives aux consommateurs. Mais cette concentration ne portait pas pour autant atteinte à la concurrence puisque d'autres acteurs disposaient des mêmes capacités. Ensuite, le second critère repose sur le caractère non essentiel des données en cause. Cela a été le cas dans l'affaire *EDF/Dalkia* en France du 25 juin 2014[604], puisque les informations sur la consommation d'électricité que détiennent EDF et Dalkia ne sont pas « essentielles » pour leurs concurrents pour la fourniture de leurs services. Enfin, le troisième critère repose sur la dynamique du marché en cause. C'est ce qui a été retenu dans l'affaire *Facebook/WhatsApp* du 3 octobre 2014[605]. En effet, la fusion de ces deux entreprises permettait le rapprochement d'un grand nombre de données d'utilisateurs. Cependant, toutes les données des utilisateurs ne devaient pas être sous le contrôle exclusif de Facebook. De plus, le marché des applications de communication en ligne est très dynamique et de nouveaux entrants peuvent pénétrer le marché rapidement et menacer les opérateurs dominants. Également, les utilisateurs sont de plus en plus sensibles à la protection de leur vie privée, ce qui fait que cette fusion pouvait les inquiéter et par conséquent, ils pouvaient décider de changer de moyens de communication. C'est ce qui s'est d'ailleurs produit en Allemagne. Dans ce cas, la concentration ne porte pas atteinte à la concurrence. Néanmoins, M. M. Bourgeois relève que « *la quantité de données détenues par les acteurs historiques peuvent constituer une barrière à l'entrée pour les nouveaux entrants, donc il n'est pas certain que l'argument invoqué par la commission de la dynamique de marché soit encore valable aujourd'hui* »[606].

199- **Effets des concentrations sur la concurrence.** Parfois des concentrations peuvent avoir un effet négatif sur la concurrence. Aussi, les juges peuvent ordonner aux sociétés opérant une concentration de favoriser le jeu de la concurrence. C'est le cas notamment lorsque les données, issues d'une base détenue par deux sociétés ayant fusionné, sont substituables (qualité et

[602] Commission européenne, 18 févr. 2010, aff. COMP/M.5727, *Microsoft c/ Yahoo! Search business*, C(2010) 1077 ; comm. HULL D. et THEOPHILE D., *Concurrences* 2010 n°3 p. 121; note BURE (de) F., *RLC* 2010 n°24 p. 12 ; note PHILIPPE J. et TRABUCCHI M., *LGP* 2010 n°281 p. 10.
[603] Commission européenne, 4 sept. 2012, aff. COMP/M.6314, *Telefonica/Vodafone/Everything EveryWhere*, C(2012) 6063 final ; note BILLARD O., *Concurrences* 2013 n°2 p. 111.
[604] Commission européenne, 25 juin 2014, aff. COMP/M.7137, *EDF c/ Dalkia en France*, C(2014) 4438 final.
[605] Commission européenne, 3 oct. 2014 aff. COMP/M.7217, *Facebook/Whatsapp*, C(2014) 7239 final ; note VERNEY C., *RLC*, 2015, n°42, p. 24.
[606] BOURGEOIS M., *Droit de la donnée*, *op. cit.*, n°1282, p. 291.

contenu) et n'ont pas d'équivalents sur le marché[607]. Mais aussi, lorsque deux sociétés ayant des monopoles légaux ont fusionné pour fournir de nouveaux services et détiennent des données complètes de consommation d'électricité et de gaz[608]. Les entreprises lors d'une fusion-acquisition peuvent donc se rendre coupable d'une atteinte au libre jeu de la concurrence. Parfois encore, les entreprises peuvent directement écarter leurs concurrents par le moyen de pratiques d'éviction. L'éviction d'un concurrent a pour cause l'exploitation abusive d'une position dominante. Il peut y avoir un double effet de la transparence du marché sur le jeu de la concurrence.

200- **Abus d'une position dominante.** Les comportements d'éviction consistent en « *l'exploitation abusive d'une position dominante, lorsqu'elle tend à l'éviction des concurrents, en visant à réduire leur part de marché, à les empêcher de progresser, voire à les éliminer complètement d'un marché ou de leur en fermer l'accès* »[609]. Celle-ci peut être directe ou indirecte, « *directe, elle consiste à neutraliser les concurrents ; indirecte à accaparer les relations avec les clients ou les fournisseurs* »[610]. Il s'agit pour une société en situation de position dominante d'opérer un blocus sur le marché sur lequel « *des concurrents actuels ou potentiels opèrent ou veulent opérer* »[611]. L'avis de l'autorité de la concurrence de 2016 relève plusieurs comportements visant cet effet. D'abord, le refus d'accès à des données peut traduire un comportement anticoncurrentiel. En effet, les juges ont déjà eu l'occasion de condamner des sociétés qui ont refusé l'accès à des données[612]. Pour cela, il faut démontrer que les données possédées par

---

[607] Commission européenne, 19 févr. 2008, aff. M. 4726, aff. *Thompson corporation/Reuters Group*, SG-Greffe(2008) D/200711; comm. GIRGENSON I. et BURE (de) F., *RLC* 2008 n°17 p. 13.

[608] Aut. Conc., déc. n°12-DCC-20, 7 févr. 2012, *Enerest/Électricité de Strasbourg ;* comm. BOSCO D., *CCC*, 2012, n°8, p. 10.

[609] DECOCQ A. et DECOCQ G., *op. cit.*, n°281, p. 346.

[610] *Ibid.*

[611] *Ibid.*, n°282, p. 346.

[612]CJUE, 26 nov. 1998, aff. C-7/97, *Bronner GmbH & Co KG c/ Mediaprint Zeitung* ; *Rec.* I. 7791 ; obs. POILLOT-PERUZZETTO S., *RTD com* 1999 p. 798 ; chron., BLAISE J.-B et IDOT L., *RTD eur.* 1999 p. 271 ; note *Journal du droit international* 1999 n°2 p. 593 ; comm. BERGMAN M., *ECLR* 2000 n°2 p. 59 ; prat. HAUTBOURG S. et QUESSON S., *Décideurs Juridiques et Financiers* 2004 n°56 p. 64 ; pan. CHAGNY M., *Journal du droit internation* 2019 n°1 p. 550 ; note BORSCO D., *CCC* 2021 n°5 p. 42 ; TPIUE, 17 sept. 2007, aff. T-201/04, *Microsoft* ; obs. CHEVRIER E., *AJ.* 2007 p. 2303 ; EDITO ROME F., *Eur.* 2007 p. 2521 ; obs. POLLAUD-DULIAN F., *RTD com.* 2007 p. 715 ; Prat. ROBIN C. et SELINSKY V., *RLC* 2008 n°14 p. 26 ; note GUNTHER J.-P *RLC* 2008 n°14 p. 169 ; note BENABOU V.-L., *PI* 2008 n°26 p. 122 ; note CHALTIEL F., BERR C., FRANCQ S. et PRIETO C., *Journal du droit international* 2008 n°2 p. 632 ; note PHILIPPE J. et JANSSENS T., *LGP* 2008 n°9 p. 17 ; LUBY M. et POILLOT-PERUZZETTO S., *JCP G* 2008 n°5 p. 20 ; note SCHMIDT-SZALEWSKI J., *PI* 2008 n°3 p. 41 ; note BEHAR-TOUCHAIS M., *CCC* 2008 n°3 p. 8 ; note DECOCQ G., *JCP E* 2008 n°10 p. 18 ; FOUQUET T., SLADIC J. et VANHAM É, *Eur.* 2008 n°148 p. 114 ; act. SELINSKY V., *RLC* 2008 n°15 p. 131 ; chron. PRIETO C., *RDC* 2008 n°3 p. 811 ; chron. LUBY M. et POILLOT-PERUZZETTO S., *JCP G* 2008 n°27 p. 28 ; pan. FERRIER D., *D.S.* 2008 n°31 p. 2193 ; comm. CARDON M., *RLC* 2008 n°17 p. 142 ; comm. Art J.-Y., *RLC* 2008 n°17 p. 173 ; comm. NOURISSAT C., *RLC* 2008 n°17 p. 176; obs. FERRIER D., *D.* 2008 p. 2193 ; chron. SARDAIN F., *JCP E* 2009 n°5 p. 28 ; chron. BACCICHETTI E. et BONNET Ph., *JCP E* 2009 n°46 p. 18 ; CJUE, 29 avr. 2004, aff. C-418/01, *IMS Health GmbH & co. OHG* ; *Rec.* p. I-5039 ; obs. KAMINA P., *PI,* 2004, n°6, p. 29 ; note IDOT L., *Eur.* 2004, n°6, p. 27 ; comm. CARON C., *CCC,* 2004, n°6, p. 28 ; Pan. BOULET PATIN A.-L., *Lexbase Hebdo,* 2004, n°126 ; note BENABOU V.-L., *PI,* 2004,

l'intéressé sont véritablement uniques et que son concurrent ne peut les obtenir autrement afin de fournir ses services. Ensuite, dès lors qu'une entreprise refuse de manière discriminatoire l'accès à ses données, alors il peut s'agir d'une atteinte à la concurrence. C'est ce qu'a retenu l'Autorité de la concurrence dans une décision du 8 juillet 2014 dans l'affaire *Cegedim/Euris* : le fait pour la société Cegedim de refuser la vente de sa base de données à certains utilisateurs d'un logiciel commercialisé par la société Euris constituait un abus de position dominante[613]. Également, parfois, l'abus de position dominante peut passer par la conclusion de contrats. Dans ce cas, les concurrents concluent des contrats d'exclusivité afin d'évincer d'autres concurrents, notamment lorsque ces entreprises sont dominantes sur le marché. Par ces contrats, les entreprises rivales ne peuvent accéder aux données de tierces parties « *au moyen d'exclusivités avec les prestataires les fournissant, ou en rendant plus difficile l'adoption par les consommateurs de leurs technologies ou l'accès à leurs plateformes* »[614]. C'est notamment ce qui s'était produit pour la société Google qui avait conclu une série de contrats exclusifs dans le marché de la publicité liée aux recherches. Ce contrat avait pour but d'empêcher ses concurrents de contester sa position[615]. Enfin, s'agissant des ventes liées et l'utilisation croisée des ensembles de données, l'utilisation des données pour impacter un marché connexe peut être sanctionnée comme une atteinte à la concurrence. En effet, l'Autorité de la concurrence dans un avis du 14 juin 2010 a retenu que : « *l'utilisation croisée des bases de clientèle est une pratique courante. Elle peut par exemple permettre à une entreprise présente sur un marché de pénétrer plus facilement un nouveau marché à l'aide des informations qu'elle détient sur ses clients. Dès lors qu'elle permet en général de dégager des gains d'efficacité, en réduisant le coût d'acquisition des nouveaux clients, cette pratique bénéficie en principe à la concurrence et aux consommateurs* »[616].

---

n°12, p. 821 ; note BONET G., *RTD eur*., 2004, p. 691 ; Prat. HAUTBOURG S. et QUESSON S., *DJF*, 2004, n°56, p. 64 ; ét. PEYRE J., *RLC*, 2004, n°1, p. 26 ; chron., ARHEL P., *LPA*, 2004, n°143, p. 17 ; note SARDAIN F., 2004, *D.*S., n°32, p. 2366 ; pan. RESPAUD J.-L., *Cah. Dr. entr*., 2004, n°4, p. 39 ; comm. PEYRE J., *RLC*, 2004, n°1, p. 26 ; note POILLOT-PERUZZETTO S., *CCC*, 2004, p. 19 ; chron. SARDAIN F., *JCP E*, 2004, n°49, p. 1927 ; ét. SARDAIN F., *D.*, 2004, n°32, p. 2366 ; Prat. HAUTBOURG S. et QUESSION S., *DJF*, 20056, n°61, p. 94 ; comm. SCHMIDT-SZALEWSKI J., *PI*, 2005, n°3, p. 36 ; pan. CORDIER-FERON L., *LGP*, n°135, p. 34 ; obs. LEMARCHAND, *Expertises*, 2002, n°258, p. 139.

[613]Aut. conc., déc. n°14-D-06, 8 juill. 2014 relative à des pratiques mises en œuvre par la société Cegedim dans le secteur des bases de données d'information médicales : *AJCA*, 2014 ; MARTY F., *concurrences*, 2014, n°4, p. 135.

[614] Aut. conc. et Bundeskartellamt, *Droit de la concurrence et données*, *op. cit.*, 2016, p. 22.

[615]CJUE, Trib., 10 nov. 2021, aff. T. 612/17, *Google LLC, Alphabet, Inc c/ Comm. UE (Google shopping)* ; comm. MASMI-DAZI F., *D.* act., 2021 ; comm. BERLEMONT J., *ADD*, 2021 ; RONZANO A., *Concurrences*. 2022 n°1.

[616] Aut. Conc. avis n°10-A-13, 14 juin 2010, relatif à l'utilisation croisée des bases de clientèle : chron. TRAN THIET J.-P., *concurrences* 2010 n°3 p. 164 ; pan. ACHILLEAS P., *CCE* 2011 n°2 p. 18 ; note FRESHFIELDS BRUCKHAUS DERINGER *LLP*, *LGP* 2011 n°42 p. 30 ; pan. *Id.*, pt. 192.

201- **Effets négatifs de la transparence du marché.** La transparence du marché peut encourager les entreprises à s'accorder en fonction de l'analyse des données, ce qui caractérise un risque de collusion. C'est dans ce sens que l'utilisation des algorithmes permet aux entreprises d'anticiper les variations de prix et fausser le jeu de la concurrence.

202- **Risques de collusion.** La transparence du marché à un double effet, il peut, côté pile, faciliter l'entrée dans un marché à de nouveaux acteurs du fait de la facilité à accéder aux informations nécessaires. Côté face, les entreprises historiques peuvent utiliser l'ensemble de leurs informations pour, au contraire, limiter l'accès aux nouveaux concurrents. Il peut y avoir collusion tacite ou explicite entre plusieurs sociétés en devançant, par l'analyse des données, le jeu de la concurrence.

203- **Anticipation des variations de prix.** L'utilisation des algorithmes, par exemple, permet d'anticiper les variations des prix et « *des concurrents peuvent plus facilement mettre en œuvre un équilibre tarifaire supra-concurrentiel durable* »[617]. Par exemple, c'est ce qui a été retenu dans l'affaire *Topkins*[618], un vendeur de posters sur Amazon Market Place utilisait un algorithme de prix avec ses concurrents leur permettant de s'ajuster automatiquement à tout facteur qui conduisait à des différences entre eux.

204- **Effets sur la concurrence.** Les algorithmes tarifaires, même en l'absence de collusion horizontale, peuvent « *porter atteinte à la concurrence en réduisant les incertitudes et les biais comportementaux qui sont favorables à la concurrence par les prix* »[619]. Mais aussi, « *en intégrant dans leurs mécanismes de fixation des prix les réactions des concurrents pouvant être déduites des données collectées au cours des expériences passées de variations de prix* »[620]. Néanmoins, la transparence du marché étant bénéfique pour le consommateur et les pratiques n'aboutissant pas obligatoirement à une collusion, il serait « *difficile d'engager des poursuites à l'encontre de telles pratiques* »[621]. Cependant, dans le cas où les données ne seraient ni accessibles ni reproductibles par ses concurrents, il y aurait alors un risque d'éviction. Notamment « *lorsque les informations ont été obtenues dans la situation particulière d'un monopole de fait ou dans le cadre de l'exercice d'une mission de service public* »[622]. C'est dans ce cadre que GDF Suez a été contrainte par l'Autorité de la concurrence française de fournir un

[617] Aut. conc. et Bundeskartellamt, *op. cit.*, p. 16.
[618] Department of justice, *Former E-Commerce Executive Charged with Price Fixing in the Antitrust Division's First Online Marketplace Prosecution*, United States of America c/ David Topkins, 6 avr. 2015.
[619] Aut. conc. et Bundeskartellamt, *op. cit.*, p. 17.
[620] *Ibid.*
[621] *Ibid.*
[622] Aut. Conc. avis n°10-A-13, 14 juin 2010, préc., pt. 193.

accès à certaines de ses données collectées en tant que fournisseur de gaz dans le cadre d'offres réglementées à ses concurrents[623]. En 2017, la société Engie a été condamnée à une amende de 100 millions d'euros pour s'être servie de « *sa base de données relatives aux clients exigibles aux tarifs réglementés de vente dont elle disposait en sa qualité de fournisseur de gaz de ses infrastructures commerciales dédiées au tarif réglementé de vente en vue de la commercialisation de ses offres de fourniture de gaz et d'électricité à prix de marché à l'égard de la clientèle résidentielle et non résidentielle (petits clients), en utilisant des avantages qui n'étaient pas reproductibles par ses concurrents* »[624].

2. Les sanctions des atteintes à la concurrence

205- Au niveau national, l'Autorité de la concurrence est compétente pour sanctionner les entreprises coupables d'une atteinte à la concurrence. Au niveau européen, il s'agit de la Commission européenne. Les autorités de concurrence peuvent ordonner des mesures conservatoires et tout un panel de sanctions comme « *des injonctions destinées à ordonner aux parties intéressées "de mettre fin à ses préoccupations de concurrence"* »[625]. Mais aussi, des sanctions pécuniaires dont le montant maximal est fixé à 10 % du chiffre d'affaires mondial aux termes des articles L. 464-2 du Code de commerce et 5 et 7 du Règlement n°1/2003. Néanmoins, dans le cas où les ententes et les concentrations permettraient d'améliorer les services, il pourrait y avoir exonération[626].

En ce qui concerne les concentrations, la peine pécuniaire peut aller jusqu'à 5 % du chiffre d'affaires mondial au titre des articles L. 430-8 du Code de commerce et 14, §2, a) du Règlement n°139/2004. Les autorités de concurrence prennent en compte les « *gains d'efficience* » afin « *[d'] apprécier le caractère compatible — ou non — d'une opération* »[627]. C'est ce qui a été retenu notamment dans la décision *Tomtom/Tele Atlas*, au sujet du rachat par Tomtom, fabricant d'appareils de navigation portables et fournisseur de logiciel de navigation, de la société Tele Atlas, fournisseur de bases de données de cartographies numériques pour la navigation. La Commission a retenu que la concentration n'entravait pas de manière

---

[623] Aut. conc., déc. 14-MC-02, 9 sept. 2014, *GDF/Suez* ; comm. LEMAIRE C. et NAUDIN S., *Concurrences* 2014 n°4 p. 213 ; comm. GUILLAUME E. et DABOUSSY S., *Concurrences* 2014 n°4 p. 223 ; obs. J.-L. FOURGOUX *AJCA* 2014 p. 340.
[624] Aut. conc., déc. n°17-D-06, 21 mars 2017, *Engie SA* ; Ét. IDOUX P., NICINSKI S. et GLASER E., *AJDA*, 2017, n°21, p. 1211.
[625] MAINGUY, D. et DEPINCE, M., *Droit de la concurrence*, *op. cit.*, n°367, p. 339.
[626] BOURGEOIS, M., *Droit des données*, *op. cit*, n°1299, p. 295.
[627] *Ibid.*, n°1300, p. 295.

significative la concurrence, du fait qu'il existe d'autres concurrents sur le marché, tels que la société Navteq. Mais ce qui est notable, c'est qu'elle a aussi retenu que la transaction permettra de réaliser des gains d'efficience puisqu'elle « *permettra d'offrir "de meilleure carte — plus vite", comme l'ont suggéré les parties, que ce qui pourrait être réalisé par des contrats en l'absence de fusion et que donc ces gains d'efficacité sont, du moins partiellement, spécifiques à une fusion* »[628]. L'abus d'une position dominante passe donc par différente pratique visant à empêcher les concurrents d'accéder aux jeux de données dont ils auraient besoin pour développer leurs propres services.

II. La théorie des infrastructures essentielles au soutien des politiques de partage

206- Afin de réguler le marché en cause, l'accès à certaines données essentielles peut être exigé (**A**). Néanmoins, cet accès exceptionnel comporte des limites (**B**).

A. La régulation du marché en cause par le droit d'accès aux données essentielles

207- Si la question de la reconnaissance des données comme facilités essentielles a pu se poser (**1**), c'est finalement la jurisprudence qui l'a reconnue (**2**).

1. Les données comme facilités essentielles

208- **Définition.** La théorie des facilités essentielles d'origine américaine « *désigne une situation dans laquelle l'accès au marché d'une firme donnée dépend de l'utilisation d'une infrastructure contrôlée par un tiers qui peut, selon les circonstances, être son concurrent sur le marché aval* »[629].

---

[628]Commission européenne, 14 mai 2008, aff. COMP/M.4854, *TomTom c/Tele Atlas*, C(2008) 1859 ; comm. LAPREVOTE F.-C., BURE (de) F. et PAROCHE E. *RLC* 2009 n°18 p. 15, pt. 249.

[629] CASTETS-RENARD C. et MARTY F., « Facilités essentielles (approche économique et juridique) », *in* CORNU, M., ORSI, F. et ROCHFELD, J., ss. dir., *Dictionnaire des biens communs*, PUF, 08/2017, pp. 591 à 597, spéc. 591 ; TPICE, 15 sept. 1998, aff. T-374/94, T-375/94 et 388/94, *European Night services ltd et a. c/commission* ; Rec. II. 3141 ; note IDOT L., *Eur*. 1998 n°11 p. 17 ; note POILLOT-PERUZZETTO S., *CCC.* 1998 n°12, p. 14 ; note *LPA* 2000 n°27 p. 14 ; chron. CHABRIER H., COULON E., LORIOT G. et TRUCHOT L., *RMCUE* 2000 n°436 p. 179 ; BLAISE J.-B et IDOT L., RTD *Eur*. 1999 n°29 : « *Lorsque les infrastructures, produits ou services ne sont pas interchangeables, et qu'en raison de leurs caractéristiques particulières et notamment du coût prohibitif de leur reproduction et/ou du temps raisonnable requis à cette fin, il n'existe pas d'alternatives viables pour les concurrents potentiels* » ; VERDIER H., « La donnée comme infrastructure essentielle », *op. cit.*, p. 16.

La Cour de cassation a donné sa propre définition dans son rapport annuel du 3 juillet 2005 : « *Celui qui, en situation de monopole ou de domination sur un marché, détient une infrastructure essentielle, non reproductible dans des conditions économiques raisonnables, ressource sans laquelle des concurrents ne pourraient servir leurs clients ou exercer leur activité, peut être contraint de permettre à ses concurrents d'accéder à cette ressource, afin de protéger le jeu de la concurrence sur un marché aval, amont ou complémentaire* ». L'accès à une infrastructure essentielle doit être garanti aux concurrents afin de favoriser le libre jeu de la concurrence.

209- **Conditions.** Cette situation se retrouve lorsqu'une entreprise détient une ressource difficilement accessible par ses concurrents, voire impossible, dont il leur interdit l'accès de manière absolue ou relative. Les conditions mises en place pour accéder à cette ressource qu'elles soient techniques ou financières peuvent représenter des obstacles à la fourniture « *[d'] un service de qualité aux consommateurs* » ou peut lui permettre de dégager de la « *marge nécessaire à son maintien sur le marché* »[630]. Ainsi, afin de rendre l'activité pérenne, l'accès à la ressource est impératif et donc cette ressource est essentielle. Par conséquent, « *l'impossibilité économique de reproduire le bien pourrait correspondre aux hypothèses, tout à fait exceptionnelles, où la collecte des données représente un investissement considérable pour l'opérateur qui souhaite avoir accès à l'information* »[631]. Aussi, par les effets de réseau, des groupes d'entreprises peuvent obtenir de grandes masses de données en interdisant l'accès aux autres opérateurs.

210- **Exemples.** En droit interne, la théorie des facilités essentielles a été retenue à l'encontre d'exploitants historiques de ressources telles que l'électricité, avec EDF[632] ou le réseau de communication avec France Télécom[633]. Dans le secteur agricole, il ne fait aucun doute qu'une base de données telle que celle de l'IGN comportant des données géographiques nationales représente un coût considérable dans sa constitution. Mais cette hypothèse reste marginale[634].

---

[630] *Ibid*.

[631] BRUGUIERE, J.-M., « Intelligence artificielle et droit d'auteur : Sortir de la science-fiction des "machines/auteurs", entrer dans la réalité du droit des données », *CCE* n°6, juin 2020, 11.

[632] EDF avait augmenté le coût du raccordement au réseau, sans porter à leur connaissance les nouveaux critères retenus, ni justifier leur nécessité, pour évincer du marché ces producteurs plus performants : Cons. conc., déc. n°96-D-80, 10 déc. 1996, *CGC e. a. c/ EDF* ; Rec. *ADCC* ; obs. BERTHAULT F., *Lamy*, n°714 ; obs. MAINGUY D. et BERTHAULT F., *JCP E* 2001 n°49 p. 1 et CA Paris, 1re ch., 27 janv. 1998 *EDF c/ Société auxiliaire de chauffage et autres* : *BOCCRF* 1998 p. 54 ; note ADAM C. et BLAZY S., *AJDA* 1998 n°5 p. 435., *D. aff.* 1998, p. 326 ; *JCP E* 1998 ; MAINGUY, D. et DEPINCE, M., *Droit de la concurrence, op. cit.*, p. 318.

[633] Cons. conc., déc. n°05-D-59, 7 nov. 2005, *relative à des pratiques mises en œuvre par la société France Télécom dans le secteur de l'Internet haut débit* : *BOCC* 14 ; comm.

[634] BRUGUIERE, J.-M., « Intelligence artificielle et droit d'auteur : Sortir de la science-fiction des "machines/auteurs", entrer dans la réalité du droit des données », *op. cit.*

2. La reconnaissance jurisprudentielle des données comme facilités essentielles

211- Afin d'identifier une infrastructure essentielle, il faut, tout d'abord, établir les installations dont il s'agit[635]. En droit interne et en droit européen, les juges ont défini les installations pouvant être concernées par la théorie des facilités essentielles. En droit interne, la Cour d'appel de Paris a retenu comme facilités essentielles dans un arrêt du 23 septembre 1997 : « *des installations ou des équipements indispensables pour assurer la liaison avec des clients et/ou permettre à des concurrents d'exercer leurs activités et qu'il serait impossible de reproduire par des moyens raisonnables* »[636]. Ensuite, en droit européen, la Cour de justice de l'Union européenne a retenu dans l'arrêt *Bronner*[637] « *qu'un produit ou un service n'est indispensable que s'il n'existe pas de produits ou services alternatifs et si des obstacles techniques, juridiques ou économiques, rendent impossible ou excessivement difficile le développement de produit ou service par une entreprise, seule ou en collaboration, sur le marché aval* »[638]. Ainsi, il peut s'agir d'une infrastructure, d'un équipement, voire encore d'un produit, d'un service ou d'un droit de propriété intellectuelle. M. le Professeur D. Mainguy et M. M. Depincé relèvent en effet que « *l'évolution de la théorie montre qu'elle se décline également avec des facilités immatérielles, comme un monopole d'exploitation résultant d'un droit d'auteur comme dans l'affaire Magill, des Messageries lyonnaises ou dans l'affaire IMS Health, voire Microsoft* »[639]. Ainsi, dans l'affaire *Magill*, un éditeur souhaitant commercialiser un guide hebdomadaire s'était vu opposer par des chaînes de télévision des droits de propriété intellectuelle sur les programmes de télévision. La Cour de justice de l'Union européenne avait retenu que ce seul motif était injustifié et constitutif d'un abus de position dominante[640]. Dans l'affaire *Messagerie lyonnaise de presse* (MLP), il s'agissait de savoir si le refus d'accès à un outil logiciel pouvait constituer un abus de position dominante. Or, les MLP pouvaient concevoir un outil logiciel équivalent. Par conséquent, il n'y avait pas d'abus puisqu'une solution alternative existait[641].

---

[635] MAINGUY, D. et DEPINCE, M., *Droit de la concurrence*, *op. cit.*, n°336, p. 320.
[636] CA Paris, déc. n°97-D-69, 23 sept. 1997, *SARL Héli-Inter Assistance* : BOCC, 1997.
[637] CJCE, 26 nov. 1998, aff. C-7/ 97, *Oscar Bronner GmbH & Co KG c/ Mediaprint Zeitung,* préc., § 44 et 45.
[638] Aut. conc. et Bundeskartellamt, *op. cit.*, pp. 20 à 21.
[639] MAINGUY, D. et DEPINCE, M., *Droit de la concurrence*, *op. cit.*, n°336, p. 320.
[640] CJCE, 6 avr. 1995, aff. jointes C-241/91 et C-242/91, *Magill* ; *Rec*. p. I-743 ; obs. BONET G., *RTD eur*. 1995 p. 835 ; note BENABOU V.-L., *PI* 2002 n°3 p. 117 ; chron. POLLAUD-DULIAN F., *RTD com.* 2004 n°3 p. 491 ; Prat. HAUTBOURG S. et QUESSON S., *DJF* n°56 p. 64 ; chron. BONET G., RTD eur. 2004 n°4 p. 690 ; obs. LEVEQUE F., *concurrences* 2004 n°1 p. 16 ; note SARDAIN F., *JCP E* 2004 n°49 p. 1927 ; obs. GYSELEN L., *concurrences* 2005 n°2 p. 24 ; comm. VIVANT M., MALLET-POUJOL N. et BRUGUIERE J.-M., *JCP E* 2006 n°23 p. 1002 ; Ét. GRYNFOGEL C., JCP E 2008 n°47 p. 42 ; chron. SARDAIN F., *JCP E* 2009 n°5 p. 28.
[641] Cons. conc. déc. n°03-MC-04, 22 déc. 2003 : *BOCCRF* 13 févr. 2004 ; Paris, 12 févr. 2004, SAEM : *BOCC* 4 mai 2004, prat. DOM J.-P. et BACCICHETTI E., *LPA*, n°126, pp. 5 à 21, 2005 ; Com., 12 juill. 2005, n°04-12.388, NMPP/MLP : Bull. civ. 2005, IV, n°163 ; Note FRISON-ROCHE, M.-A., *RDA*, n°2006/2, 2006 ; CA Paris, 31 janv.

Dans l'affaire *IMS Health GmbH & Co. OHG*, la société IMS Health avait refusé une licence sur sa base de données à la société commercialisant des données sur les ventes régionales de produits pharmaceutiques. Les juges européens ont alors relevé la nécessité que le refus fasse obstacle à l'apparition d'un produit nouveau pour que ce refus d'accès à une infrastructure essentielle soit qualifié d'abus[642]. À l'inverse, l'obstacle à l'apparition d'un produit identique n'est pas considéré comme un abus. Enfin, dans l'affaire *Microsoft*[643], la société du même nom avait refusé de communiquer les informations nécessaires pour permettre l'interopérabilité des produits de la société Sun Microsystems (Sun) et les systèmes d'exploitation Windows pour PC. Ainsi, en raison de l'impact sur l'innovation de ce refus, la Commission européenne avait retenu que Microsoft était en situation de position dominante, cette décision a été confirmée par le TPICE. Par conséquent, tant au niveau européen avec les affaires *Magill* et *IMS Health* que national avec l'affaire des *Messageries lyonnaises de presse*, les juges ont eu l'occasion de reconnaître les données comme pouvant constituer des facilités essentielles. De ce fait, un refus d'accès injustifié ou des conditions d'accès prohibitives ou discriminatoires peuvent placer la firme qui détient la ressource essentielle, en l'occurrence des données, en situation d'abus de position dominante[644]. Donc, la mise en œuvre de la théorie permet d'organiser l'accès à la ressource « *par une injonction faite au détenteur de la facilité de garantir la concurrence sur un marché dérivé et de lutter contre le risque d'exclusion d'un opérateur* »[645]. Ainsi, « *des obligations de mise à disposition sous licence non discriminatoire pourraient alors être établies au niveau sectoriel, sur le modèle des licences FRAND (Fair, Raisonnable and Non-Discriminatory)* »[646].

B. Les limites de la théorie des facilités essentielles appliquée aux données agricoles

212- De prime abord, il semble difficile d'admettre que la théorie des facilités essentielles peut s'appliquer aux données agricoles du fait, tout d'abord, de leur caractère non rival (**1**), et ensuite, du fait du développement des nouvelles technologies (**2**).

2006, n°2005/14782 : obs., SELINSKY V., *Lamy conc.*, 2006, n°7, pp. 16 à 19 ; Com., 20 févr. 2007, n°06-12.424 : obs. PHILLIPE, J. et JANSSENS T., *LGP*, 2007, n°166, pp. 37 et 38.

642 CJUE, 29 avr. 2004, aff. C-418/01, *IMS Health GmbH & co. OHG*, préc.

643 TPICE, 22 déc. 2004, aff. T-201/04, *Microsoft*, Rec. 2004 II-04463 ; note BENABOU V.-L., *PI*, 2005 n°14, p. 89.

644 BOURGEOIS M., *Droit de la donnée*, *op. cit.*, n°1266, p. 287.

645 *Ibid.*

646 ZOLYNSKI, C., « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », *Dalloz IP/IT*, 2018, p. 94.

1. Le caractère non rival des données agricoles

213- Comme on l'a vu, la donnée est une chose particulière qui ne peut être saisie et qui peut être détenue par plusieurs personnes en même temps sans que son utilisation impacte les autres. Elles ont, donc, un caractère non rival. Il est alors particulièrement difficile de démontrer l'impossibilité pour les concurrents d'une entreprise qui détiendrait des données d'y accéder par d'autres moyens. En effet, de nombreuses bases de données sont aujourd'hui accessibles que ce soit gratuitement ou moyennant un prix et permettent de répondre à de nombreux besoins, comme le registre parcellaire graphique (IGN), les cartes d'occupation des sols (IGN, DRAAF), les données météorologiques (Météo France, Weather measures, etc.), etc. Isagri par exemple couple les données collectées sur l'exploitation de l'agriculteur avec celles de l'IGN pour obtenir une carte de rendement détaillée par parcelle, afin de fournir des informations précieuses à l'agriculteur sur les endroits de son champ où semer, où apporter de l'engrais, etc[647]. En ce qui concerne les données des agriculteurs, les entreprises spécialisées dans la gestion parcellaire, telle qu'Isagri, collectent elles-mêmes les données dont elles ont besoin au moyen d'outils qu'elles développent (capteurs, stations météorologiques, drones, etc.). En outre, l'Autorité de la concurrence a soulevé dans son avis du 10 mai 2016 que les « *critères de la CJUE ne seraient remplis que s'il est démontré que les données possédées par l'intéressé sont véritablement uniques et si son concurrent ne peut les obtenir autrement pour fournir ses services* »[648]. Par exemple, des données satellitaires, celles issues de la télédétection (Equipex GEOSUD, Projet Copernicus, etc.), sont difficiles à reproduire, mais ces données sont en grande partie ouvertes puisqu'il s'agit de données scientifiques[649], sur lesquelles il est difficile d'admettre un droit de propriété intellectuelle[650].

2. L'impact du développement de nouvelles technologies

214- Le développement des technologies permet de collecter et d'héberger des données de plus en plus facilement. Ceci facilite l'acquisition des données dont les concurrents auraient besoin pour le développement de leur activité à des coûts raisonnables. Juridiquement, il n'existe pas d'obstacles à la collecte des données par les concurrents. Si une entreprise souhaite collecter des données, rien ne l'y empêche. Aussi, l'application de la théorie des infrastructures

[647] https://geoservices.ign.fr/agriculture
[648] Aut. conc. et Bundeskartellamt, *op. cit.*, p. 21.
[649] Voir *supra*, n°59 et s.
[650] *Ibid.*

essentielles aux données agricoles, semble d'un intérêt mineur, puisque les données satellitaires particulièrement difficiles à obtenir font déjà l'objet d'une mise à disposition.

215- **Conclusion de la section.** L'accessibilité des données agricoles privées est une question sensible pour les acteurs du secteur agricole. Pourtant, l'ouverture des données agricoles d'intérêt général ou commun est plébiscitée et doit aujourd'hui faire l'objet d'un consensus afin de faire circuler l'information en fonction des demandes et des besoins. Le secteur agricole est particulièrement exposé à ce genre de revendication puisque ses activités touchent de près à la santé humaine et animale et à l'environnement. De plus, l'accessibilité des données doit répondre à des considérations économiques puisque celui qui est à l'origine des données brutes dans le secteur agricole est bien souvent l'agriculteur lui-même par l'utilisation qu'il fait des objets connectés au cours de ses activités. C'est en raison de sa position de générateur de données qu'un droit d'accès de principe doit lui être accordé sur les données qu'il génère. Ce n'est qu'à cette condition que l'agriculteur sera replacé au centre de l'économie des données agricoles. Enfin, il ne faut pas omettre l'intérêt concurrentiel des données. Leur rétention par certains acteurs pourrait s'avérer délétère dans le futur pour le libre jeu de la concurrence. Néanmoins, il faut faire le constat, d'une part, qu'un grand nombre de données agricoles, notamment géographiques, sont déjà mises à disposition des acteurs du secteur. D'autre part, les évolutions technologiques permettent aujourd'hui à n'importe quel acteur de collecter les données dont il a besoin afin de développer ses propres services. Pour l'heure, la concurrence se situe donc plutôt sur la variété des services proposés et leur qualité plutôt que sur la détention des données agricoles. Le manque d'interopérabilité peut toutefois limiter le partage des données et ostraciser les plus petits acteurs dont l'utilisation des services nécessite un appariement avec les outils ou les solutions logiciels de leurs concurrents. Mais dans un marché dynamique, il sera néanmoins difficile de démontrer une atteinte au libre jeu de la concurrence.

216- **Conclusion du chapitre.** Les réflexions menées sur le terrain de l'accessibilité des données agricoles privées ont pour ambition de démontrer l'importance de l'accès en tant que clef de voûte de la maîtrise de l'usage des données. Sans accès, les données ne peuvent faire l'objet de différents usages selon les besoins et les intérêts de chacun. La circulation de l'information est également au cœur de la démocratie et doit permettre à tout un chacun d'obtenir les informations qui ont une importance sociale, sanitaire, économique, environnementale, etc. Aussi, la question de l'accessibilité semble fondamentale dans une société qui tend plutôt à la

réservation de l'information en portant atteinte à la liberté d'information et à la liberté du commerce et de l'industrie.

Conclusion du titre. Afin d'obtenir un juste équilibre dans les jeux de pouvoir entre détenteurs des données et utilisateurs, seul le développement d'un principe légal d'accès aux données peut contraindre les acteurs à les mettre à disposition quand cela est nécessaire. Cette mise à disposition des données peut être rendue obligatoire en raison de leur nature, de leur objet ou de la personne qui les a générées. Le législateur a déjà organisé l'accès aux données agricoles produites ou collectées par une personne chargée d'une mission de service public ou par les chercheurs, à travers la politique d'ouverture des données publiques et celle du libre accès aux données de la recherche. Néanmoins, un travail considérable reste à faire concernant les données faisant l'objet d'une réservation privative.

Titre II. La réservation privative des données agricoles : l'organisation de l'exclusivité par les entreprises

217.- Le droit de la propriété intellectuelle permet de réserver économiquement une chose tout en permettant sa circulation[651]. Comme l'énonce M. le Professeur J.-C. Galloux, « *la question de l'accès va évidemment de pair avec celle de l'appropriation des données ou la reconnaissance d'un droit exclusif sur ces dernières* »[652]. La question de la réservation de l'accès aux données doit donc nécessairement passer par celle de leur appropriation. Au contraire, la réservation privative par le secret empêche, par définition, l'accès. Un droit de propriété sur les données aura pour conséquence d'octroyer des prérogatives au titulaire de droits sur la base qui pourra notamment organiser l'accès aux données. Les détenteurs de données agricoles ont donc la possibilité d'en réserver l'accès en les agrégeant dans des bases de données (**Chapitre 1**), mais aussi au moyen de la technique et du contrat (**Chapitre 2**).

[651] MOUSSERON J.-M. et VIVANT M., « Les mécanismes de réservation et leur dialectique : le "terrain" occupé par le droit », *JCP E*, n°11, 1988-1.
[652] GALLOUX, J.-C., « Libres propos sur le droit d'accès aux données », *op. cit.*, n°76.

Chapitre 1. La réservation de l'accès aux données agricoles protégées

218- Le secteur agricole produit et génère de nombreuses données qui, une fois modélisées, offrent des outils d'aide à la décision et divers services aux agriculteurs. Certaines de ces données sont agrégées et structurées dans des bases de données sur lesquelles leur créateur ou producteur revendiquent des droits. D'autres en revanche sont collectées au moyen d'objets connectés sans qu'un travail de structure soit accompli. Aussi, ces données peuvent être agglomérées dans des bases de données, dans des entrepôts de données (*Datawarehouse*) ou dans des lacs de données (*Datalake*). Le droit apporte donc une protection sur les bases de données contre les utilisations non autorisées par des tiers. En revanche, c'est le contrat qui permet de contrôler l'accès aux données. Il convient d'envisager, dans un premier temps, le principe d'un droit sur les bases de données (**Section 1**) pour s'intéresser, dans un second temps, à la contractualisation de l'accès aux bases de données (**Section 2**).

Section 1. Le principe de la protection duale des bases de données

219- Au vu de l'importance du partage de l'information dans nos sociétés de la connaissance, les bases de données ont très tôt été dans le viseur du législateur. Les données étant de libre parcours, celui-ci a octroyé une protection à ceux qui investissent de l'argent et du temps pour les assembler au sein de bases ou de banques[653]. M. le Professeur M. Vivant évoque d'ailleurs, au sujet de ce droit, un « *contournement, débordement de la propriété intellectuelle* »[654]. Dans le secteur agricole, de nombreuses données sont collectées et agrégées pour former des bases de données. Pour leur protection, deux régimes cohabitent. Si le droit d'auteur offre une protection aux bases de données originales, témoignant de l'activité créatrice de leur auteur **(§1)**, le droit du producteur de bases de données offre une plus grande amplitude en protégeant les bases de données qui ont fait l'objet d'un investissement substantiel (**§2**). Quoi qu'il en soit, ces dispositifs légaux de protection créent un « péage » pour l'accès aux données et donc aux informations.

---

[653] MALLET-POUJOL, N., *La commercialisation des banques de données, contribution à une approche juridique des richesses informationnelles*, thèse, LAMBERTERIE, I. (de), ss. dir., CNRS éd., 1992.
[654] VIVANT, M., « La privatisation de l'information par la propriété intellectuelle », *RIDE*, 2006/4 (t.XX,4), n°44, pp. 361 à 38.

§1. *La protection des bases de données originales par le droit d'auteur*

220- Tout d'abord, il convient de s'intéresser aux conditions de la protection des bases de données par le droit d'auteur (**I**) pour, ensuite, envisager le contenu de la protection du droit d'auteur (**II**).

I. Les conditions de la protection des bases de données par le droit d'auteur

221- Le Code de la propriété intellectuelle (CPI) protège la création (**A**) originale (**B**).

A. Création de forme: la base de données

222- En premier lieu, il est nécessaire d'envisager la notion d'œuvre de compilation (**1**). En second lieu, il faudra s'intéresser à la base de données, elle-même (**2**).

1. La notion d'œuvre de compilation

223- **Définition.** Une œuvre de l'esprit est une création intellectuelle qui résulte « *des choix opérés par l'auteur* »[655]. L'article L. 112-3 du CPI dispose que le bénéfice du droit d'auteur est accordé à l'auteur « *d'anthologies et de recueils d'œuvres ou de données diverses, tels que les bases de données, qui, par le choix ou la disposition des matières, constituent des créations intellectuelles* ». Ces auteurs bénéficient de la protection du droit d'auteur « *sans préjudice des droits de l'auteur de l'œuvre originale* ». L'article assure la protection des compilations de données, mais pas les données elles-mêmes. Ainsi, « *la compilation n'est pas, au sens propre, une œuvre dérivée, puisqu'elle ne doit rien à une œuvre protégée* »[656].

Les œuvres de compilation de données ont été prises en considération lors de la modification de l'article L. 112-3 du CPI par la loi du 18 décembre 1996. Le législateur a alors tenu compte de l'Accord sur les ADPIC[657] pour faire application du droit de la propriété intellectuelle aux compilations utilitaires. Toutefois, ces compilations doivent répondre aux

[655] *Ibid.*, n°53, p. 69.
[656] LUCAS, A., LUCAS, H.-J. et LUCAS-SCHLOETTER A., *Traité de la propriété littéraire et artistique*, LexisNexis, 4e éd., n°132, p. 138.
[657] Accord de l'Organisation Mondiale du Commerce sur les aspects des droits de propriété intellectuelle qui touchent au commerce du 15 avr. 1994.

conditions d'application du droit d'auteur et doivent constituer des créations intellectuelles, « *par le choix ou la disposition des matières* ». En outre, la préposition « ou » implique qu'il n'est plus exigé un cumul de conditions, à l'inverse du texte initial[658]. Il n'est, donc, pas utile que le producteur ait choisi et disposé la matière pour obtenir la protection, il s'agit d'une simple alternative.

2. La base de données

224- **Définition**. La base de données est définie par l'article L. 112-3, alinéa 2 du CPI comme « *un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou tout autres moyens* ». C'est une universalité de fait[659], c'est-à-dire « *une collection de biens qui, par interprétation de la volonté du propriétaire, est traitée comme un bien unique et soumise à un régime particulier* »[660]. Donc, c'est un ensemble constitué[661] d'éléments — recueil d'œuvres, de données ou autres — réunis en un seul, la base de données. La difficulté réside dans la démonstration de la réunion des éléments dans la base.

225- **Importance de l'apport intellectuel.** Qualifiées d'œuvres de « *petite monnaie* »[662], les bases de données, catalogues, annuaires et guides, sont les *parents pauvres* du droit d'auteur. Ce sont des « *œuvres du langage de caractère technique et des compilations utilitaires* »[663], pour lesquelles il est très difficile de démontrer une création intellectuelle. Or, les juges du fond ont affirmé dans plusieurs affaires qu'un simple travail, de compilation[664] ou dans le choix des matières, ne suffit pas à caractériser une création[665]. Par conséquent, il faut constater un

---

[658] Art. L. 112-3 du CPI dans sa version initiale issu de la loi n°92-597 du 1er juill. 1992 : JORF du 3 juill. 1992 : « *Les auteurs de traductions, d'adaptations, transformations ou arrangements des œuvres de l'esprit jouissent de la protection instituée par le présent code sans préjudice des droits de l'auteur de l'œuvre originale. Il en est de même des auteurs d'anthologies ou recueils d'œuvres diverses qui, par le choix et la disposition des matières, constituent des créations intellectuelles* ».

[659] CARBONNIER, J., *Droit civil, les biens, les obligations*, t.3, 2e éd., PUF, Paris, 2017, n°724, p. 1625 : « *L'universalité de fait n'est qu'un ensemble de biens ; l'universalité de droit ou universalité juridique est, à la fois, un ensemble de biens et de dettes, comporte un passif en même temps qu'un actif, tous deux en réciproque dépendance, le passif naissant de la gestion de l'actif, l'actif affecté au paiement du passif* ».

[660] *Ibid.* ; COHEN A., *Traité théorique et pratique des fonds de commerce*, vol. 1, rec. S., 1937, n°17 et s, pp. 10 à 16.

[661] LIBCHABER, R., « Le portefeuille de valeurs mobilières : bien unique ou pluralité de biens ? », *Defrénois*, 1997, n°4 et s., p. 65.

[662] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique*, *op. cit.*, n°113, 119 et 125.

[663] *Ibid.*, n°113, p. 130.

[664] Civ. 1ère, 2 mai 1989, n°87-17.657, *Coprosa*, Bull. 1989 I n°180 p. 120 ; *RIDA* 1/1990, n°309, comm., POLLAUD-DULIAN, F., *Légipresse*, n°118, pp. 1 à 17 ; note LUCAS A., *JCP G* 1990, II, 21392.

[665] POLLAUD-DULIAN, F., « Idées. Méthode intellectuelle. Choix arbitraires mais pas créatifs », *RTD Com.*, 2006, p. 78 ; Civ. 1re, 29 nov. 2005, *Marie-Claire Album c/ Hamel*, n°04-12.721 : obs. DALEAU J., *D.* 2006, AJ p. 145,

véritable apport intellectuel et c'est cette position qu'a retenue la Cour d'appel de Paris, dans un arrêt du 15 janvier 1997[666]. Aussi, la reconnaissance des bases de données comme œuvre de l'esprit n'a pas fait l'unanimité au sein de la doctrine puisque, pour considérer une base de données comme une œuvre de l'esprit, encore faut-il démontrer son originalité.

B. Création originale : originalité de la structure de la base

226- Une seule condition est nécessaire pour que le droit d'auteur s'applique à une base de données, il faut démontrer son caractère original. Plusieurs critères ont été dégagés afin de démontrer l'originalité d'une base de données (**1**), encore faut-il apprécier cette « originalité » (**2**).

1. La notion d'originalité

227- **L'originalité : condition *sine qua non* de la protection.** « *L'existence d'originalité, comme condition de la protection des œuvres, est universelle* »[667], elle en serait même la « *pierre angulaire* »[668]. C'est cette unique condition qui permet de reconnaître comme objet de droit d'auteur, la base de données, et ce peu importent le genre, la forme d'expression, le mérite ou la destination[669].

Aussi, la condition d'originalité est comprise dans la directive 96/9/CE du 11 mars 1996 concernant la protection juridique des bases de données. L'article 3.1 prévoit à cet effet que « *les bases de données qui, par le choix ou la disposition des matières, constituent* ***une création intellectuelle propre à leur auteur*** *sont protégées comme telle par le droit d'auteur.* ***Aucun autre critère*** *ne s'applique pour déterminer si elles peuvent bénéficier de cette protection* » [nous soulignons]. À la lecture de cet article, le seul critère retenu par la directive est donc une « *création propre à son auteur* ». Cette formulation peut interroger quant à l'interprétation que l'on peut en faire. Elle témoigne d'une acception large de la notion *d'originalité*[670]. La directive précise, également, qu'aucun autre critère ne doit être pris en compte pour déterminer si cette

---

et note TRICOIRE A., *Jur.* p. 517 ; obs. CARON C., *CCE*. févr. 2006, n°18 ; Cass. 1ére civ., 2 mai 1989, *Coprosa*, préc.

[666] CA Paris, 4e ch., 15 janv. 1997 ; JurisData n°1997-022369 ; *Expertises* 1997, p. 193, note TELLIER-LONIEWSKI, L., *LGP*, n°18, pp. 52 et 53.

[667] VIVANT, M., « À la recherche de la condition d'originalité », *GAPI*, Dalloz, 2e éd., 2020, comm. 44 à 46, p. 274 s.

[668] LUCAS, A. et SIRINELLI, P., « L'originalité en droit d'auteur », *JCP*, 1993. I. 3681, n°1.

[669] Civ. 1re, 6 mars 1979, n°76-15.367 : Bull. civ. I, n°82 ; obs. FRANÇON A., *RTD com.* 1979. 462.

[670] LUCAS, A., « Propriété littéraire et artistique », fasc. 1650 : droits des producteurs des bases de données, (CPI, art. L.112-3 L.341-1 à L.343-7), *J.-Cl Civil Annexes*, 3 nov. 2010, mis à jour 1er févr. 2018, n°13.

protection peut s'appliquer[671]. De cette manière, le législateur distingue nettement l'application de la protection du droit d'auteur de celle du droit *sui generis* contenu dans la même directive. Ainsi, les conditions d'application du droit *sui generis* ne seront pas recherchées pour la protection d'une base de données originale déjà soumise au droit d'auteur.

Par conséquent, l'originalité est la condition de fond pour que la base de données puisse bénéficier de la protection par le droit d'auteur. Cependant, il faut apporter une précision quant à l'application de l'originalité. Celle-ci est à rechercher dans la forme de la chose, c'est-à-dire dans le « *choix ou la disposition des matières* » aux termes de la Convention de Berne de 1886[672], formulation reprise à l'article 3.1 de la directive précédemment évoquée. La condition d'originalité est, donc, remplie « *lorsque, à travers le choix de la disposition des données, qu'elle contient, son auteur exprime sa capacité créative de manière originale en effectuant des choix libres et créatifs [...] et imprime ainsi sa touche personnelle* »[673]. L'arrêt *Infopaq* « *a étendu le critère à toutes les œuvres et en faisant de l'originalité une notion autonome de droit de l'Union* »[674].

2. L'appréciation de l'originalité sur la base

228- Si certaines voix dissonantes ne reconnaissent pas qu'une base de données puisse être originale[675], la question de l'originalité a néanmoins suscité des réflexions quant à la conception qu'il faut en retenir. En effet, l'originalité est reconnue comme « *une "notion-cadre" ouverte à toutes les interprétations* »[676]. Aussi la question s'est posée de savoir si l'originalité devait être envisagée de manière subjective ou de manière objective dans la directive.

229- **Conception subjective.** Seule l'empreinte de la personnalité de l'auteur est prise en compte. C'est ce qu'a pu laisser entendre la CJCE dans son arrêt du 16 juillet 2009. Dans cet arrêt, la Cour de justice a retenu que c'est à travers « *le choix, la disposition et la combinaison de ces*

---

[671] VIVANT, M., « À la recherche de la condition d'originalité », *op. cit.*, spéc. p. 274 s. : « *Pour juger du caractère protégeable d'une base, il n'y a pas lieu de s'attacher à un autre critère que celui de l'originalité* ».
[672] Convention de Berne, pour la protection des œuvres littéraires et artistiques, 9 sept. 1886, art. 5 ; MALLET-POUJOL, N., « Droit des bases de données », *J.-Cl. Communication*, fasc.
[673] VIVANT, M., « À la recherche de la condition d'originalité », *op. cit.*, pt. 38, p. 284.
[674] BERNAULT C., LUCAS A. et LUCAS-SCHLOETTER A., *Traité de la propriété littéraire et artistique*, *op. cit.*, n°123, p. 142.
[675] EDELMAN, B., « Les bases de données ou le triomphe des droits voisins », *op. cit.*, n°5, p. 89 : Les bases de données sont « *de vulgaires compilations sans le moindre gramme d'originalité et qui ont seulement exigé des investissements plus ou moins importants en temps, en argent, en matériel* » ; BINCTIN, N., *Droit de la propriété intellectuelle, op. cit.*, n°257, p. 189 : « *Quelle originalité lorsque l'information est classée par ordre croissant, décroissant, alphabétique, historique, etc. ?* ».
[676] VIVANT, M., « À la recherche de la condition d'originalité », *op. cit.*, pp. 274 et s.

mots qu'il est permis à l'auteur d'exprimer son esprit créateur de manière originale et d'aboutir à un résultat constituant une création intellectuelle »[677]. Dans ce cas, « *le monopole est fondé sur le lien entre la personne de l'auteur et l'œuvre qui en est le prolongement* »[678]. Ainsi, donc, « *il suffit qu'une œuvre donne prise aux droits d'auteurs, [pour] qu'elle soit originale* »[679]. Mais cette conception de l'originalité conduit à s'interroger sur l'intégration dans le droit d'auteur des bases de données et des logiciels, puisqu'il est difficile de démontrer la marque de la personnalité du créateur dans la constitution d'une base de données.

230- **Conception objective.** D'autres auteurs, comme M. le Professeur A. Lucas, retiennent une conception objective de la notion d'originalité en la rapprochant de la créativité. Selon cet auteur, il ne faut pas « *fonder la protection sur le travail d'organisation de la base ou sur l'arrangement des données* », car cela permettrait de « *monopoliser un savoir-faire* »[680]. Ainsi, conseille-t-il d'opérer « *la même rupture que pour les logiciels* »[681] en reconnaissant que « *l'originalité s'entend, en droit d'auteur, d'une activité créative procédant de l'arbitraire du créateur* »[682]. Selon cet auteur, c'est cette conception, en définitive, que retient l'arrêt *Infopaq* puisque « *l'originalité, dans la définition très générale que retient la Cour de justice, qui s'applique à toutes les œuvres, n'est rien d'autre que l'activité créative, dépouillée de toute connotation subjective* »[683]. Par conséquent, la notion d'originalité est suffisamment large pour englober un grand nombre de bases de données.

231- **Éléments de reconnaissance de l'originalité de la base de données**. C'est l'organisation de l'information qui doit être originale, le contenant, c'est-à-dire, la base elle-même, et non pas le contenu c'est-à-dire, les données incluses dans cette base. En effet, si les bases de données ne sont constituées que de manière automatique alors les bases de données ne résultent que du savoir-faire de l'entreprise et non pas d'une véritable création originale protégée par le droit

---

[677] CJUE, 16 juill. 2009, aff. C-5/08, *Infopaq International A/S contre Danske Dagblades Forening*, note SARDAIN, F., *JCP E*, n°30 à 33, pp. 30 à 31 ; note MICHAUX B., *Auteurs & Média*, n°5, pp. 473 à 488 ; note VELARDOCCHIO D., *Droit et Patrimoine*, n°185, pp. 106 à 107 ; note POLLIAUD-DULIAN F., *RTD com.*, n°4, pp. 715 à 717 ; note MARINO L., *Revue des aff. Eur.*, n°2, pp. 361 à 365, pt. 45. LUCAS, A., « Propriété littéraire et artistique », *op. cit.*, n°11, dans ce sens MICHAUX, B., « L'originalité en droit d'auteur, une notion davantage communautaire après l'arrêt Infopaq », *Auteurs & Média* 5/2009, pp. 473 à 488.

[678] BERNAULT, C., LUCAS, A., et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique*, *op. cit.*, n°125, p. 145.

[679] DESBOIS, H., « Le droit d'auteur en France », *RIDC*, vol. 31, n°2, 1978, n°3.

[680] CJUE, 16 juill. 2009, aff. C-5/08, *Infopaq*, préc., pt. 45. LUCAS, A., « Propriété littéraire et artistique », *op. cit.*, n°11, dans ce sens MICHAUX, B., « L'originalité en droit d'auteur, une notion davantage communautaire après l'arrêt Infopaq », *op. cit.*

[681] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique*, *op. cit.*, n°125, p. 145.

[682] *Ibid.*, n°126, p. 146.

[683] *Ibid.*

d'auteur. Or, dans l'arrêt de principe *Coprosa*[684] du 2 mai 1989, la Cour de cassation a eu l'occasion de refuser la protection d'une base de données qui ne représentait qu'un simple travail de compilation d'informations non protégé par la loi[685].

Aussi, la jurisprudence a eu l'occasion de reconnaître l'originalité de différentes bases de données, par exemple, le « *répertoire SIRENE créé et exploité par* l'INSEE »[686], ou encore l'annuaire de France Télécom[687]. La Cour de justice retient que « *la protection par le droit d'auteur est subordonnée à la condition que le choix ou la disposition des données qu'elle contient constitue une expression originale de la liberté créatrice de son auteur* »[688].

Dans d'autres cas, les juges du fond ont pu refuser de reconnaître le caractère original de la base de données. Pour donner quelques exemples, il en a été ainsi lorsque « *la représentation est imposée par le propre contenu des données traitées et les usages en vigueur* »[689]. Il en est de même, lorsque « *les catégories et critères retenus par la société demanderesse pour "classer et rechercher les éléments collectés"* sont dictés *"par le sujet même de la base de données et par son objet"* »[690], ou encore, lorsque « *le choix et la disposition des données contenues dans la base de données revendiquée par la SAS Michelin Travel Partner au titre du droit d'auteur sont banals et ne constituent pas une expression originale de la liberté créatrice de son auteur* »[691], lorsque « *le classement "strictement fonctionnel" ne caractérise pas "une création originale témoignant d'une inspiration personnelle"* »[692], ou bien encore lorsqu'il « *traduit la "simple mise en œuvre d'une logique automatique et contraignante dans la conception et l'écriture"* »[693].

Pour l'heure, il semble qu'aucune jurisprudence ne porte sur une base de données du secteur agricole. En étudiant les bases de données créées par les instituts techniques et les

---

[684] Civ. 1ère, 2 mai 1989, n°87-17.657, *Coprosa*, préc.
[685] CA Paris, 4e ch., 8 oct. 1998, n°15, p. 24, note MECARY.
[686] CE ass., 10 juill. 1996, *Sté Direct mail promotion*, n°168702, 168734, 169631, 169951 ; *Rec.* 277 ; concl. DENIS-LINTON M., *RFDA* 1997. 115 ; note MAISL H., *AJDA* 1997, 189.
[687] Paris, 1ère ch., 30 sept. 2008 : JurisData n°2008-371143.
[688] CJUE, 1er mars 2012, aff. C-604/10, *Football Dataco Ltd et autres c/Yahoo ! UK Ltd*, I, note 447, note VELARDOCCHIO D., *Droit et Patrimoine*, n°228, p. 64 ; note BENABOU V.-L., *PI*, n°46, pp. 88 à 92 ; note MARINO L., *LGP*, n°214 à 215, pp. 11 à 12 ; note IDOT, L., *Europe*, n°5, pp. 45 à 46, 2012.
[689] LUCAS, A., « Propriété littéraire et artistique », *op. cit.*, n°14 ; T. Com., Lyon, 30 juill. 1993 : note LATREILLE A., *LPA* 28 avr. 1995, p. 14 ; obs. VIVANT M. et LE STANC C., *JCP E* 996, I, 559 ; obs. KÉRÉVER A., *RIDA* 4/1994, p. 297.
[690] LUCAS, A., *id.* ; TGI, Paris, 3e ch., 13 avr. 2010 : note CARON C., *CCE*, 2010, comm. 84, 3e esp. ; obs. BERNAULT C., *LEPI* nov. 2010, p. 3.
[691] CA Paris, pôle 5, 27 oct. 2015 : obs. BRUGUIERE, J.-M., *PI*. 2016, p. 69 ; note LARRIEU, *D.*, 2016, p. 2141.
[692] *Ibid.* ; CA Paris, 4e ch., 18 juin 1999 : *RIDA* 1/2000, p. 316 ; note CARON C., *CCE*, 1999, comm. 21, 3e esp.
[693] *Ibid.* ; CA Paris, 4e ch., 18 juin 2003 : JurisData n°2003-223155 ; note CARON C., *CCE*, 2003, comm. 106, ; obs. SIRINELLI P., *D.* 2003, p. 2756 ; voir aussi pour une base regroupant les coordonnées professionnelles et personnelles des anciens élèves d'une école, CA Paris, 4e ch., 28 févr. 2007 : *RIDA* 2/2007, p. 315 ; obs. LUCAS, A., *PI*, 2007, p. 331.

instituts de recherche agricole, il apparaît néanmoins que certaines d'entre elles, dans leur conception, caractérisent une œuvre de l'esprit originale. C'est le cas, notamment, des bases de données dans lesquelles différents jeux de données sont croisés afin d'obtenir des informations utiles en agronomie, pour développer des modèles prédictifs. C'est le cas notamment des bases de données créées par *INRAE*. Y sont ainsi croisées les données de suivis des pratiques, sur différentes parcelles dans plusieurs sites pendant une période déterminée, avec les données d'observations de prédateurs de cultures. L'objectif de ce croisement de données est d'observer des services écosystémiques. Dans une autre base de données de l'*INRAE*, les données agrégées décrivent l'évolution des systèmes agricoles dominants sur les cinquante dernières années à l'échelle d'un bassin hydrographique et sont couplées à des outils de modélisations[694]. Également, il est possible de relever la base de données d'Arvalis dans laquelle sont comparées des données de pratiques culturales et des données d'observations. L'organisation des données dans ces bases témoigne d'un choix de création afin d'obtenir des informations déterminées. Il y a sans nul doute une véritable création intellectuelle dans le choix de l'organisation des bases de données.

En comparaison, les bases de données agricoles, constituées de données brutes générées par des machines ou des capteurs sans classement ni organisation, détenues par les éditeurs de logiciels ou fournisseurs de matériels ne semblent pas pouvoir bénéficier de la protection du droit d'auteur. De même, les lacs de données dans lesquels sont stockés de gros volumes de données hétérogènes dans leurs formats originaux ne témoignent pas d'une activité créatrice. Le processus est dans les deux cas automatisé, il n'y a, donc, pas d'apport intellectuel dans le choix de classement et d'organisation des matières. Également, lorsque l'entreprise effectue un travail d'analyse sur les données qui résulte d'un simple savoir-faire[695], le droit d'auteur ne peut pas s'appliquer. Ces bases de données ne sauraient donc bénéficier de la protection du droit d'auteur.

II. Le contenu de la protection du droit d'auteur

232- Les instituts de recherche, les instituts techniques et l'ensemble des acteurs du secteur agricole qui créent des bases de données originales afin d'obtenir des informations nécessaires à la recherche en agronomie ou pour le développement de matériels et de services à destination des

[694] Base de données Arseine, INRAE, CNRS.
[695] Voir *infra*, n°528.

agriculteurs peuvent bénéficier du droit d'auteur. Il convient donc d'en envisager l'étendue (**A**) et les exceptions (**B**).

A. L'étendue du droit d'auteur

233- **Définition**. L'article L. 111-1 du CPI dispose que « *l'auteur d'une œuvre de l'esprit jouit de cette œuvre, du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous* ». Ainsi, dès lors qu'il a créé son œuvre, l'auteur en devient propriétaire, sans modalités supplémentaires. Le simple fait de créer est le fait générateur du droit de propriété et est constitutif de droit. Il faut préciser qu'à la différence du droit des logiciels, la qualité de salarié n'a pas pour effet de transmettre le droit à l'employeur[696]. Il se peut que la base de données soit créée par plusieurs personnes auquel cas il s'agira d'une œuvre collective[697] ou d'une œuvre de collaboration[698] au sens de l'article L. 113-2 du CPI. Dans le secteur agricole, les éditeurs de logiciel, les instituts techniques agricoles, les instituts de recherche et les fournisseurs de matériels sont susceptibles de créer des bases de données qui relèvent du droit d'auteur. C'est donc la personne qui crée la base qui détient le droit d'auteur en l'occurrence un chercheur ou un salarié d'une entreprise de l'*Agtech*. Le ou les titulaires du droit d'auteur bénéficieront des droits patrimoniaux et moraux sur la base qu'il a ou qu'ils ont créés. Cette protection dure toute la vie de l'auteur et soixante-dix ans après son décès[699]. Ainsi, les articles L. 122-1 et suivants du CPI déterminent les droits exclusifs détenus par l'auteur de la base de données. Il convient d'envisager succinctement, les droits patrimoniaux (**1**), puis les droits moraux (**2**).

1. Les droits patrimoniaux

234- L'auteur d'une base de données originale dispose de droits patrimoniaux, c'est un droit d'exploitation qui « *comprend le droit de représentation et le droit de reproduction* »[700] de celle-ci. Il s'agit de droits exclusifs, l'article 5 de la directive 96/9 dispose en effet que « *l'auteur d'une base de données bénéficie […] du droit exclusif de faire ou d'autoriser…* »[701].

---

[696] GRYNBAUM, L., LE GOFFIC, C. et MORLET-HAÏDARA, L., *Droit des activités numériques*, Dalloz, 1e éd., 2014, n°666, p. 464.
[697] CA Paris, 27 juin 2012 : obs. COSTES, L., *RLDI* 2012/85, n°2859.
[698] *Ibid.*
[699] CPI, art. L. 123-1.
[700] CPI, art. L. 122-1, I.
[701] Dir. 96/9/CE, du 11 mars 1996 concernant la protection juridique des bases de données, préc., art. 5.

L'auteur n'est donc « *pas obligé de consentir à l'exploitation et, s'il choisit de le faire, c'est aux conditions qu'il pose* »[702].

2. Les droits moraux

235- L'auteur bénéficie de droits moraux sur son œuvre régis par les articles L. 121-1 et suivants du CPI. L'auteur « *jouit du droit au respect de son nom, de sa qualité et de son œuvre* »[703]. Il « *a seul le droit de [la] divulguer* »[704] et « *jouit d'un droit de repentir ou de retrait vis-à-vis du cessionnaire* »[705].

B. Les exceptions spécifiques du droit d'auteur

236- La protection des bases de données par le droit d'auteur connaît les exceptions communes à toutes les œuvres prévues à l'article L. 122-5 du CPI, seulement quelques exceptions lui sont spécifiques. Aussi, deux exceptions seront évoquées ici, à savoir l'exception de copie privée (**1**) et l'exception relative à l'accès aux bases de données divulguées (**2**). D'autres exceptions sont communes au droit d'auteur et au droit *sui generis* et seront étudiées dans le cadre de la protection des bases de données par le droit *sui generis*.

1. L'exception de copie privée

237- L'article L. 122-5, 2e du CPI exclut l'exception de copie privée pour les bases de données électroniques. Ainsi, « *lorsque l'œuvre a été divulguée, l'auteur ne peut interdire les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective* »[706]. Cette exception ne vaut pas pour les bases de données électroniques, elle ne s'applique qu'aux bases de données sur support-papier. En outre, l'article L. 122-5, 6e du CPI exclut l'exception de copie technique transitoire pour toutes les bases de données[707].

---

[702] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique*, *op. cit.*, n°251, pp. 247 et 248.
[703] CPI, art. L. 121-1.
[704] CPI, art. L. 121-2.
[705] CPI, art. L. 121-4.
[706] ROBIN, A., *Droit des données de la recherche*, *op. cit*., n°185, p. 144.
[707] GRYNBAUM, L., LE GOFFIC, C. et MORLET-HAÏDARA, L., *Droit des activités numériques*, *op. cit*., n°669, p. 464.

2. L'exception relative à l'accès aux bases de données

238- L'article L. 122-5, 5e du CPI prévoit que lorsque la base de données a été divulguée, l'auteur ne peut interdire « *les actes nécessaires à l'accès au contenu d'une base de données électronique pour les besoins et dans les limites de l'utilisation prévue par contrat* ». Cet article fait échapper au droit exclusif, c'est-à-dire au droit de reproduction, ces actes. Aussi, l'auteur ne cède son monopole que pour l'accès à la base et non pas pour son utilisation. La portée du droit d'accès en droit français est donc réduite par rapport à celui du droit européen qui prévoit à l'article 6.1 de la directive du 11 mars 1996 qui autorise l'utilisateur légitime de la base à effectuer, sans l'autorisation de l'auteur, « *tous les actes visés à l'article 5 qui sont nécessaires, à l'accès au contenu de la base de données et à son utilisation normale par lui-même* ».[708]

§2. *La protection des bases de données agricoles par le droit* sui generis

239- Le droit du producteur de bases de données a été créé en 1996 par l'Union européenne, puis il a été transposé en droit français en 1998[709] et codifié au livre IV « Droit des producteurs de bases de données » du CPI[710]. Le droit *sui generis* « *complète la protection fondée sur le droit d'auteur* »[711] et peut « *s'exercer sans préjudice du droit d'auteur auquel la base en elle-même peut donner prise* »[712]. Par conséquent, si le producteur de la base de données est en même temps titulaire du droit d'auteur ou si les droits sont dans des mains différentes, les deux régimes — le droit d'auteur et le droit *sui generis* — s'appliquent de manière distributive, ce qui peut compliquer l'analyse[713]. De même, le droit d'auteur est susceptible de protéger les éléments contenus dans la base lorsque ces éléments répondent aux conditions d'application du régime, « *ce qui peut viser des œuvres (ou des parties d'œuvres) préexistantes ou spécialement créées en vue de la constitution de la base* »[714]. Or, les règles du droit d'auteur et du droit *sui generis* n'ont pas le même champ d'application, ainsi les deux régimes s'appliqueront de façon

---

[708] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique, op. cit.*, n°417, p. 385.
[709] Loi n°98-536, 1er juill. 1998 portant transposition dans le code de la propriété intellectuelle de la directive 96/9/CE du Parlement européen et du Conseil, du 11 mars 1996, concernant la protection juridique des bases de données : *JORF* n°151 du 2 juill. 1998.
[710] CPI, art. L. 341-1 et s.
[711] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique, op. cit.*, n°1354, p. 1053.
[712] *Ibid.*
[713] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Ibid*.
[714] *Ibid.*

distributive. En effet, le producteur de la base de données n'est pas investi des prérogatives d'un auteur sur les éléments contenus dans sa base.

Dans le secteur agricole, il existe des bases de données de très gros volumes, telles que les bases de données météorologiques ou d'occupations du sol. Ces bases de données ne sont, en général, pas originales, puisqu'elles sont composées de données dont le classement est fonctionnel et ne témoignent pas d'une activité créatrice de leur auteur. En revanche, elles représentent de gros investissements nécessitant une protection du résultat. Aujourd'hui, les observateurs soulèvent une difficulté concernant les bases de données ne contenant que des données brutes générées par des capteurs et des machines connectés qui sont le coproduit d'une activité principale sur les exploitations. Aussi, la question se pose de savoir si ces bases de données peuvent bénéficier de la protection du droit *sui generis*. Afin de répondre à cette question, il convient d'envisager, en premier lieu, les bénéficiaires du droit *sui generis* (**I**) pour étudier, en second lieu, le contenu du droit *sui generis* (**II**).

I. Les bénéficiaires du droit *sui generis*

240- Le titulaire du droit *sui generis* est la personne qui prend l'initiative, le risque d'investir et qui fait un investissement substantiel pour l'obtention, la présentation et la vérification du contenu de la base de données[715]. Aussi, il est nécessaire de s'intéresser à l'investissement (**A**) et à sa caractérisation (**B**).

A. Condition d'application du droit *sui generis* : l'investissement

241- L'article 7 de la directive 96/9/CE du 11 mars 1996 portant sur la protection juridique des bases de données permet « *d'interdire l'extraction et/ou la réutilisation de la totalité ou d'une partie substantielle du contenu de celle-ci, évaluée de façon qualitative ou quantitative, lorsque l'obtention, la vérification ou la présentation de ce contenu attestent un investissement substantiel d'un point de vue qualitatif ou quantitatif* ». Cette protection en faveur du « fabricant » de la base est d'une durée de quinze ans. L'étude de la condition d'application

[715] CPI, art. L. 341-1 : « *Le producteur d'une base de données, entendu comme la personne qui prend l'initiative et le risque des investissements correspondants, bénéficie d'une protection du contenu de la base lorsque la constitution, la vérification ou la présentation de celle-ci atteste d'un investissement financier, matériel ou humain substantiel* ».

du droit *sui generis* suppose d'étudier, tout d'abord, l'objet du droit *sui generis* (**1**) et, ensuite, la définition de l'investissement (**2**).

1. L'objet du droit sui generis : le contournement de la condition d'originalité

242- **Logique propre du droit *sui generis.*** Le droit *sui generis* des bases de données est un droit voisin du droit d'auteur. Il a pour vocation de protéger le producteur de la base de données qui a investi dans l'élaboration de la base. Ainsi, « *il ne s'agit [plus] de reconnaître le droit d'un auteur sur une création intellectuelle, mais de permettre à une entreprise de financer les coûts de collecte et de traitement de cette matière première que constituent les données* »[716]. Le droit *sui generis* permet donc « *l'appropriation de la valeur économique que constitue l'information, plus exactement d'un ensemble informationnel* »[717]. Néanmoins, ce droit doit être limité afin de « *concilier la rémunération de l'investissement et le principe selon lequel les idées (et donc les informations en elles-mêmes) sont de libre parcours* »[718]. Le droit *sui generis* a pour objectif « *de protéger les fabricants de bases de données contre l'appropriation des résultats obtenus de l'investissement financier et professionnel consenti par celui qui a recherché et rassemblé le contenu* »[719]. Ainsi, « *ce droit sui generis n'a rigoureusement rien à voir avec le droit d'auteur. C'est un droit sur l'investissement qui obéit à une logique propre* »[720].

243- **Objet du droit *sui generis.*** À la différence du droit d'auteur qui ne protège que le contenant — la structure de la base de données, le droit *sui generis* protège, lui, le contenu informationnel de la base. Aussi, le droit *sui generis* porte sur les informations contenues dans la base[721], il y a donc appropriation d'un « contenu informationnel »[722], ainsi ces conditions permettent « *d'assurer une privatisation de l'information — de l'information contenue dans la base* »[723]. L'objectif, dans lequel s'inscrit la Directive, est donc de protéger l'investisseur du parasitisme ou de la concurrence déloyale en interdisant « *les actes d'extraction et/ou de réutilisation de la*

---

[716] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique*, *op. cit.*, n°1355, p. 1054.
[717] *Ibid.*
[718] *Ibid.*
[719] Dir. 96/9/CE, *op. cit*., consid. 39, in FERAL-SCHUHL C., *Cyberdroit, Le droit à l'épreuve de l'Internet*, Dalloz, 7e éd., 2018-201, n°341.21, p. 921.
[720] VIVANT, M., « l'investissement, rien que l'investissement », *RLDI*, 2005/3, p. 41.
[721] DOUTRELEPONT, C., « Le nouveau droit exclusif du producteur de bases de données consacré par la directive européenne 96/9/C du 11 mars 1996 », *Mél. M. WAELBROECK*, *Bruylant*, 1999, pp. 903 à 920.
[722] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique*, *op. cit.*, 4e éd., n°1198, p. 983.
[723] VIVANT, M., « La privatisation de l'information par la propriété intellectuelle », *op. cit*., pp. 361 à 388.

base qui portent atteinte à l'investissement du producteur »[724]. La protection est, ainsi, plus efficace que celle assurée par le droit d'auteur, elle protège « *l'information, même non appropriée* »[725]. Cependant, cette protection ne peut exister qu'à la condition d'attester d'un investissement substantiel.

2. La notion d'investissement

244- **Définition.** L'investissement est « *un transfert finalisé, destiné à servir les objectifs de celui qui le réalise* »[726]. La directive ne prévoyait que l'investissement et n'envisageait pas sa nature. Ainsi, le législateur français a précisé la nature de cet investissement à l'article L. 341-1 alinéa 1er du CPI : il doit s'agir d'un « *investissement financier, matériel ou humain substantiel* ». Le producteur de la base de données doit avoir opéré des investissements en termes de ressources humaines, techniques et financières importants en vue de sa constitution. Ces notions semblent difficiles à interpréter, l'investissement humain ne devant pas se réduire à un quelconque effort intellectuel, ce qui « *reviendrait à subordonner la protection à l'originalité* »[727], alors que « *l'investissement matériel [se ramène] à l'investissement financier* »[728]. En revanche, sont exclus de la protection du droit *sui generis* les investissements affectés à la création des données[729].

B. La caractérisation de l'investissement substantiel

245- Le droit *sui generis* est fondé sur la protection de l'investissement substantiel. Il convient, donc, d'envisager les conditions permettant d'attester d'un investissement (**1**) avant de s'intéresser à l'étendue du caractère substantiel (**2**).

---

[724] COSTES, L. et al., « Intérêt et objet de cette protection », *Lamy Droit du numérique (Guide*), 3352, 2019.
[725] MALLET-POUJOL, N., « Appropriation de l'information : l'éternelle chimère », *D.*, p. 330.
[726] GAUDRAT, P. et SARDAIN, F., *Traité de droit civil du numérique*, t.1 Droit des biens, Larcier, sept. 2015, n°1085, p. 667.
[727] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique*, *op. cit.*, n°1360, pp. 1058 à 1059.
[728] *Ibid.* ; GAUDRAT, P. et SARDAIN, F., *Traité de droit civil du numérique*, *op. cit*., n°2088, p. 668.
[729] Voir *infra*, n°247.

1. L'existence d'un investissement

246- **Interprétation stricte de l'investissement.** La Cour de Justice des Communautés européennes a défini les conditions de l'investissement dans différents arrêts du 9 novembre 2004[730]. Elle a désormais une « *lecture très stricte* » de la notion d'investissement[731]. Ainsi, il faut que l'obtention, la vérification ou la présentation du contenu de la base attestent un investissement substantiel d'un point de vue qualitatif ou quantitatif. Il convient d'envisager chacune de ses conditions.

247- **Obtention du contenu.** La première condition qui consiste à obtenir le contenu de la base de données est définie comme « *désignant les moyens consacrés à la recherche d'éléments existants et à leur rassemblement dans ladite base. Elle ne comprend pas les moyens mis en œuvre pour la création des éléments constitutifs du contenu d'une base de données* »[732]. Ceci a pour effet d'exclure les éditeurs de logiciel. En effet, ces derniers détiennent des droits sur le logiciel qu'ils ont créé, mais pas sur les données incluses dans ou générées par le logiciel.

Le droit *sui generis* protège les données obtenues et exclut celles qui sont créées par une activité principale[733]. Selon la jurisprudence européenne, l'objectif est de « *stimuler la mise en place de système de stockage et de traitements d'informations existants, et non la création d'éléments susceptibles d'être ultérieurement rassemblés dans une base de données* »[734]. De même, le juge français retient que les données ainsi créées ne peuvent pas être protégées par le droit *sui generis*[735]. En somme, ces données représentent des faits historiques et ne peuvent être ni mises à jour ni modifiées[736]. Échappe donc à la protection du droit *sui generis* « *un nombre croissant de bases de données générées automatiquement par l'intelligence artificielle, les capteurs, l'internet des objets…* »[737]. Les données enregistrées dans la nature, telles que les

---

[730] COSTES, L. et al., « Précisions de la CJCE sur la signification de l'investissement », *Lamy Droit du numérique (Guide)*, 3354, 2019.
[731] MALLET-POUJOL, N., « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *RLDI*, 2013, n°93.
[732] CJCE, 9 nov. 2004, aff. n° C-444/02, *Fixtures Marketing Ltd c/ Organismos Prognostikon agonon podosfairou AE (OPAP)*, préc., §37.
[733] CJCE, 9 nov. 2004, aff. C-203/02, *The British Horseracing Board Ltd e.a. c/ William Hill Organization Ltd.* ; comm., TELLIER-LONIEWSKI, L. et MAURIELLO, P., *LGP*, 2005, n°201, pp. 9 à 11, §31 ; CJCE, *Fixtures Marketing Ltd c/ Organismos Prognostikon agonon podosfairou AE (OPAP)*, préc., §40.
[734] CJCE, 9 nov. 2004, aff. n° C-338/02, *Fixtures Marketing Ltd* c/ *Svenska Spel AB* ; comm., TELLIER-LONIEWSKI, L., et MAURIELLO, P., *LGP*, 2005, n°201, pp. 9 à 11, §24.
[735] Civ. 1ère, 5 mars 2009, n°07-19.734, 07-19.735, aff. *Précom, Ouest France Multimédia c/ Direct annonces*, bull ; note POLLAUD-DULIAN, F., *RTD com.*, 2009, n°4, pp. 724 à 727.
[736] *Ibid.*
[737] CSPLA, *Rapport de la mission sur la réforme européenne du droit sui generis des bases de données*, juill. 2022, p. 64

données des capteurs ou celles issues des observations satellites, sont donc des données créées[738].

Par conséquent, toutes les données créées par des capteurs, produites par des machines agricoles, des dispositifs de l'internet des objets, mais aussi toutes les données résultant de l'intelligence artificielle ou encore les mégadonnées devraient être exclues de la protection. Néanmoins, M. le Professeur M. Leistner tempère le propos en reconnaissant que des données mesurées ou observées peuvent autant être des données obtenues au sens de la directive que des données créées. Cette distinction entre données obtenues au sens de la directive et données créées complexifie la mise en œuvre du droit *sui generis* « *[puisqu'] il est parfois difficile, en pratique, d'identifier l'objet exact de l'investissement, notamment en raison de la concomitance des opérations* »[739]. Ainsi, le CSPLA admet que « *la summa divisio entre données créées et obtenues ne semble plus adaptée au contexte des mégadonnées* »[740]. Une telle limite au droit *sui generis* a pour conséquences d'en exclure les bases de données *spin-off*, c'est-à-dire, « *celles qui sont le coproduit d'une activité principale de création de données* »[741]. De même, « *les bases de données issues d'une source unique, qui est aussi à l'origine des données, seront rarement protégées par le droit sui generis* »[742]. En effet, il faut pouvoir démontrer que l'investissement a permis d'assembler les données dans la base. Cette question est fondamentale désormais pour le développement de l'économie des données dans l'Union européenne. Or, les données qui sont générées par les machines et capteurs agricoles sont certes générées pendant une activité principale, mais elles n'en sont pas la condition nécessaire. Elles peuvent donc être séparées de l'activité principale. L'agriculteur peut en effet exploiter son champ sans l'existence des données et surtout il peut collecter les données d'une autre manière. Par conséquent, dans ce cas, l'investissement dans l'obtention des données pourrait être protégé, à la différence des « *données inhérentes à l'activité de production, nécessaires et simultanées à son accomplissement même* »[743].

De plus, il est difficile de déterminer qui est le « fabricant » de la base de données. De nombreuses personnes peuvent prendre l'initiative et le risque dans le processus de production et de traitement des données et, donc, en revendiquer la propriété. Il pourrait tout aussi bien s'agir du fabricant de la machine que de l'agriculteur qui acquiert cette machine et l'utilise sur

[738] *Ibid.*; HUGENHOLTZ, B., « Against "Data Property" », in ULLRICH H., DRAHOS P. & GHIDINI G. (Eds.), *Kritika : Essays on Intellectual Property* (Vol. 3, pp. 48-71), Elgar, 2018.
[739] CSPLA, *Mission sur la réforme européenne du droit des bases de données*, Note d'étape, avr. 2021, p. 8.
[740] *Ibid.*, p. 17.
[741] *Ibid.*, p. 8.
[742] *Ibid.*
[743] CSPLA, *Mission sur la réforme européenne du droit sui generis des bases de données, op. cit.*, p. 68.

son exploitation. Si celui qui prend l'initiative ou le risque est souvent le fabricant des capteurs, l'agriculteur qui investit dans le matériel, l'utilise et génère les données pourrait également revendiquer un droit de propriété sur ces données[744]. Aussi, l'investissement matériel dans la fabrication des machines et l'internet des objets n'est pas automatiquement valorisé par le droit *sui generis*. Or, la commission avait soulevé dans son évaluation de 2018 que « *les investissements se déplacent de la constitution des bases de données vers la création même des données et leur vérification* »[745].

Un temps, la Commission européenne avait proposé l'adoption d'un droit nouveau du producteur de données. Dans ce cas, le producteur entendu comme « *le propriétaire ou l'utilisateur à long terme du dispositif (le locataire)* » disposerait « *[d'] un droit d'utiliser et d'autoriser l'utilisation de données à caractère non personnel* »[746]. Mais pour certains auteurs, la création d'un nouveau droit sur les données produites ne semblait pas opportune en raison de son empiètement sur le droit *sui generis*. Selon eux, un tel droit poserait différents problèmes d'articulation[747]. Notamment, il aurait pour conséquence de surprotéger les données, de créer des problèmes de concurrence et viendrait en opposition avec l'exception relative à la fouille de textes et de données[748]. Finalement, la Commission européenne avait renoncé à la création d'un nouveau droit en faveur du producteur de données[749]. Le législateur européen a, néanmoins, proposé une nouvelle exception au droit *sui generis* prévu à l'article 35 de la Proposition de règlement sur les données du 23 février 2022 selon laquelle « *les bases de données contenant des données provenant de dispositifs et d'objets de l'internet des objets ne devraient pas faire l'objet d'une protection juridique distincte. Il sera ainsi possible d'y avoir*

---

[744]DERCLAYE, E., « Le marché européen des données. La directive Bases de données est-elle toujours adaptée à l'ère de l'internet des objets ? », *PI*, juill. 2020, n°76, pp. 20 à 32.

[745] CSPLA, *Mission sur la réforme européenne du droit des bases de données*, *op. cit*., p. 17.

[746] Commission européenne, *Créer une économie européenne fondée sur les données*, 10 janv. 2017, COM(2017) 9 final.

[747] HUGENHOLTZ, B., « Against "Data Property" », *op. cit*. « Introducing such an all-empassing property right in Data would seriously compromise the system of intellectual *property law that currently exists in Europe. It would also contravene fundamental freedoms enshrined in the European Convention on Human Rights and the EU Charter, distort freedom of competition and freedom of services in the EU, restrict scientific freedoms and generally undercut the promise of big Data for European economy and society. In sum, it would be a very bad idea* ».

[748] DERLAYE, E., « Le marché européen des données. La directive Bases de données est-elle toujours adaptée à l'ère de l'internet des objets ? », *op. cit.*

[749] Commission européenne, *Créer une économie européenne fondée sur les données*, *op. cit.*, art. 3.5. : « *Droit du producteur de données : il serait possible d'accorder au "producteur de données", c'est-à-dire le propriétaire ou l'utilisateur à long terme du dispositif (le locataire), un droit d'utiliser et d'autoriser l'utilisation de données à caractère non personnel. Une telle approche aurait pour but de clarifier la situation et d'offrir un choix plus étendu au producteur de données, en donnant aux utilisateurs la possibilité d'utiliser leurs données, ce qui contribuerait à libérer les données produites par des machines […]* » ; BENABOU, V.-L., « Essai de prospective juridique sur les modes de valorisation des données : fonds informationnel, droit à la portabilité et dividende de la donnée », ss. dir. G'SELL, F., *Le Big Data et le Droit*, Dalloz, 2020, p. 189.

accès et de les utiliser »[750]. Cet article aura pour conséquence de modifier la directive de 1996, puisque l'article 7 n'aura plus vocation à s'appliquer aux bases de données contenant des données provenant de dispositifs de captation. Par conséquent, le producteur de la base de données ne pourra plus interdire l'extraction ou la réutilisation de ces données, au contraire, il devra permettre aux utilisateurs et aux tiers d'accéder, d'utiliser et de partager les données qu'ils ont générés au moyen des objets connectés. La consécration de la future réforme sur les données devrait mettre un terme à ces hésitations jurisprudentielles et doctrinales quant à la protection des données créées et des données obtenues.

En outre, il faut faire le constat de l'obsolescence, au moins en partie de la directive de 1996, due à l'émergence d'une économie de la donnée[751]. Le CSPLA propose à ce sujet d'apporter des points d'éclairage et de moduler la directive de 1996, notamment au sujet de l'accès aux données d'intérêt général ou essentiel. Ceci afin, d'une part, d'éviter les monopoles des entreprises sur les données, tout en favorisant, d'autre part, l'accès aux bases de données.

248- **Vérification du contenu.** La deuxième condition qui consiste à vérifier le contenu de la base de données s'entend comme « *visant les moyens consacrés, en vue d'assurer la fiabilité de l'information contenue dans ladite base, au contrôle de l'exactitude des éléments recherchés, lors de la constitution de cette base ainsi que pendant la période de fonctionnement de celle-ci* »[752], à l'exclusion « *des moyens consacrés à des opérations de vérification au cours de la phase de création d'éléments par la suite rassemblés dans une base de données* »[753]. Ainsi, la vérification du contenu de la base de données peut participer à démontrer l'investissement du producteur. Cette vérification ne se fait pas nécessairement qu'au jour de la constitution de la base de données, elle peut s'effectuer tout au long de la vie d'une base mouvante, à mesure que des données sont intégrées[754].

249- **Présentation du contenu.** La troisième condition qui consiste à présenter le contenu s'entend comme « *les moyens visant à conférer à ladite base sa fonction de traitement de l'information, à savoir ceux consacrés à la disposition systématique ou méthodique des éléments contenus dans cette base ainsi qu'à l'organisation de leur accessibilité individuelle* »[755].

---

[750] https://www.lexisveille.fr/data-act-la-commission-europeenne-devoile-le-contenu-du-projet-de-reglement-sur-lutilisation-des

[751] CSPLA, *Mission sur la réforme européenne du droit des bases de données*, préc. ; Commission européenne, 10 janv. 2017, *Créer une économie européenne fondée sur les données*, préc.

[752] CJCE, *Fixtures Marketing Ltd c/ Organismos Prognostikon agonon podosfairou AE (OPAP),* préc., §27 ; CJCE, *The British Horseracing Board Ltd e.a. c/ William Hill Organization Ltd*., préc., §42.

[753] CJCE, *The British Horseracing Board Ltd e.a. c/ William Hill Organization Ltd.*, préc., §42.

[754] CA Paris, 2 févr. 2021, n°17/17688, *Le Bon coin*.

[755] CJCE, *Fixtures Marketing Ltd c/ Organismos Prognostikon agonon podosfairou AE (OPAP),* préc., §27

La Cour de justice a interprété les conditions de la présentation du contenu. Aussi, pour démontrer un investissement à ce titre, les informations collectées doivent avoir un caractère indépendant, leur recueil doit être systématique ou méthodique et une fois collectées, elles doivent être accessibles.

Tout d'abord, il est nécessaire que les données collectées et classées dans la base de données soient indépendantes les unes des autres[756]. Ainsi, les cartes topographiques de l'IGN ou les bases de données interconnectées ne semblaient pas pouvoir bénéficier de la protection du droit *sui generis* en raison du croisement des données pour fournir les informations. Néanmoins, la CJUE a précisé que les éléments constitutifs devaient être « *séparables les uns des autres sans que la valeur de leur contenu informatif, littéraire, musical ou autre s'en trouve affectée* »[757]. Ainsi, des données qui peuvent être détachées les unes des autres sans qu'elles s'en trouvent altérées entrent dans la condition d'indépendance des données. La question s'est donc posée auprès de la Cour de Justice de l'Union européenne[758] de savoir si une carte topographique sur papier pouvait constituer une base de données au sens de la directive 96/9. Le fait que la base de données soit constituée sur papier ne posait pas de problème, la directive englobe les recueils de données, « *quelles que soient leurs formes* »[759], électronique ou non électronique[760]. La difficulté provenait du fait qu'indépendamment les unes des autres, les données de la carte topographique perdaient leur valeur informative puisqu'en n'étant plus reliées les unes aux autres, elles ne pouvaient plus « *former une image du territoire* »[761]. Pourtant, le juge a considéré que même une fois extraites, les données conservaient leur valeur informative. Cette décision étend l'application du droit *sui generis* à des bases de données qui de prime à bord ne répondent pas au caractère indépendant du contenu de la base, du moment qu'une fois extraites ces données conservent une valeur informative pour les utilisateurs finaux. Ainsi, le caractère indépendant des données dans une base est démontré dès lors que les données extraites et isolées fournissent des informations à l'utilisateur, et ce, même si c'est le contenu

[756] CJUE, 29 oct. 2015, aff. C-490/14, *Freistaat Bayern c/ Verlag Esterbauer GmbH* ; obs. BERNAULT, C., *LEPI*, 2016, n°25 ; obs. BERNAULT, C., *PI* 2016, n°58, p. 68 ; obs. BENABOU, V.-L., *Dalloz IP/IT*, 2016, p. 89 ; obs. POLLAUD-DULIAN, F., *RTD com*., 2016, p. 125 ; obs. FAVRE, C. et ZOLLINGER, A., *JCP E*, 2016, 1481, n°9.

[757] CJCE, 9 nov. 2004, aff. C-444/02, *Fixtures Marketing Ltd c/ Organismos prognostikon agonon podosfairou AE (OPAP)*, préc. : Rec. CJCE 2004, I, p. 10590 ; *Propr. industr*. 2005, comm. 7, 3e esp., note KAMINA, P. et 22, 1er arrêt, note DERCLAYE, E., pt. 29.

[758] CJUE, 29 oct. 2015, aff. C-490/14, *Freistaat Bayern c/ Verlag Esterbauer GmbH* ; obs. BERNAULT, C., *LEPI*, 2016, n°25 ; obs. BERNAULT, C., *PI* 2016, n°58, p. 68 ; obs. BENABOU, V.-L., *Dalloz IP/IT*, 2016, p. 89 ; obs. POLLAUD-DULIAN, F., *RTD com*., 2016, p. 125 ; obs. FAVRE, C. et ZOLLINGER, A., *JCP E*, 2016, 1481, n°9.

[759] Dir. 96/9/CE, préc., art. 1. 1.

[760] *Ibid.*, consid. 14.

[761] BENABOU, V.-L., « Une carte topographique est une base de données en raison de sa valeur informationnelle, observations sous CJUE, 29 oct. 2015, aff. C490/14, *Freistaat Bayern* c/ *Verlag Esterbauer GmbH* – Qualification de l'arrêt : important », *Dalloz IP/IT*, 2016, p. 89.

global de la base de données qui fournit des informations grâce aux liens entre les données. Par exemple, c'est le cas pour des cartographies géologiques ou encore des cartes topologiques ou des jeux de données interconnectées (des données de parcelles, des données météorologiques et des données du sol).

Ensuite, en ce qui concerne le caractère systématique ou méthodique, le recueil de données ou d'éléments doit être disposé en fonction de critères précis permettant de démontrer l'investissement. La Cour de justice précise là encore que la méthode ou le système mis en œuvre par la base doit permettre « *de retrouver chacun de ses éléments constitutifs* »[762].

Enfin, les données doivent être accessibles. Autrement dit, elles doivent pouvoir être exploitées « *par la mise en place de moyens électroniques ou autres permettant à partir d'un mot clé d'accéder à un des éléments* »[763].

2. L'existence d'un investissement substantiel

250- **Notion de substantialité.** La CJUE est venue apporter quelques précisions sur la notion de substantialité. Elle l'entend de manière large, quelle que soit la forme des bases de données et s'est affranchie de considérations d'ordre formel, technique ou matériel[764]. Il est, d'ailleurs, indifférent que les éléments constitutifs présentent « *un caractère officiel et accessible au public* »[765]. Elle a affirmé également que « *la notion de partie substantielle, évaluée de façon quantitative, du contenu de la base au sens de l'article 7, paragraphe 1, de la directive […] doit être appréciée par rapport au volume du contenu total de celle-ci* » et qu'une « *partie quantitativement négligeable* » du contenu de la base peut représenter un « *important investissement humain, technique ou financier* »[766]. C'est dans le même sens que la Cour de cassation a relevé que la *base annuaire* de France Télécom ne se résout pas à l'annuaire. En effet, elle est enrichie d'autres informations, dont plus de la moitié proviennent de la société France Télécom et ce, de façon à former un ensemble spécifique pour lequel celle-ci a conçu et défini les opérations utiles en leur affectant les moyens correspondants[767].

---

[762] CJCE, 9 nov. 2004, aff. C-444/02, *Fixtures Marketing Ltd c/ Organismos prognostikon agonon podosfairou AE (OPAP),* préc.
[763] TGI Paris, 3e ch., 30 mars 2010, préc.
[764] Dir. 96/9/CE, *op. cit.*, art. 1er; ex. *Fixtures Marketing Ltd c/ Organismos prognostikon agonon podosfairou AE (OPAP),* préc. ; CJCE, 9 nov. 2004, aff. C-444/02, préc. n°46, pt 20.
[765]CJCE, 5 mars 2009, aff. C-545/07, *aff. Apis-Hristovich c/ Lakorda AD* : obs. SIRINELLI, P., *RIDA* 3/2009, p. 415 et p. 389 ; note CARON, C., *CCE* 2009, comm. 44 ; note LARRIEU, J., *Propr. industr.* 2009, comm. 48 ; *RLDI* avr. 2009, 1571 ; obs. SARDAIN, F., *JCP E* 2010, 1070, n°10 ; obs. BENABOU, V.-L., *PI* 2009, p. 383.
[766] CJCE, 9 nov. 2004, aff. C-203/02, préc. n°46, pt. 70 et 71.
[767] Com., 23 mars 2010, n°08-20.427, n°08-21.768 : JurisData n°2010-002593 ; note CARON C., *CCE* 2010, comm. 83, 1re esp. ; *Expertises* 2010, p. 230 ; note BOUCHE N., *Propr. industr.* 2010, comm. 43 ; obs. BRUGUIÈRE J.-M.,

251- Preuve du caractère substantiel. Le caractère substantiel est donc déterminé au cas par cas selon la base de données. Il appartient, d'ailleurs, au producteur qui revendique le bénéfice de la protection de prouver le caractère substantiel de son investissement[768].

II. Le contenu du droit *sui generis*

252- La protection d'une base de données par le droit *sui generis* offre au producteur des droits sur cette base (**A**). Néanmoins, ce droit souffre quelques exceptions (**B**).

A. Les droits du producteur sur la base de données

253- Le producteur de la base de données, qui détient un droit *sui generis* en raison de son investissement, peut interdire l'extraction ou la réutilisation des données contenues dans sa base (**1**). L'étude de ces interdictions suppose d'en étudier l'étendue (**2**).

1. Les interdictions d'extraction ou de réutilisation

254- Droit d'interdire. Le producteur qui obtient la protection par le droit *sui generis* en démontrant la substantialité de l'investissement effectué pour réaliser une base de données bénéficie de divers droits. Ce sont avant tout des droits *d'interdire*. En effet, l'article L. 342-1 du CPI octroie au bénéfice du titulaire le droit d'empêcher « *l'extraction ou la réutilisation non autorisée de la totalité ou d'une partie non substantielle du contenu de la base de données* ».

255- Notions d'extraction et de réutilisation. Il est nécessaire d'expliquer ce qu'on entend par extraction et réutilisation. Pour cela, il faut se référer à la directive de 1996 qui définit l'extraction comme « *le transfert permanent ou temporaire de la totalité ou d'une partie substantielle du contenu de la base de données sur un autre support par quelque moyen ou sous quelque forme que ce soit* »[769]. S'agissant de la réutilisation, le législateur européen l'a définie comme « *toute forme de mise à la disposition du public de la totalité ou d'une partie*

PI 2010, p. 856 ; obs. CASTETS-RENARD C., *RLDI* juill. 2010, n°62, 2030, rejetant le pourvoi contre CA Paris, 1re ch., 30 sept. 2008, préc. n°13.

[768] CA Paris, 4e ch. B, 13 mars 2009 : JurisData n°2009-002638.

[769] Dir. 96/9/CE, préc., art. 7.2 a).

substantielle du contenu de la base par distribution de copies, par location, par transmission en ligne ou sous d'autres formes »[770].

La CJCE a elle aussi effectué un travail de qualification dans ses arrêts précités de 2004 en interprétant l'article 7 de la Directive. Elle a retenu dans son arrêt *The British Horseracing, Board Ltd e. a.,* le principe selon lequel « *les notions d'extraction et de réutilisation au sens de l'article 7 de la directive doivent être interprétées comme se référant à tout acte non autorisé d'appropriation et de diffusion au public de tout ou partie du contenu d'une base de données* »[771]. De même, dans l'arrêt *Football Dataco* du 18 octobre 2012, elle a retenu que la notion de réutilisation devait être interprétée dans un sens large, comme visant « *tout acte non autorisé par le fabricant de la base de données protégée par le droit sui generis qui consiste à diffuser au public tout ou partie de celle-ci* »[772]. La Cour de justice souligne également que « *la reprise d'éléments d'une base de données protégée dans une autre base de données à l'issue d'une consultation de la première base sur écran et d'une appréciation individuelle des éléments contenus dans celle-ci est susceptible de constituer une extraction, au sens de l'article 7* »[773]. Par conséquent, selon Mme N. Mallet-Poujol, par la notion de « transfert », la CJUE « *n'entend pas d'acte matériel de reproduction, mais envisage le résultat final qui fait que l'on retrouve une partie substantielle du contenu de la base sur un autre support d'information* », ce qui peut entraîner « *des difficultés probatoires* ». Néanmoins, ces droits d'interdire ne doivent pas « *porter atteinte aux droits légitimes de l'utilisateur* »[774].

Le droit du producteur de la base de données est emprunté au parasitisme. En effet, selon M. le Professeur M. Vivant, ce droit ne serait « *rien d'autre qu'un droit sur l'investissement dans la filiation directe des constructions jurisprudentielles faites sur le continent pour lutter contre le parasitisme* »[775]. Ainsi, le droit *sui generis* interdit l'extraction ou la réutilisation d'une

---

[770] *Ibid.*, art. 7.2 b).

[771] CJCE, 9 nov. 2004, aff. C-203/02, *The British Horseracing Board Ltd e.a.*, préc.

[772] CJUE, 1er mars 2012, aff. C-173/11 *Football Dataco* : *RLDI* 2012/87, nº 2710, obs. Costes L., *JCP E* 2012, aff. 161, *JCP E* 2012, nº 1489, § 4, obs. VIVANT M., MALLET-POUJOL N. et BRUGUIERE J.-M., *D.* 2012, act. p. 735, D. 2012, 2838, obs. SIRINELLI P., *PI*. 2012, nº 45, p. 421, obs. BENABOU V.-L., *RIDA* 2012, nº 232, p. 487, obs. SIRINELLI P., *CCE* 2012, comm. 47, note CARON C., *Propr. indust*. 2012, comm. 75, note LARRIEU L., pt 19 ; voir comm. VARET E., *in RLDI* 2012/87, nº 2933.

[773] MALLET-POUJOL, N., « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *op. cit.* ; CJCE, 9 oct. 2008, aff. C-304/07, *Directmedia Publishing GmbH c/ Albert-Ludwigs-Universität Freiburg* ; note CARON, C., *CCE*, 2009, nº 3, comm. 24 ; *Légipresse* 2008, nº 256, I, p. 149 ; note BENABOU, V.-L., *PI* 2009, nº 30, p. 77 ; chron. SIRINELLI, P., *RIDA* 2009, nº 219, p. 297.

[774] MALLET-POUJOL, N., « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *op. cit*., 2013, n°93.

[775] VIVANT, M., « L'investissement rien que l'investissement », *op. cit.*, voir MARTIN, N. et LE GAL, C., « Droit des bases de données et parasitisme : un arrêt en demi-teinte de la cour d'appel de Paris », *RDLI*, 2006, n°12, p. 15; VIVANT, M. et BRUGIERE, J.-M., *Droit d'auteur et droits voisins*, *op. cit.*, n°228, p. 264.

partie ou de la totalité de la base de données pendant une durée de quinze ans[776]. Ce droit peut être « *transféré, cédé ou donné en licence contractuelle* »[777]. S'il souffre certes d'exceptions listées à l'article 7 de la directive 96/9, telles que l'extraction non substantielle ou à des fins privées, le producteur de la base de données dispose du droit d'interdire l'accès à celle-ci aux utilisateurs tiers au contrat.

256- **Actions en cessation du trouble.** Afin de faire respecter son droit, le producteur de la base de données peut agir en cessation du trouble. Ces actions confortent l'idée d'un droit d'accès exclusif et privatif à la base de données, comme en témoignent également les sanctions prévues par la loi en cas de non-respect de ces interdictions.

Tout d'abord, la reproduction, la représentation ou la diffusion d'une base de données constituent un délit de contrefaçon sanctionné par l'article L. 335-3 du CPI[778]. Le trouble peut se prouver par tout moyen, toute personne ayant qualité pour agir dispose du droit de « *faire procéder par tous huissiers sur ordonnance rendue sur requête par la juridiction civile compétente, soit à la description détaillée […] soit à la saisie réelle de ces supports* »[779]. La juridiction compétente peut également, aux mêmes fins, ordonner ces mesures afin de rapporter la preuve de la contrefaçon. La juridiction peut aussi ordonner « *toutes mesures d'instruction légalement admissibles, même si une saisie-contrefaçon n'a pas été préalablement ordonnée* »[780]. De même, à la demande de toute personne ayant qualité pour agir dans cette situation des mesures urgentes peuvent être ordonnées par la juridiction compétente afin de prévenir une atteinte aux droits du producteur de bases de données ou à faire cesser le trouble. Ainsi, la sanction civile de l'action en contrefaçon est la saisie-contrefaçon.

Le délit de contrefaçon est sanctionné par trois ans d'emprisonnement et 300 000 euros d'amende. Cette sanction peut être portée à sept ans d'emprisonnement et 750 000 euros d'amende dans le cas où le délit aurait été commis en bande organisée[781]. Concernant les sanctions à l'encontre des personnes morales, elles sont prévues à l'article L. 343-6 du CPI. En cas de récidive les peines sont doublées[782]. Les récidivistes peuvent être privés du droit d'élection et d'éligibilité pour les tribunaux de commerce, les chambres de commerce et d'industrie, territoriales et les chambres de métiers ainsi que pour le Conseil de prud'hommes

[776] CPI, art. L. 342-1.
[777] Dir. 96/9/CE, préc., art. 7.3.
[778] CPI, art. L. 335-3 : « … *est […] un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi* ».
[779] CPI, art. L. 343-1.
[780] CPI, art. L. 343-1-1.
[781] CPI, art. L. 343-4.
[782] CPI, art. L. 343-7, al. 2.

pour une durée qui ne peut excéder cinq ans. Lorsque ce délit a été commis par une personne physique, elle peut être condamnée, à ses frais, « *à retirer des circuits commerciaux les objets jugés contrefaisants et toute chose qui a servi ou était destinée à commettre l'infraction* »[783], ainsi que « *la destruction à [ses] frais ou la remise à la partie lésée des objets et choses retirées des circuits commerciaux ou confisqués, sans préjudice de tous dommages et intérêts* »[784]. Enfin, la juridiction peut ordonner, à ses frais, « *l'affichage ou la diffusion du jugement prononçant la condamnation* »[785]. À la lecture de ces éléments, il apparaît que les sanctions en cas d'atteinte aux droits du producteur d'une base de données sont conséquentes et représentent une véritable limite à l'accès aux données pour les tiers. Elles dissuadent quiconque voudrait accéder à la base de données sans l'autorisation de l'ayant droit.

2. L'étendue de l'extraction ou de la réutilisation

257- **Analyse du caractère substantiel de l'extraction ou de la réutilisation.** L'appréciation de l'interdiction d'extraction ou de réutilisation s'opère en vérifiant le caractère substantiel de la partie de la base de données extraite ou réutilisée. Cette appréciation doit se faire de manière qualitative ou quantitative au sens de l'article L. 342-1 du CPI[786].

Tout d'abord, s'agissant du caractère qualitatif, l'idée est ici de protéger le producteur de la base de données contre l'extraction ou la réutilisation d'une partie qualitativement substantielle. Comme ne manque pas de le relever Mme N. Mallet-Poujol « *ce concept est fort difficile à appréhender en raison de son extrême subjectivité et de sa relativité* »[787]. La jurisprudence a dû fournir une grille de lecture pour déterminer ce qui est *qualitativement* substantiel. Ainsi, dans l'affaire *Cadremploi* contre *Keljob*, la société *Keljob* avait extrait des annonces d'offres d'emploi de la base de données produite par la société *Cadremploi*, dont elle présentait les éléments essentiels aux internautes, pillant ainsi les données produites et intégrées dans la base de données et donc les investissements réalisés par le producteur de cette base. Le Tribunal de Paris se prononçait en faveur de *Cadremploi* en retenant que « *si le contenu des*

[783] CPI, art. L. 343-5, al. 1.
[784] CPI, art. L. 343-5, al. 2.
[785] CPI, art. L. 343-5, al. 3.
[786] CPI, art. L. 342-1, al. 1 : « *L'extraction, par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit » ; CPI, L. 342-1, al. 2 : « La réutilisation par la mise à disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme* ».
[787] MALLET-POUJOL, N., « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *op. cit.*, n°93.

offres n'était pas reproduit, il n'en demeurait pas moins que d'autres éléments qualitativement substantiels (à savoir les éléments essentiels de l'offre : intitulé du poste, secteur d'activité, zone géographique) l'étaient »[788]. L'appréciation du caractère substantiel de l'extraction est donc évaluée au regard de la nature des données extraites[789]. Mais, par la suite, la Cour de justice a affiné son raisonnement dans l'arrêt *The British Horseracing Board Ltd e. a.*. en retenant, qu'« *afin d'apprécier si (les) éléments (en cause) représentent une partie substantielle, d'un point de vue qualitatif, du contenu de la base de données […] il y a lieu d'examiner si les efforts humains, techniques et financiers consentis par la personne qui a constitué la base pour l'obtention, la vérification et la présentation de ces données représentent un investissement substantiel* »[790]. Elle affirme ainsi que « *la notion de partie substantielle, évaluée de façon qualitative, du contenu d'une base de données se réfère à l'importance de l'investissement lié à l'obtention, à la vérification ou la présentation du contenu de l'objet de l'acte d'extraction et/ou de réutilisation, indépendamment du point de savoir si cet objet représente une partie qualitativement substantielle du contenu général de la base de données protégée* ».

Par conséquent, avec ce raisonnement, pour que l'extraction d'une partie qualitative soit retenue, il faut pouvoir démontrer l'existence d'un investissement substantiel, mais non au regard de la valeur des données extraites[791]. De même, la Cour a précisé dans une autre affaire que « *d'un point de vue qualitatif, une telle partie substantielle en ce qu'il représente, en termes d'obtention, de vérification ou de représentation, un important investissement humain, technique ou financier* »[792]. Ce qui compte c'est l'investissement et non « *l'origine ou la nature des données* »[793].

---

[788] VIVANT, M. et BRUGUIERE, J.-M., *Droit d'auteur et droits voisin, op. cit.* ; TGI, Paris, 3ech., 5 sept. 2001, n°00/1796 : JurisData, n°2001-161802 ; obs. MAFFRE-BAUGE A, *JCP G*, 2002, n°73 ; obs. COSTES L., *RLDA*, 2001, n°43, n°2735 ; obs. TELLIER-LONIEWSKI L., *Légipresse*, 2001, n°187, III, p. 219 ; note CARON Ch., *CCE*, 2002, n°2, comm. 16.

[789] MALLET-POUJOL, N., « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *op. cit.*

[790] CJCE, 9 nov. 2004, aff. C-203/02, *The British Horseracing Board Ltd e.a. c/ William Hill Organization Ltd,* préc., pt. 76 ; VIVANT, M., WARUSFEL, B., MALLET-POUJOL, N. et COSTES, L., *Lamy droit du numérique*, mai 2021, n°262.

[791] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique, op. cit.*, n°1413, p. 1094.

[792] MALLET-POUJOL, N., « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *op. cit.* ; Civ. 1ère, 5 mars 2009, *News invest c/ PR Line* : Bull. civ. I, nº 46 ; note CARON C., *CCE* 2009, nº 5, comm. 43 ; obs. DALEAU J., *D.*, 2009, AJ, 948 ; *JCP G* 2009, IV, nº 1570 ; obs. BRUGUIERE J.-M., *PI*, 2009, nº 32, p. 275 ; chron. SIRINELLI P. *RIDA*, 2009, nº 221, p. 491 ; note RAMBAUD S., *RLDI* 2009/49 nº 1572 et *RLDI* 2009/49 nº 1594.

[793] MALLET-POUJOL, N., « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *op. cit.*

D'un point de vue quantitatif, les juges retiennent la notion de *« volume de données extrait et/ou réutilisé de la base et doit être appréciée par rapport au volume du contenu total de celle-ci* »[794]. Il faut donc comparer les deux bases de données pour apprécier « *le caractère quantitativement substantiel de l'extraction* », et ce, même si la base de données a « *un caractère officiel et accessible au public* »[795]. La question ne se pose pas dans le cas où l'intégralité de la base de données est copiée[796]. De même, lorsque l'extraction ou la réutilisation est pratiquée de manière « *répétée et systématique de partie qualitativement ou quantitativement non substantielle du contenu de la base* ». Ainsi, le caractère substantiel n'est pas recherché dès lors que « *ces opérations excèdent manifestement les conditions d'utilisation normale de la base de données* »[797]. La Cour de justice a précisé dans son arrêt *The British Horseracing Board Ltd e. a.* que « *l'objectif de cette disposition est de faire obstacle à des extractions et/ou réutilisations répétées et systématiques de parties non substantielles du contenu d'une base de données qui par leur effet cumulatif, porteraient gravement atteinte à l'investissement de la personne qui a constitué la base, à l'instar des extractions et/ou réutilisations visées par l'article 7, paragraphe 1, de la directive* »[798]. Encore une fois, c'est la protection de l'investissement qui est recherchée. La notion de réutilisation a aussi fait l'objet d'une précision par la Cour de justice. Effectivement, cette dernière retient une approche extensive de la notion de réutilisation[799] en la définissant comme « *tout acte, non autorisé par le fabricant de la base de données protégée par ce droit sui generis, qui consiste à diffuser au public tout ou partie du contenu de celle-ci* »[800]. Elle renvoie notamment à « *tout acte consistant […] à mettre à la disposition du public, sans le consentement de la personne qui a constitué la base de données, les résultats de son investissement* »[801].

[794] CJCE, 9 nov. 2004, aff. C-203/02, *The British Horseracing Board Ltd e.a.,* préc., pt 70.
[795] MALLET-POUJOL, N., « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *op. cit.* ; Civ. 1ère, 5 mars 2009, préc.
[796] CA Montpellier, 3e ch. corr., 2 juin 2015, JurisData n°2015-028856.
[797] CPI, art. L. 342-2 ; MALLET-POUJOL N., « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *op. cit.*
[798] CJCE, 9 nov. 2004, aff. C-203/02, *The British Horseracing Board Ltd e.a,* préc., pt 86.
[799] LUCAS, A., LUCAS-SCHLOETTER, A. et BERNAULT, C., *Traité de la propriété littéraire et artistique, op. cit.,* n°1409, p. 1092 ; GRYNBAUM, L., LE GOFFIC, C. et MORLET-HAÏDARA, L., *Droit des activités numériques, op. cit.,* n°699, p. 489.
[800]CJCE 9 nov. 2004, aff. Jtes C-203/03, C-444/02, C-46/02 et C-338/02, *CCE* 2005, comm. 2, C-203/02, Rec. p. I-10415, pts 45, 46, 51 et 67, CARON, C. ; *RTD com.* 2005, 90, obs. POLLAUD-DULIAN, F.
[801] *Ibid.* pt 51.

B. Les exceptions au droit *sui generis*

258- Le droit *sui generis* des bases de données n'est pas illimité. Il existe des exceptions au droit exclusif du producteur bénéficiant à l'utilisateur légitime de la base de données. Elles figurent à l'article L. 342-3 du CPI et renvoient pour certaines aux exceptions du droit d'auteur. Aussi, les exceptions spécifiques au droit *sui generis* et celles communes avec celles du droit d'auteur seront étudiées ici. Il faut donc envisager l'extraction ou la réutilisation d'une partie non substantielle (**1**), l'extraction à des fins privées (**2**), la consultation par des personnes handicapées (**3**), la consultation à des fins pédagogique ou de recherche (**4**) et la fouille de texte pour la recherche scientifique (**5**). Il ne faut pas oublier, toutefois, que le droit *sui generis* ne peut pas être invoqué par l'État quand il s'agit de données publiques[802].

1. L'extraction ou la réutilisation d'une partie non substantielle

259- L'article L. 342-3, al. 1er du CPI dispose que le producteur ne peut interdire « *l'extraction ou la réutilisation d'une partie non substantielle, appréciée de façon qualitative ou quantitative, du contenu de la base, par la personne qui y a licitement accès* ». Ainsi, l'utilisateur légitime peut « *procéder, pour des besoins propres, à des extractions et/ou réutilisations non substantielles* »[803]. Le fait que le texte précise que toute clause contraire est nulle interdit au titulaire du droit d'interdire par contrat ce que la loi permet[804]. Cette exception ne bénéficie qu'à l'utilisateur légitime, ce qui implique que « *cette liberté d'extraire et de réutiliser des parties non substantielles ne bénéficie qu'à celui qui accède licitement à la base* »[805]. Or, l'accès est licite lorsqu'il « *est offert à chacun ou autorisé par le contrat* »[806]. Ainsi, l'article L. 342-3 précise « *[qu'] est nulle toute clause par laquelle le producteur prétendrait limiter cette liberté d'extraire et de réutiliser des parties non substantielles* ». Toutefois, lorsque la base de données ne répond pas aux conditions de la protection du droit *sui generis,* le producteur de la base est libre de limiter contractuellement l'accès à la base sur le fondement de la liberté contractuelle[807].

---

[802] Voir *supra*, n°120.
[803], VIVANT, M., WARUSFEL, B., MALLET-POUJOL, N. et COSTES, L., *Lamy droit du numérique*, 2021, n°264.
[804] *Ibid.*
[805]BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique*, *op. cit.*, n°1424, p. 1102.
[806] *Ibid.*
[807] Voir *infra*, n°306 et s. ; CJUE, 15 janv. 2015, n° C-30/14, *Ryanair Ltd* c/ *PR Aviation BV* : *JurisData* n°2015-002578 ; obs. SIRINELLI, P., *RIDA*, 2015/2, p. 319 et p. 301 ; obs. LAMBRECHT, M., *Auteurs et medias*, 2015, p.

2. L'extraction à des fins privées

260- L'article L. 342-3, 2e du CPI prévoit que le titulaire des droits ne peut interdire « *l'extraction à des fins privées d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données non électronique sous réserve du respect des droits d'auteurs ou des droits voisins sur les œuvres ou éléments incorporés dans la base* ». Cette exception ne concerne que les bases de données non électroniques[808]. Aussi, elle ne vaut que pour les bases de données papier. En revanche, il n'est pas possible d'extraire pour des fins privées des données d'une base électronique. Cette interdiction repose sur l'article L. 122-4 du CPI qui dispose que « *toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite. Il en est de même pour la traduction, l'adaptation ou la transformation, l'arrangement ou la reproduction par un art ou un procédé quelconque* ». Ceci se justifie par le fait qu'il est plus facile d'extraire ou de reproduire des données issues d'une base de données électroniques que d'une base de données sur support papier[809].

3. La consultation par des personnes handicapées

261- L'article L. 342-3, 3e du CPI prévoit que le producteur ne peut interdire « *l'extraction et la réutilisation d'une base de données dans les conditions définies au 7e de l'article L. 122-5, au 1e de l'article L. 122-5-1 et à l'article L. 122-5-2* ». Cette exception est née de la loi DADVSI du 1er aout 2006 qui a permis de faciliter l'accès aux œuvres par les personnes atteintes d'un handicap[810]. Aussi, l'article L. 122-5, 7e du CPI énonce cette exception pour les œuvres d'art et l'article L. 342-3e du CPI l'a reprise pour les bases de données.

181 ; obs. BERNAULT, C., *PI*, 2015, n°55, p. 211 ; obs. CASTETS-RENARD, C., *RLDI*, mars 2015, n°3685 ; note LARRIEU, J., *Pr. Industr*., 2015, comm. 71.

[808] MALLET-POUJOL, N., « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *op. cit.*

[809] *Ibid.*

[810] *Ibid.*

4. La consultation à des fins pédagogique ou de recherche

262- La loi DADVSI du 1er aout 2006 a également autorisé la consultation des bases de données à des fins pédagogique ou de recherche à l'article L. 342-3, 4e du CPI[811]. De sorte que le savoir et la connaissance doivent continuer à prospérer. M. le Professeur B. Warusfel commente à ce sujet que « *ni la propriété intellectuelle, ni la protection sui generis européenne ne confère, en elle-même, au producteur de la base ou à d'autres ayants-droits, la possibilité d'imposer des restrictions à l'usage intellectuel et scientifique des données* »[812]. En revanche, Mme N. Mallet-Poujol note une exception en faveur de l'édition électronique puisque les bases de données pédagogiques sont exclues du jeu de l'exception[813].

263- L'ordonnance du 24 novembre 2021 est venue remanier l'article L. 122-5 du CPI en distinguant la finalité d'illustration à des fins d'enseignement désormais prévu aux articles L. 122-5, 12° et L. 122-5-4 du CPI et l'exception d'illustration de recherche scientifique. Cette dernière exception est maintenue à l'article L. 122-5, 3° du CPI et est « *conçue pour répondre aux besoins de reproduction puis de diffusion des œuvres protégées lors des cours ou conférences en présence ou à distance qu'elles permettent d'illustrer ou encore pour la conception des sujets d'examen, etc.* »[814]. Cette exception n'a pas pour finalité de reproduire et de diffuser les bases de données à des fins de recherche. Toutefois, l'exception du droit *sui generis* contenue à l'article L. 342-3, 4° du CPI semble plus adaptée à la finalité de reproduction et de diffusion des bases de données à des fins de recherche puisqu'elle prévoit « *que, lorsque la base de données a déjà été mise à la disposition du public, le titulaire du droit sui generis ne peut interdire l'extraction et la réutilisation d'une partie substantielle du contenu de la base lorsque celui-ci est utilisé à des fins strictement pédagogiques et de recherche* ». Cette exception ne vaut toutefois qu'à condition, « *que le public auquel cette extraction et cette réutilisation sont destinées [soit] composé majoritairement de chercheurs directement concernés, que la source [soit] indiquée, que l'utilisation de cette extraction et cette réutilisation ne donnent lieu à aucune exploitation commerciale et qu'elle [soit] compensée par une rémunération négociée sur une base forfaitaire* »[815].

---

[811] *Ibid*.
[812] WARUSFEL, B., « La protection des bases de données en question : un autre débat sur la propriété intellectuelle européenne », *PI*, n°13, 2004, p. 903.
[813] MALLET-POUJOL, N., « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *op. cit.*
[814] ROBIN, A., *Droit des données de la recherche, op. cit*., n°186, p. 144.
[815] CPI, art. L. 342-3, 4°.

5. La fouille de textes et de données

264 **Définition de la fouille de textes**. L'exception de *Text and Data Mining* permet de « *libérer les incitatives et les technologies en facilitant l'accès spécialement au bénéfice des chercheurs* »[816]. La fouille de textes et de données est définie comme « *toute technique d'analyse automatisée visant à analyser des textes et des données sous une forme numérique afin d'en dégager des informations, ce qui comprend, à titre non exhaustif, des constantes, des tendances et des corrélations* »[817]. Elle est codifiée à l'article L. 342-3, 5° du CPI pour le droit *sui generis* et à l'article L. 122-5, 10° du même code pour le droit d'auteur. Ces deux articles renvoient à l'article L. 122-5-3 du CPI.

L'exception de fouille de textes (*Text and Data Mining – TDM*) est une exception *ad hoc* qui permet notamment d'autoriser la fouille de textes à des fins de recherche. Le TDM consiste en un processus technique d'extraction des données, de transformation par l'ajout de métadonnées, de stockage et de production de résultats.

L'exception de TDM ne concernait à l'origine que la recherche publique. Cette exception permet aux chercheurs de fouiller des textes et des données inclus ou associés aux écrits scientifiques pour les besoins de la recherche publique à l'exclusion de toute finalité commerciale[818]. C'est l'article 38 de la loi n°2016-925 du 7 octobre 2016 pour une République numérique qui a introduit l'exception d'exploration et de fouille de textes au 10° de l'article L. 122-5 du CPI. Ce texte est d'interprétation stricte, il « *ne peut servir que la seule recherche publique à l'exclusion de toute finalité commerciale* »[819]. La LRN a également ajouté l'article L. 342-3 du CPI visant l'exception de fouille de textes à destination de la recherche scientifique pour les « *données incluses ou associées aux écrits scientifiques* » qui cette fois-ci s'adresse à toute la recherche et non pas seulement à celle qui est publique[820]. Ces articles ont été introduits « *en raison de l'existence potentielle de droits de propriété intellectuelle sur les bases de données* »[821].

---

[816] LATREILLE, A., « La fouille de textes et de données à l'épreuve de la propriété intellectuelle », *CDST*, 2017.
[817] Dir. n°2019/790 du 17 avr. 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE : *JOUE* L 130 du 17 mai 2019, p. 92, art. 2.
[818] ROBIN, A., « Les données scientifiques au prisme du dispositif *Open Data* », *op. cit.* ; CPI, arts. L. 122-5, 10e et L. 342-3, 5e.
[819] CARON C., « République numérique rime avec exceptions et limitations en droit d'auteur, Commentaires », *CCE*, nov. 2016.
[820] *Ibid.*
[821] ROBIN, A, « Les données scientifiques au prisme du dispositif *Open Data* », *op. cit.*

La directive 2019/790 du 17 avril 2019, retranscrite dans le CPI par l'ordonnance du 24 novembre 2021[822], va au-delà des simples actes de fouille[823]. Elle autorise au titre de l'article 3, le stockage des copies des données issues de la fouille dès lors qu'il est réalisé « *avec un niveau de sécurité approprié* » et qu'il a lieu « *à des fins de recherche scientifique* ». En dehors de la recherche scientifique, l'article 4 prévoit désormais la possibilité de conserver des reproductions ou des extractions « *aussi longtemps que nécessaire aux fins de la fouille de textes et de données* ». Le texte français n'autorisait que les actes de reproduction au sens du droit d'auteur et d'extraction au sens du droit *sui generis* des bases de données[824]. De même, la directive ne limite plus la fouille de textes à la recherche publique[825], l'article 4 de la directive prévoit une exception « générale » au droit des bases de données, désormais « *toute personne est susceptible de pouvoir en bénéficier* ». Aussi, l'ordonnance du 24 novembre 2021 est venue modifier l'exception de TDM en créant l'article L. 122-5-3 du CPI. Cet article définit, en son premier alinéa, l'exception de fouille de textes et de données comme « *la mise en œuvre d'une technique d'analyse automatisée de textes et données sous forme numérique afin d'en dégager des informations, notamment des constantes, des tendances et des corrélations* ».

265- **Régimes des exceptions de TDM.** Il existe ainsi désormais deux régimes applicables à l'exception de TDM.

Dans la première hypothèse, l'article L. 122-5-3, II, du CPI prévoit que l'exception s'applique de plein droit à des fins de recherche scientifique. L'objectif est *« [d'] analyser de grandes séries de données et contenus, auxquelles [les chercheurs] ont légalement accès, à des fins scientifiques et de recherche* »[826]. Aussi, l'auteur ou le producteur de la base de données ne peut pas retirer son consentement. Les bénéficiaires de cette exception sont les organismes de recherche et les institutions du patrimoine culturel, du moment qu'ils accèdent de manière licite[827] aux bases de données. Aux termes de l'article 2, la directive entend par « organismes

[822] Ord. n°2021-1518 du 24 nov. 2021 complétant la transposition de la directive 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE : *JORF* n°0274 du 25 nov. 2021.

[823] ALLEAUME, C. et MARTIN, D., « La directive 2019/790 sur le droit d'auteur dans le marché numérique », *RJC*, juill./août 2019, num. 4.

[824] CARRE, S. et MACREZ, F., « Les ambivalences du copyright européen dans la construction du marché unique numérique », *Europe* n°7, ét. 6, juill. 2020.

[825] ALLEAUME, C., « Les exceptions en faveur de l'enseignement et de la recherche scientifique, Commentaire des articles, 3 et 5 de la directive », *CCE*, n°10, oct. 2019.

[826] CASTETS-RENARD, C., « Marché unique numérique : la Commission européenne présente les premières mesures en droit d'auteur », *D.*, 2016. p. 388.

[827] L'accès licite s'entend au sens du cons. 14 de la dir. 2019/790, préc., comme « *couvrant l'accès à des contenus fondé sur une politique de libre accès ou en vertu d'arrangements contractuels entre, d'une part, les titulaires de droits et, d'autre part, les organismes de recherche ou les institutions du patrimoine culturel, comme des abonnements, ou en vertu d'autres voies légales. Par exemple, les personnes rattachées à un organisme de recherche ou à une institution du patrimoine culturel qui a souscrit des abonnements à certains contenus sont*

de recherche » : les universités, y compris les bibliothèques, les instituts de recherche ou autre entité, dont l'objectif premier est la recherche scientifique ou l'exercice d'activités éducatives comprenant également des travaux de recherche scientifique. Ces recherches doivent être menées dans un but non lucratif et dans le cadre d'une mission d'intérêt public reconnue par l'État. Toutefois, cette exception n'est pas applicable « *lorsqu'une entreprise, actionnaire ou associée de l'organisme ou de l'institution diligentant les fouilles, dispose d'un accès privilégié à leurs résultats* »[828], ce qui limite l'application de l'exception et oblige « *à évaluer le degré d'autonomie structurelle et décisionnaire de l'organisme public de recherche concerné* »[829]. Également, les copies et les reproductions effectuées dans le cadre de l'exception de TDM sont stockées avec un niveau de sécurité approprié et peuvent être conservées à des fins exclusives de recherche scientifique, y compris pour la vérification des résultats de la recherche[830]. Ainsi, comme le prévoyait déjà la directive, les mesures de sécurité ne doivent pas excéder ce qui est nécessaire pour atteindre l'objectif de fouille de textes et de données. En outre, l'article prévoit que les organismes et institutions visés au II du texte et les organisations représentatives des titulaires des droits sur les bases de données doivent s'accorder pour définir les bonnes pratiques relatives à la mise en œuvre des dispositions légales. Par conséquent, l'exception de TDM doit permettre aux chercheurs de procéder aux techniques de fouille de textes et de données « *plus facilement et avec une plus grande sécurité juridique* ». Enfin, la directive de 2019 prévoit que les États peuvent envisager une contrepartie financière pour les titulaires des droits[831] seulement en ce qui concerne l'utilisation des œuvres et autres objets protégés dans le cadre d'activité d'enseignement numérique et transfrontière. Mais elle est expressément rejetée « *pour les titulaires de droits en ce qui concerne les utilisations relevant des exceptions en matière de fouille de textes et de données* »[832]. Le législateur européen considère en effet que « *le préjudice potentiel* » est « *minime* » puisque l'exception est limitée à la recherche scientifique.

Dans la seconde hypothèse, il s'agit d'une exception générale de fouille de textes et de données reconnue à toute personne, quelle que soit la finalité. Pour cela, le bénéficiaire de l'exception doit avoir accès de manière licite aux données. Néanmoins, cette exception est supplétive de volonté, le titulaire des droits peut s'opposer à la fouille de textes et de données par un système d'*Opt out* en la limitant ou en l'interdisant expressément, conformément aux

réputées bénéficier de l'accès licite à ces abonnements. L'accès licite devrait également désigner l'accès à des contenus librement accessibles en ligne ».

[828] CPI, art. L. 122-5-3, II.

[829] ROBIN, A., *Droit des données de la recherche, op. cit*., n°203, p. 158.

[830] CPI, art. L. 122-5-3, II.

[831] Dir. n°2019/790, préc., art. 5.4.

[832] *Ibid.*, cons. 17.

articles 3 et 4 de la directive. Ainsi, le bénéficiaire n'a accès aux données que s'il a un accès licite et « *dans la mesure où les titulaires de droits n'ont pas réservé de manière appropriée les droits de reproduction et d'extraction pour la fouille de textes et de données* »[833]. Le titulaire des droits peut donc s'y opposer, notamment par des procédés lisibles par machine pour les contenus mis à la disposition du public[834], ou utiliser des mesures techniques, des métadonnées, le prévoir contractuellement ou par une déclaration unilatérale[835]. Enfin, les copies et reproductions doivent, ici encore, être stockées avec un niveau de sécurité approprié. Elles doivent ensuite être détruites à l'issue de la fouille de textes et de données.

266. **Conclusion de la section.** Les acteurs de l'agriculture numérique collectent les données agricoles et peuvent les intégrer dans des bases de données. Dès lors qu'elles revêtent un caractère original ou que leur fabrication a nécessité un investissement significatif, les acteurs peuvent obtenir un droit de propriété intellectuelle sur ces bases. Elles font alors l'objet d'une réservation privative. En revanche, le droit des bases de données n'influe pas sur le régime applicable aux données incluses dans la base. La réforme du droit des bases de données engagée par le législateur européen dans la Proposition de règlement sur les données de 2022 devrait, toutefois, exclure les données industrielles obtenues au moyen d'objets connectés ou de service lié de la protection des bases de données.

Section 2. Les effets sur l'organisation de l'accès aux bases de données protégées

267. La directive 96/9 a pour objectif de protéger les auteurs et les producteurs contre les extractions et les réutilisations du contenu des bases de données. À l'origine cette directive devait harmoniser la protection des bases de données dans l'Union européenne, encourager l'investissement dans ces bases et préserver l'équilibre entre les droits et les intérêts des producteurs et des utilisateurs. Aussi, la Commission européenne avait déjà pris en compte l'importance de la circulation des données et souhaitait éviter un « verrouillage » de l'accès aux informations contenues dans les bases de données. Cette protection était donc nécessaire pour sécuriser les investissements. Cependant, avec l'évolution des technologies, elle ne devrait plus aujourd'hui s'appliquer à l'ensemble de l'économie fondée sur les données[836]. En effet, les

[833] *Ibid.*, cons. 18.
[834] CPI, art. L. 122-5-3, III.
[835] CASTETS-RENARD, C., « Marché unique numérique : la Commission européenne présente les premières mesures en droit d'auteur », *op. cit.*
[836] CHATRY S., « Droits *des producteurs de* bases de données », *J.-Cl. Propr. litt. et art.*, fasc 1650, 2018, n°1.

données générées par des machines, des dispositifs de l'internet des objets, des mégadonnées ou encore par l'intelligence artificielle devraient être exclues du champ d'application de la protection des bases de données. Les observateurs attendaient, en ce sens, une réforme de la directive, au vu des « *évolutions technologiques matérialisées par la montée en puissance des objets et des services connectés* »[837]. Or, si la Commission européenne avait annoncé, une telle réforme dans les évaluations de 2005[838] et de 2018[839], elle a finalement procédé en insérant un article 35 relatif au droit *sui generis* dans sa Proposition de règlement des données, *Data Act* de 2022[840]. Aussi, pour prendre en compte l'évolution du contexte depuis la directive de 1996, la Commission européenne est en voie de réformer le droit *sui generis* des bases de données dans le sens d'un assouplissement du droit au bénéfice des utilisateurs d'objets connectés ou de services liés et des tiers. Or, les acteurs de l'agriculture numérique détiennent de très nombreuses bases de données qui contiennent des données industrielles. Par conséquent, si l'accès n'était jusqu'alors réservé qu'à l'utilisateur légitime de la base de données, la Commission européenne en proposant un assouplissement du droit *sui generis*, le rendrait inapplicable aux utilisateurs d'objets connectés et aux tiers.

Dans l'attente de cette réforme, il faut, tout d'abord, constater que le droit des bases de données n'organise qu'une indisponibilité relative des données pour les tiers (**§1**). En revanche, dès lors que l'utilisateur légitime a accès au contenu de la base de données par un moyen licite, les données sont par principe disponibles pour lui (**§2**).

§1. *L'indisponibilité relative des données pour les tiers*

268- Malgré les exceptions au droit d'auteur et au droit *sui generis*, les bases de données ne sont en principe accessibles qu'aux utilisateurs qui se soumettent à la licence d'exploitation[841]. Par conséquent, les tiers n'ont pas accès aux données incluses dans une base. En principe, donc, le contenu de la base de données est réservé au titulaire des droits (**I**). Néanmoins, le droit organise l'accès aux bases de données pour les tiers en matière de concurrence et s'apprête à autoriser,

---

[837] CSPLA, *Rapport de la mission sur la réforme européenne du droit sui generis des bases de données*, juill. 2022, p. 8.
[838] DG *Internal Market And Services Working Paper, First evaluation of Directive 96/9/EC on the legal protection of databases*, 12 déc. 2005.
[839] Com. Staff working document, *Evaluation of Directive 96/9/EC on the legal protection of databases* {SWD(2018) 147 final}, 25 avr. 2018, p. 15.
[840] *Ibid.*
[841] Voir *infra*, n°274.

grâce à la Proposition de règlement sur les données, l'accès aux bases contenant des données provenant de dispositifs et de l'internet des objets (**II**).

I. Le principe de la réservation du contenu de la base pour le titulaire des droits

269- Le droit des bases de données permet au producteur de réserver les données qui sont incluses dans la base (**A**). Aussi, il sera nécessaire de développer les effets de cette appropriation (**B**).

A. La réservation des données incluses dans les bases

270- Si la reconnaissance de la réservation du contenu de la base de données a fait l'objet d'une évolution législative (**1**), il a été, finalement, reconnu que la base permet une appropriation indirecte des données (**2**).

1. L'évolution législative sur la réservation du contenu de la base de données

271- Une position confuse du législateur dans la directive 96/9. L'article 3.2 de la directive 96/9 prévoit que « *la protection des bases de données par le droit d'auteur prévu par la présente directive* ***ne couvre pas leur contenu*** »[842] [nous soulignons]. À la lecture de cet article, il apparaît que le législateur a voulu protéger seulement le contenant dans l'originalité de la composition des matières. Cependant, l'article 7 de cette même directive dispose au sujet du droit *sui generis* des bases de données que « *les États membres prévoient pour le fabricant d'une base de données le droit d'interdire l'extraction et/ou la réutilisation de la totalité ou d'une partie substantielle, évaluée de façon qualitative ou quantitative du* ***contenu*** *de celle-ci* » [nous soulignons]. Cette formulation a été reprise à l'article L. 342-1 du CPI. M. le Professeur C. Alleaume relève ainsi que « *les législateurs européens et français n'ont pas vraiment su départir (mais le pouvaient-ils) les bases de données (entendues comme un contenant) et les données (le contenu)* »[843]. M. le Professeur M. Vivant relève également l'ambiguïté de la loi à ce sujet : le droit *sui generis* serait une « *protection du contenu, c'est-à-dire non plus de l'agencement, mais des données elles-mêmes (au moins des données réunies)* »[844]. De ce fait,

[842] Dir. 96/9/CE, préc., art. 3.2.
[843] ALLEAUME, C., « Á propos de la propriété des données agricoles… », *Droit rural*, n°469, dossier 2, janv. 2009, p. 7.
[844] VIVANT, M. et BRUGUIERE, J.-M., *Droit d'auteur et droits voisins*, Dalloz, 4e éd., 2019, n°152, p. 199.

« *pour la première fois l'information comme telle, devient bien direct (et non point indirect) d'un droit, et d'un droit qui n'est pas loin d'être privatif* »[845]. Aussi, l'appréciation qualitative de l'extraction des données démontre la volonté « *de rendre indisponible une information brute* »[846]. Mme la Professeure M. Clément-Fontaine soutient aussi cette thèse en reconnaissant une appropriation indirecte des données[847].

2. L'appropriation indirecte des données

272- La capacité d'interdire l'extraction et la réutilisation du contenu d'une base de données a pour conséquence de conserver un monopole sur les données. C'est ce qui permet à M. le Professeur C. Alleaume d'affirmer « *[qu'] elles permettent aux producteurs (ceux qui ont assumé le risque des investissements substantiels, etc.) d'avoir une maîtrise monopolistique du "contenu" de leurs bases de données, c'est-à-dire des données elles-mêmes ! Or, de la maîtrise monopolistique protégée par la loi au droit de propriété, il n'y a qu'un pas…* »[848]. Mais les exceptions prévues par la directive pour l'accès à la base de données ne sont possibles que dans la mesure où la personne a accès à la base. Or, pour avoir accès à cette base, encore faut-il avoir accepté les conditions contractuelles[849]. Les exceptions au droit *sui generis* sont, alors, théoriques s'agissant des tiers.

B. Les effets d'appropriation des bases de données

273- La maîtrise monopolistique des bases de données s'étend aux données elles-mêmes (**1**). Néanmoins, il ne s'agit pas pour autant d'une reconnaissance d'un droit de propriété sur les données (**2**).

---

[845] VIVANT, M., « An 2000 : l'information appropriée ? », *Mélanges offerts Jean-Jacques Burst*, Litec, 1997, p. 657 ; MALLET-POUJOL, N., « La directive concernant la protection juridique des bases de données : la gageure de la protection privative », *DIT*, 1, 1996, p. 5.
[846] VIVANT, M. et BRUGUIERE, J.-M., *ibid.*
[847] CLEMENT-FONTAINE, M., « De l'exclusion des idées (Propriété intellectuelle. Principes généraux) in VIVANT M., ss. dir., *GAPI.*, préf. JESTAZ Ph., Dalloz, 2015, p. 69 : « *Les enjeux économiques qui entourent le sort des idées sont à l'origine de la création de régimes spéciaux… l'adoption du régime sui generis des producteurs de base de données a permis l'appropriation indirecte des données ou informations brutes en vue de protéger l'investissement* ».
[848] ALLEAUME, C. « Á propos de la propriété des données agricoles… », *op. cit.*
[849] *Ibid.*

1. La maîtrise monopolistique des bases de données étendue aux données elles-mêmes

274- La question de l'appropriation des bases de données a fait l'objet d'études doctrinales[850]. Le droit de propriété est exclusif dans le sens où il a un caractère individuel. Ainsi, le propriétaire dispose d'un monopole sur le bien, il a le droit d'user de la chose, d'en récolter les fruits et d'en disposer comme il le souhaite. Il peut exercer seul toutes les prérogatives du droit de propriété dans la limite des lois et des règlements. En l'occurrence, en présence d'une base de données, ces prérogatives s'étendent aux données elles-mêmes. En effet, le fabricant de la base de données dispose des pleins pouvoirs sur le contenu, même si les données sont régies par une loi ou un règlement particulier — tel que les données personnelles, les données publiques ou les données de santé. À condition de respecter les dispositions légales particulières, le titulaire des droits sur la base peut transformer, supprimer, diffuser les données qui y sont contenues. Il peut également disposer de la base de données, en la louant, la vendant ou encore en octroyant des licences d'utilisation aux utilisateurs, etc.

2. Le maintien de l'absence de droit de propriété sur les données

275- Certains auteurs ont pu retenir, à la lumière de la jurisprudence, que le producteur d'une base de données obtenait un véritable droit de propriété sur les données. Pour affirmer cela, ils s'appuient sur la décision du Conseil constitutionnel du 5 aout 2015 à propos de la loi pour la croissance, l'activité et l'égalité des chances économiques[851] dont l'article 60 impose aux greffiers des tribunaux de commerce de transmettre à l'INPI les données relatives aux registres des sociétés. Des députés et sénateurs ont contesté la conformité à la Constitution de cet article considérant qu'il portait atteinte, entre autres, au droit de propriété. Le Conseil constitutionnel a estimé qu'il n'y avait pas d'atteinte au droit de propriété « *eu égard à la nature de ces données et dès lors que ne sont pas en cause les éventuelles bases de données élaborées dans le cadre de leur exploitation privée* »[852]. D'aucuns ont, sur la base de cette décision, considéré qu'*a contrario* « *une obligation de communication de base de données constituées dans le cadre*

---

[850] MALLET-POUJOL, N., *La commercialisation des banques de données, contribution à une approche juridique des richesses informationnelles*, dir. LAMBERTERIE, I. (de), CNRS éd., 1992 ; WARUSFEL, B., « La protection des bases de données en question : un autre débat sur la propriété intellectuelle européenne », *PI*, oct. 2004, n°13, pp. 896 à 906 ; MICHAUX, B., « La cour de justice favorise-t-elle l'appropriation des données par celui qui les a traitées ? », note ss CJUE, 2e ch., aff. n° C-490/14, 29 oct. 2015, *Auteurs & Media*, n°1, pp. 28 à 34.

[851] Loi n°2015-990 du 6 août 2015 pour la croissance, l'activité et l'égalité des chances économiques : *JORF* n°0181 du 7 août 2015.

[852] Cons. constit., déc. n°2015-715 DC, 5 août 2015 : *JORF* n°0181 du 7 août 2015, cons. n°107.

d'une activité privée serait regardée comme une atteinte au droit de propriété »[853]. Néanmoins, cette analyse est de toute évidence dévoyée. Il s'agissait seulement de confirmer que l'obligation de transmettre des données, même contenues dans une base de données, ne pouvait pas porter atteinte au droit de propriété. Et ceci s'expliquait par le fait qu'il n'existe tout simplement pas de droit de propriété sur les données[854]. C'est d'ailleurs, ce qu'a retenu le Conseil d'État dans un arrêt du 12 juillet 2017, au sujet de ce même article 60 de la loi pour la croissance, l'activité et l'égalité des chances économiques. Cette fois, le Conseil national des greffiers des tribunaux de commerce avait lui-même contesté ledit article. Il soutenait que le décret portait atteinte au droit de propriété garanti par la Constitution. Le Conseil d'État rejette cet argument en précisant, tout comme l'avait fait le Conseil constitutionnel, que les dispositions ne portent pas atteinte au droit de propriété. Le Conseil d'État fonde sa décision sur le fait que les données ne sont pas « *des biens dont il puisse revendiquer la propriété* »[855]. Au vu de ces éléments, il apparaît que les juges ne soutiennent pas l'existence d'un droit de propriété sur les données contenues dans une base. Cependant, le droit *sui generis* offre au producteur de la base un droit de propriété sur les bases de données qu'il produit. Déjà en 2006, le Conseil constitutionnel[856] reconnaissait que le droit d'auteur et les droits voisins relevaient du droit de propriété[857]. Aussi, même si « *la directive 96/9/CE n'emploie pas directement l'expression de droit de propriété* »[858], il est acquis que le droit *sui generis* s'apparente à un droit de propriété sur la base. Le fabricant d'une base de données dispose donc de droits d'une grande amplitude qui lui octroient de fait les mêmes attributs qu'un propriétaire sur les données elles-mêmes.

II. Les limites externes à la réservation des bases de données

276- Des limites à l'appropriation des bases de données peuvent se trouver, tout d'abord, dans la réforme du droit des bases de données (**A**), ensuite dans le droit de la concurrence (**B**).

---

[853] CYTERMANN, L., « Rapport relatif aux données d'intérêt général », *op. cit.*, p. 43. *A contrario*, CYTERMANN, L., « Le partage des données, un enjeu d'intérêt général à l'ère de l'Intelligence artificielle », *Rev. Aff. eur.*, 2018/1, pp. 65 à 72.

[854] L'auteur du rapport relatif aux données d'intérêt général a changé de point de vue et a adopté une vision similaire.

[855] CE, 6e et 1e ch. réunies, 12 juill. 2017, n°397403, rec.

[856] C. constit., déc. n°2006-540 DC, 27 juill. 2006, cons. 15 : « *Les conditions d'exercice du droit de propriété ont subi depuis 1789 une évolution caractérisée par une extension de son champ d'application à des domaines nouveaux ; que, parmi ces derniers, figurent les droits de propriété intellectuelle et notamment le droit d'auteur et les droits voisins* ».

[857] CYTERMANN, L, Maitre des requêtes au CE, « Rapport relatif aux données d'intérêt général », *op. cit.*, p. 42.

[858] *Ibid.*

A. La future consécration de l'exclusion des données industrielles de la protection par le droit *sui generis*

277.- La Commission européenne propose dans sa future réforme du droit *sui generis* d'annihiler les possibilités de réservation par le producteur des bases contenant des données issues d'objets connectés ou de services liés. Pour cela, elle envisage l'ouverture de l'accès et souhaite permettre l'utilisation du contenu de la base aux utilisateurs d'objets connectés (**1**), mais aussi aux tiers (**2**).

1. L'ouverture de l'accès pour les utilisateurs d'objets connectés

278.- L'article 7 de la directive 96/9 prévoit que le fabricant de la base de données peut interdire l'extraction et/ou la réutilisation des données contenues dans sa base à toute personne qui n'est pas un utilisateur légitime[859]. Cependant, la Commission européenne réduit la portée de cet article à travers plusieurs dispositions[860]. Notamment, elle propose d'exclure les bases de données contenant des données obtenues ou générées par l'utilisation d'un produit ou d'un service lié de la protection du droit *sui generis* des bases de données à l'article 35 de la Proposition de règlement sur les données de 2022[861]. Par conséquent, elle pose le principe selon lequel l'utilisateur d'un objet connecté ou d'un service lié, qui possède ou loue un produit ou reçoit un service, puisse accéder aux données générées par l'utilisation qu'il fait de ces produits et services et qu'il ait le droit de les utiliser[862]. Le producteur de la base de données ne pourra donc plus s'opposer à l'extraction ou la réutilisation des bases de données pour les utilisateurs d'objets connectés ou de services liés.

2. L'ouverture de l'accès pour les tiers

279.- En neutralisant l'article 7 de la directive 96/9, la Commission européenne ne se contente pas d'autoriser l'accès à la base et de rendre utilisables les données aux seuls utilisateurs d'objets

---

[859] Voir *infra*, n°284 et s.
[860] Voir *supra*, n°258 et s.
[861] Art. 35 de la Proposition de règlement sur les données prévoit que « *afin de ne pas entraver l'exercice du droit des utilisateurs d'accéder aux données et de les utiliser conformément à l'article 4 du présent règlement ou du droit de partager ces données avec des tiers conformément à l'article 5 du présent règlement, le droit "sui generis" prévu par l'article 7 de la directive 96/9/CE ne s'applique pas aux bases de données contenant des données obtenues ou générées par l'utilisation d'un produit ou d'un service lié* ».
[862] Proposition de Règl. du 23 fèvr. 2022 fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), COM(2022) 68 final, 2022/0047(COD), art. 4.

connectés, mais bien à tous les tiers à la licence d'exploitation. Ainsi, « *dès lors qu'une base de données contiendra des données générées au moyen d'objets connectés, le producteur ne pourra plus en interdire l'accès* »[863]. L'article 5 de la Proposition de règlement propose en effet que le détenteur des données mette à disposition d'un tiers les données générées par l'utilisation d'un produit ou d'un service lié sur demande de l'utilisateur. L'objectif poursuivi de cette proposition est clairement de réduire la portée du droit *sui generis* et de faire en sorte que « *ces données ne puissent être appropriées par le producteur de la base de données, et par suite [qu'elles] demeurent sur le marché des données* »[864] et qu'elles puissent circuler.

B. L'impact du droit de la concurrence sur la réservation des bases de données

280- Si le droit *sui generis* des bases de données permet au producteur d'organiser une réservation privative, le droit de la concurrence peut au contraire imposer l'ouverture de l'accès de celles-ci. Aussi, lorsque deux corps de textes de même valeur s'appliquent à une même situation, il est nécessaire de faire la balance entre les deux textes afin de connaître leur articulation. En effet, sur le plan concurrentiel, le refus discriminatoire d'accès à une base de données d'une entreprise en position dominante sur le marché à un concurrent peut constituer un abus de position dominante sanctionné par le droit de la concurrence. Dans un tel cas, la base de données peut être ouverte afin de rééquilibrer le jeu de la concurrence au mépris des règles du droit de la propriété intellectuelle. Aussi, afin de constater un abus de position dominante, il faut dans un premier temps envisager les marchés bifaces du secteur de l'agriculture numérique (**1**) pour, dans un second temps, étudier les effets d'un abus de position dominante (**2**).

1. Les marchés bifaces dans l'agriculture numérique

281- Définition. Le marché biface est « *l'architecture des services fournis par les acteurs du numérique* »[865]. Le caractère biface du marché est pris en compte par la Commission européenne, la DGCCRF et l'Autorité de la concurrence[866] pour analyser les effets concurrentiels sur un marché[867]. Les marchés bifaces sont définis comme des « *marchés au sein desquels une ou plusieurs plateformes permettent des interactions entre des utilisateurs finaux*

[863] CSPLA, *op. cit.*, p. 26
[864] CSPLA, *op. cit.*, p. 31.
[865] LENOIR, N., « Le droit de la concurrence confrontée à l'économie du *Big Data* », *AJCA*, févr. 2016.
[866] REY, P., « L'approche économique des marchés "biface" », *RLC*, n°35, 1er avr. 2013.
[867] Voir *supra*, n°187.

et essayent de développer les deux (ou multiples) faces du marché en appliquant un tarif approprié à chacune d'elle […]. Un marché est biface si la plateforme peut influer sur le volume des transactions en faisant payer un prix plus élevé à une face du marché et en réduisant le prix payé par l'autre côté pour une quantité équivalente »[868]. Une décision de l'Autorité de la concurrence n°11-D-11 du 6 juillet 2011 caractérise le marché biface « *par des externalités de réseau croisées entre deux populations (les deux faces), par lesquels l'utilité procurée par l'usage d'un bien (ou d'un service) à un individu d'une population dépend du degré d'usage des individus de l'autre population* »[869]. Le marché biface est donc composé de deux populations qui interagissent au travers d'une plateforme sur laquelle les utilisateurs rencontrent des fournisseurs. Il faut donc des « *externalités positives* » et la « *symétrie des externalités que chaque face exerce sur l'autre* »[870].

282- Dans le secteur de l'agriculture numérique, des sociétés se sont positionnées sur les activités de collecte et de partage des données des exploitants agricoles créant de ce fait des marchés bifaces ou multifaces. Par exemple, la société *Wiuz* est une plateforme ouverte grâce à l'interconnectivité avec d'autres outils internes et externes et vise toutes les coopératives et tous les opérateurs issus ou non du monde agricole. Il s'agit d'une plateforme qui propose des services différents sur deux faces de marchés[871]. D'une part, *Wiuz* crée des partenariats avec d'autres opérateurs de l'agriculture numérique afin de toucher un grand nombre d'agriculteurs dans l'objectif de rassembler sur une même plateforme l'ensemble des données agricoles. *Wiuz* propose en sus aux agriculteurs de faciliter la gestion administrative de leur exploitation grâce à un mode de saisie simplifié et d'intégrer automatiquement les données dans les documents réglementaires. L'agriculteur peut, également, grâce à la plateforme, accéder à l'ensemble des données de son exploitation. D'autre part, la plateforme propose un système ouvert de partage des jeux de données agronomiques afin qu'un grand nombre de développeurs puissent y accéder dans l'objectif de développer de nouvelles applications et promouvoir de nouveaux usages. Aussi, les utilités que les développeurs peuvent retirer des services de la plateforme Wiuz dépendent du nombre d'agriculteurs utilisant ladite plateforme sur l'autre face du marché. Ainsi, la plateforme présente des effets de réseaux croisés[872].

---

[868] ROCHET, J.-C. et TIROLE, J., « Two sided markets : An overview », *The Economics of Two-Sided Markets* 12 mars 2004, p. 2.
[869] REY, P., *op. cit.*
[870] *Ibid.*
[871] ROBIN, A., « Les places de marché en ligne. Définitions et distinctions », *J.Cl., comm.*, fasc. 825, oct. 2019.
[872] *Ibid.*

De même, la société *AgDatahub* propose une plateforme d'échange de données agricoles, API-AGRO, sur laquelle l'ensemble des opérateurs de l'agriculture numérique sont amenés à partager leurs bases de données. D'un côté, les entreprises, les instituts de recherche, les instituts techniques agricoles ou d'autres organismes publics proposent l'accès à leurs bases de données au moyen de la plateforme et forment un premier groupe de population en proposant leurs services. De l'autre côté, une seconde population, parmi laquelle les agriculteurs, les consommateurs ou les concurrents souhaitent accéder aux données mises en ligne. Ainsi, la plateforme API-AGRO propose d'une part un écosystème pour le partage des bases de données, d'autre part, elle permet aux utilisateurs de la plateforme d'accéder à ces données, moyennant parfois paiement.

2. La caractérisation de l'abus de position dominante sur le marché biface

283- En position de domination sur un marché biface, une entreprise peut se retrouver en situation d'abus susceptible d'être sanctionné par les autorités de la concurrence. En effet, la « *nature biface des marchés peut […] engendrer de fortes barrières à l'entrée, car les plateformes qui ont émergé les premières profitent d'une spirale de croissance et sont plus attractives que les suivantes* »[873]. Pour caractériser un abus de position dominante[874], une position dominante de l'entreprise sur le marché doit être caractérisée. Ensuite, il faut démontrer l'exploitation abusive de cette position. Enfin, cet abus de position dominante doit avoir pour objet ou pour effet de restreindre la concurrence sur le marché. « *Cet abus doit […], être de nature à éliminer toute concurrence actuelle ou potentielle sur un marché dérivé* »[875]. C'est ainsi que les juges communautaires ont retenu que le refus d'accorder une licence d'utilisation pouvait être constitutif d'un abus de position dominante[876]. Pour cela trois conditions cumulatives doivent être réunies. D'abord, le refus doit faire obstacle à l'apparition d'un produit nouveau pour lequel il existe une demande potentielle de la part des consommateurs. Ensuite, le refus ne doit pas être justifié par des considérations objectives. Enfin, le refus doit être de nature à exclure toute concurrence sur un marché dérivé.

Aussi, en 2015, l'Autorité de la concurrence a sanctionné la société *Google* sur ce fondement parce qu'elle utilisait « *son positionnement sur le marché des services de recherche générale afin de profiter d'un effet de levier en promouvant ses propres services (comparateurs*

[873] *Ibid.*
[874] Voir *supra*, n°200.
[875] ROBIN, A., « Les places de marché en ligne. Responsabilité », *J.Cl com.*, fasc. 827, oct. 2019, n°70.
[876] CJUE, 29 avr. 2004, aff. C-418/01, *IMS Health GmbH & Co. OHG.*

de prix de Google Shopping) au détriment des services de ses concurrents »[877]. Ainsi, il ne suffit plus de rechercher les parts de marché pour savoir s'il y a abus de position dominante. L'autorité de la concurrence s'est intéressée aux effets de réseaux dans l'arrêt *Booking.com* qui aboutissent « *à la création des positions fortes liées à un phénomène de concentration autour d'acteurs dominants, voire très dominants* »[878]. Lorsque de nombreuses plateformes desservent plusieurs types d'utilisateurs, c'est ce que l'on appelle couramment les « marchés multi-faces », ils peuvent « *donner lieu à un type particulier d'effet de réseau, dans lequel les externalités dépendent de la consommation des agents "compatibles" sur la face opposée du marché* »[879]. Parfois il peut se produire un phénomène appelé le « basculement », lorsqu'un fournisseur croît beaucoup plus vite que ses concurrents parce qu'il a acquis un avantage initial sur eux. Dès lors, des fournisseurs peuvent se retrouver avec de grandes parts de marché, ce qui peut avoir des effets d'éviction. Dans ce cas, le refus d'accès à une base de données peut être considéré comme un effet d'éviction discriminatoire. L'Autorité de la concurrence a dû se prononcer dans deux décisions quant au verrouillage du marché lorsque les sociétés refusaient l'accès à leur base de données pour des raisons discriminatoires. En effet, dans la décision du 8 juillet 2014[880], la société Cegedim a été sanctionnée pour son refus de fournir un accès à sa base de données OneKey aux clients de la société Euris. Or, ce refus constitue un « traitement discriminatoire »[881], puisqu'il a « *fait perdre toute possibilité de se développer sur le marché des logiciels de gestion […] les laboratoires qui utilisaient ou étaient intéressés par la solution logicielle ne pouvaient accéder à la base de données leader du marché et se sont, par conséquent, détournés d'Euris* »[882]. En revanche, l'Autorité de la concurrence ne retient pas la théorie des facilités essentielles pour ces bases de données, mais relève le caractère discriminatoire du refus d'accès pour qualifier l'abus de position dominante. Il y a donc un effet d'éviction des sociétés concurrentes. De même, dans l'affaire *GDF/Suez*, l'Autorité de la concurrence a retenu que la société GDF/Suez se mettait en situation de position dominante en profitant des « *informations sur ses abonnés au gaz en tant qu'opérateur historique astreint à des tarifs réglementés afin de promouvoir ses offres de marché de gaz et d'électricité, par exemple en proposant à certains clients une offre duale comportant le gaz au tarif réglementé*

[877] LENOIR, N., « Le droit de la concurrence confrontée à l'économie du Big Data », *op. cit.* ; T. com. Paris, 31 janv. 2012, n°2009061231.
[878] Aut. conc., déc. n°15-D-06, 21 avr. 2015, pt. 112.
[879] *Ibid.*
[880] Aut. conc., déc. n°14-D-06, 8 juill. 2014 relative à des pratiques mises en œuvre par la société *Cegedim* dans le secteur des bases de données médicales, *AJCA*, 2014. 332, obs. I. Luc.
[881] LENOIR, N., « Le droit de la concurrence confrontée à l'économie du *Big Data* », *op. cit.*
[882] Aut. conc., décis. n°14-D-06 du 8 juill. 2014, préc.

et l'électricité au tarif du marché »[883]. Cette base représente « *de facto presque l'ensemble des ménages eu égard à l'ancienne position de monopole de l'entreprise* » et elle « *n'était donc pas reproductible par les concurrents* »[884]. Ceci octroyait « *un effet potentiel d'éviction des opérateurs alternatifs nouveaux entrants, qui ne disposent pas des moyens nécessaires pour prospecter la clientèle sur un pied d'égalité* »[885].

À l'heure actuelle, *a priori*, aucune entreprise de l'agriculture numérique n'a pris l'ascendant sur le marché des données agricoles en France, de sorte que pour le moment aucun abus de position dominante ne peut être caractérisé. En effet, le marché de l'agriculture numérique est relativement récent et ne cesse de croître depuis le milieu des années 2010, il est passé de 9,58 milliards de dollars en 2017 au niveau mondial à une estimation de 23,4 milliards de dollars en 2022[886]. La plateforme Wiuz a été lancée en 2016 et ne fonctionne pas seule, elle nécessite des partenariats avec d'autres acteurs afin d'échanger entre différents outils et services connectés pour faire circuler les données. Cette plateforme n'a donc pas pour objet ou pour effet de limiter le marché, mais au contraire de faciliter les échanges de données. En ce qui concerne la plateforme API-AGRO, la société AgDatahub, qui a créé cette plateforme, a été désignée comme l'un des sept projets phares du programme européen Gaia-X[887], avec pour objectif d'équiper les 10 millions d'exploitations européennes[888]. Elle propose des solutions technologiques et des services aux filières agricoles parmi lesquelles se trouve cette plateforme créée en 2019. Aussi, en accédant à cette position, la société AgDatahub pourrait se trouver en position de domination sur le marché et en limiter l'entrée à ses concurrents. La plateforme API-AGRO pourrait répondre aux caractéristiques de l'infrastructure essentielle et être considérée comme une « contrôleuse d'accès » au sens du DMA en raison de l'avance qu'elle a prise sur l'agglomération des bases de données du secteur agricole. Toutefois, cette dernière ne compte, pour le moment, que peu d'inscrits et peu de bases de données, ce qui l'exclut de la définition des « contrôleurs d'accès »[889]. Par conséquent, il ne semble pas que sa position soit dominante sur le marché. Dans le futur, néanmoins, si tel était le cas, le droit de la concurrence sanctionnerait le refus discriminatoire d'accès aux bases de données qu'elle détient. En tant que « contrôleuse d'accès », elle ne pourra alors refuser l'accès de son infrastructure à ses concurrents qui souhaiteraient pénétrer le marché pertinent du moment que l'infrastructure n'est

[883] LENOIR, N., « Le droit de la concurrence confrontée à l'économie du *Big Data* », *op. cit.*
[884] *Ibid.*
[885] Aut. Conc., 9 sept. 2014, n°14-MC-02, *GDF c/ Suez*.
[886] https://lesillon.fr/lagriculture-numerique-en-quelques-chiffres-cle/
[887] Voir *infra*, n°498
[888]https://www.larevuedudigital.com/partage-de-donnees-agricoles-les-premieres-applications-en-france/
[889] Voir *infra*, n°497.

pas interchangeable et qu'il n'existe pas d'alternatives viables[890]. Les concurrents potentiels se trouveraient alors exclus du marché.

§2. *La pleine disponibilité des données pour l'utilisateur légitime*

284- L'utilisateur légitime de la base de données doit avoir un accès licite à cette base (**I**). Ainsi, le contrat permet d'organiser l'accès aux bases de données (**II**).

I. L'accès licite aux bases de données protégées

285- Il convient d'envisager, tout d'abord, l'organisation de l'accès aux bases de données (**A**), pour envisager ensuite, les modalités de l'accès (**B**).

A. L'organisation de l'accès aux bases de données protégées

286- En principe, seul l'utilisateur légitime (**1**) peut obtenir la mise à disposition de la base de données (**2**).

1. L'obtention de l'accès pour l'utilisateur légitime

287- **Notion d'« utilisateur légitime ».** La directive 96/9, ainsi que la directive 2001/29 (DADVSI)[891], dite société de l'information, définissent la notion de l'« utilisateur légitime ». Il s'agit « *[d]es bénéficiaires qui disposent d'un accès licite à l'œuvre protégé* »[892]. Cependant, un doute subsiste sur cette notion. En effet, le caractère licite de l'accès n'a pas été explicité par la jurisprudence. Ainsi, trois acceptions peuvent être évoquées, il peut s'agir de « *tout utilisateur pouvant se prévaloir d'une exception prévue par la loi ou le contrat* », ou bien « *du seul utilisateur titulaire d'une licence d'utilisation* », ou encore « *de l'utilisateur ayant légitimement acquis la base de données par des moyens qui ne se limitent pas à l'obtention d'une licence (prêt, don, vente, revente, location, héritage…)* »[893]. *A minima*, il faut retenir que dès

[890] ROBIN, A., « Les places de marché en ligne. Responsabilité », *op. cit.*, n°70.
[891] Dir. 2001/29/CE, 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information (DADVSI) : *JOCE* L 167 du 22 juin 2001.
[892] FERAL-SCHUHL, C., ss. dir., *Cyberdroit*, *op. cit.*, n°314.41, p. 827.
[893] CSPLA, *Rapport de la mission sur la réforme européenne du droit sui generis des bases de données*, juill. 2022, p. 14.

lors que le titulaire du droit sur la base de données a décidé de mettre à disposition d'un utilisateur sa base, soit en ligne soit par une autre forme de distribution, la personne qui souscrit à la licence devient un utilisateur légitime. Par conséquent, il doit « *pouvoir accéder à la base de données et l'utiliser aux fins et de la manière prescrite dans le contrat de licence conclu avec le titulaire du droit* »[894].

Il est à noter que parfois la loi détermine les utilisateurs légitimes d'une base de données en prévoyant légalement les personnes qui pourront avoir accès à la base. Par exemple, les systèmes nationaux d'information génétique des espèces bovine, ovine, caprine et porcine, sont accessibles aux personnes définies à l'article 5 de l'arrêté du 16 janvier 2019[895].

288- **Future exception au droit d'interdire l'accès.** Comme il a été étudié plus haut, la proposition de règlement *Data Act* présentée le 23 février 2022 aura pour effet d'exclure du champ d'application du droit *sui generis*, les « *données provenant de dispositifs et d'objets de l'internet des objets* »[896]. Ainsi, les utilisateurs d'objets connectés bénéficieront d'un accès de principe aux données qu'ils auront générées par leur activité et qui seront organisées dans une base de données. Les agriculteurs pourront donc avoir accès aux données générées par les objets connectés qu'ils utilisent sur leur exploitation, les producteurs de bases de données ne pourront plus leur opposer leurs droits d'extraction et de réutilisation[897].

2. La mise à disposition de la base de données

289- **Droit d'auteur.** Au titre de l'article L. 122-7 du CPI, les droits exclusifs de représentation et de reproduction détenus par l'auteur sur sa base de données peuvent être cédés à titre gratuit ou onéreux. Ainsi, l'auteur d'une base de données peut céder ses droits au moyen d'un contrat qui devra nécessairement être constaté par écrit[898]. L'auteur est également en mesure de déterminer la façon dont son œuvre sera exploitée. Il peut aussi décider qui peut exploiter sa base de données et il peut contrôler la distribution de son œuvre à des personnes non autorisées[899].

290- **Droit *sui generis*.** Le titulaire du droit sur la base de données peut décider de mettre à disposition « *une copie de sa base de données, soit par un service en ligne, soit par une autre*

[894] Dir. 96/9/CE, préc., cons. 34.
[895] Arrêté, 16 janv. 2019 relatif aux systèmes nationaux d'information génétique des espèces bovine, ovine, caprine et porcine : *JORF* n°0015, 18 janv. 2019.
[896]https://www.lexisveille.fr/data-act-la-commission-europeenne-devoile-le-contenu-du-projet-de-reglement-sur-lutilisation-des
[897] Voir *supra*, n°247.
[898] CPI, art. L. 131-2.
[899] Dir. 96/9/CE, préc., cons. 30.

forme de distribution »[900]. Cette mise à disposition au public n'a pas pour effet d'épuiser ses droits lorsque la base de données est mise en ligne puisqu'il s'agit d'une prestation de services[901]. L'alinéa 3 de l'article 7 de la directive retranscrit à l'article L. 342-1, al. 4 du CPI prévoit que le titulaire des droits sur une base de données peut disposer de ses droits d'extraction et de réutilisation sur la base de données. En effet, ces droits peuvent être transmis, cédés ou faire l'objet d'une licence non exclusive[902]. Ainsi, le producteur de la base de données doit décider de mettre à disposition sa base de données. Cet acte de disposition s'opère au moyen d'une licence afin de permettre l'accès à la base aux utilisateurs. C'est seulement à cette condition que l'utilisateur devient légitime.

B. Les modalités de l'accès aux bases de données de l'agriculture numérique

291- **Licences d'utilisation.** Pour connaître les modalités d'accès aux bases de données de l'agriculture numérique, il faut se référer aux licences d'utilisation que nous avons pu étudier. En analysant les licences contractuelles des bases de données, il s'avère que trois modèles d'accès se dégagent. Le premier, concerne les bases de données publiques, telles que les bases de données produites par l'INSEE qui sont totalement ouvertes au public. Ensuite, l'accès à certaines bases de données nécessite de souscrire un abonnement ou de faire une demande d'accès auprès de l'auteur ou du producteur afin d'obtenir une autorisation d'accès aux données qui se fera au moyen de *login* et mot de passe. Cet accès demeure gratuit, mais est conditionné à une demande préalable. C'est sur ce modèle que le Système Professionnel d'Information en Élevage géré par l'association SPIE[903] est formaté, ou encore s'agissant des accès aux outils des CUMA. Enfin, les entreprises privées (SMAG, Phytosol, Ekylibre…) ont des modèles-propriétaires conditionnant l'accès à leurs bases de données au paiement d'un abonnement.

II. Le contenu des licences d'utilisation

292- Le contrat prévoit des droits pour l'utilisateur légitime de la base de données (**A**) ainsi que des obligations pour le producteur de la base (**B**).

---

[900] *Ibid.*, cons. 34.
[901] *Ibid.*, cons. 33.
[902] LE TOURNEAU, Ph., *Contrats informatiques et électroniques,* Dalloz référence, 9e éd., 2016, n°343.42, p. 546.
[903] Arrêté du 5 mars 2012, agréant le gestionnaire du système d'information de l'élevage : *JORF* n°0094 du 20 avr. 2012, p. 7110.

A. Les droits de l'utilisateur légitime

293- Il convient d'envisager le contenu des droits de l'utilisateur légitime (**1**) avant de s'intéresser aux limites (**2**).

1. Le contenu des droits de l'utilisateur légitime

294- Effets de l'utilisation d'une licence. C'est la directive 92/100/CE du 19 novembre 1992 qui régit la location et le prêt d'une base de données[904]. Aussi, dès lors qu'un contrat de licence est conclu, l'utilisateur légitime dispose des mêmes droits que le titulaire des droits. Il s'agit d'un droit en pleine propriété. Il contracte en même temps un abonnement de mise à jour[905]. En outre, « *le contrat doit prévoir l'intensité de l'obligation de l'auteur ou du producteur que ce soit quant à la qualité du service et quant aux données proposées (fiables, récentes, complètes, etc.)* »[906].

295- Étendue des droits de l'utilisateur légitime d'une base de données. Dans le cadre du droit *sui generis*, l'utilisateur légitime qui dispose d'un accès licite au contenu de la base « *peut effectuer tous les actes qui sont nécessaires […] à l'accès au contenu de la base de données et à son utilisation normale par lui-même* » et cela « *sans l'autorisation de l'auteur de la base* »[907]. Ces droits ne peuvent s'appliquer qu'à une partie de la base de données et non pas à son intégralité[908]. L'utilisateur légitime bénéficie de ces mêmes droits dès lors que le producteur de la base la met à la disposition du public. Dans le cadre du droit d'auteur, l'utilisateur légitime peut « *extraire et/ou réutiliser des parties non substantielles de son contenu, évaluées de façon qualitative ou quantitative, à quelques fins que ce soit* »[909].

2. Les limites aux droits de l'utilisateur légitime

296- Concernant, tout d'abord, le droit *sui generis*, il existe certaines limites aux droits de l'utilisateur légitime. Il « *ne peut pas effectuer des actes qui sont en conflit avec l'exploitation normale de cette base, ou qui lèsent de manière injustifiée les intérêts légitimes du fabricant de*

---

[904] *Ibid.*
[905] LE TOURNEAU, Ph., *Contrats informatiques et électroniques, op. cit.*, n°343.00 s.
[906] *Ibid.*
[907] Dir. 96/9/CE, préc., art. 6.
[908] *Ibid.*, art. 6, al. 1.
[909] *Ibid.*, art. 8, al. 1.

la base »[910]. De même, il ne peut pas « *porter préjudice au titulaire d'un droit d'auteur ou d'un droit voisin portant sur des œuvres ou des prestations contenues dans cette base* »[911]. Ensuite, s'agissant du droit d'auteur, les droits de l'utilisateur légitime ne peuvent causer un préjudice injustifié aux intérêts légitimes du titulaire du droit ou porter atteinte à l'exploitation normale de la base de données[912].

B. Les obligations du producteur sur la base de données

297- Tout d'abord, il est nécessaire d'envisager l'obligation prétorienne d'interdiction qui incombe au producteur de la base de données (**1**) puis son contenu (**2**).

1. Une obligation prétorienne

298- Limitation de l'utilisation de la base. La possibilité d'interdire l'extraction et/ou la réutilisation du contenu de la base de données a été limitée par les juges qui ont imposé une obligation aux producteurs de bases de données. En effet, dans un arrêt de la Cour d'appel de Versailles du 18 novembre 2004, sur la base des articles 6.1 et 8 de la directive, les juges du fond ont décidé que « *l'incrimination pénale […] suppose donc que le producteur qui se dit lésé ait préalablement interdit l'extraction du contenu de sa base de données faute de quoi cette dernière ne disposera pas de la protection instaurée par la disposition pénale citée* »[913]. Par conséquent, le titulaire des droits sur la base de données doit interdire expressément l'extraction du contenu de sa base de données dans la licence contractuelle.

2. Le contenu de l'obligation d'interdire l'utilisation de la base

299- Jurisprudence. Dans un arrêt du 6 septembre 2005[914], la Cour de cassation a repris les arguments selon lesquels le producteur de la base de données doit expressément interdire l'extraction des données dans le contrat de licence : « *le producteur d'une base de données doit donc mentionner, dans les différents contrats et sur chacun des supports de diffusion, les limites d'utilisation du contenu de sa base de données* »[915]. La CJUE a, elle aussi, eu l'occasion de se

---

[910] *Ibid.*, art. 8, al. 2.
[911] *Ibid.*, art. 8, al. 3.
[912] *Ibid.*, art. 6, al. 3.
[913] Versailles, 9e ch., 18 nov. 2004, *Rojo R…* c/ *Guy R…*, *RLDI* 2005/2, n°50, p. 21, note COSTES, *RLDI* 2005/2, n°50, p. 21.
[914] Crim. 6 sept. 2005, *RLDI*, 2005/19, n°279, p. 18, note COSTES.
[915] FERAL-SCHUHL,, C., SS. dir., *Cyberdroit, op. cit.*, n° 341.43.

prononcer sur une affaire similaire, dans l'arrêt du 9 novembre 2004 selon lequel « *la circonstance que le contenu de la base de données [ait] été rendu accessible au public par la personne qui l'a constituée ou avec son consentement n'affecte pas le droit de cette dernière d'interdire des actes d'extraction et/ou de réutilisation portant sur la totalité ou sur une partie substantielle du contenu d'une base de données* »[916]. Par conséquent, le producteur d'une base de données doit limiter l'utilisation de sa base et interdire les extractions et/ou la réutilisation du contenu s'il veut pouvoir se prévaloir de la protection. Il faut noter également qu'aucune clause contraire aux articles 6.1 et 8 de la directive ne peut être stipulée. Ces articles sont d'ordre public, toute clause contraire serait donc nulle et non avenue. En revanche, il ne peut interdire de manière globale l'extraction et la réutilisation au titre de l'article L. 342-3, 1e du CPI. Toute clause contraire serait également nulle[917]. Le producteur d'une base de données peut donc prévoir l'accès à sa base par le moyen d'un contrat dans lequel il doit limiter l'utilisation du contenu de sa base.

300- **Modèle de clause.** Pour donner un exemple de clause concernant l'utilisation des données contenues dans la base, il est possible de la formuler ainsi : « *La propriété intellectuelle des bases de données visées à l'article X et des informations qu'elles contiennent appartiennent exclusivement à la société Z. Sauf accord particulier entre les parties, le souscripteur s'engage à n'utiliser celles-ci que pour ses besoins propres et à ne pas en faire directement d'exploitation commerciale. Il se porte garant du respect de cette clause par toute personne qu'il a autorisée à consulter ces bases. Dans tous les cas, le souscripteur s'engage à : ne pas utiliser ou ne pas interroger les bases pour le compte ou au profit d'autrui ; ne pas reproduire en nombre à des fins lucratives des informations obtenues par la consultation des fichiers ; ne pas recopier les informations sur des supports de toute nature permettant de reconstituer tout ou partie des fichiers d'origine. En cas d'utilisation frauduleuse du système, la société Z pourra suspendre l'accès du souscripteur aux bases de données* »[918].

301- **Conclusion de la section.** Les acteurs du secteur agricole qui produisent ou créent des bases de données peuvent limiter l'accès à leurs bases aux seuls utilisateurs légitimes au moyen de licences d'utilisation. Néanmoins, la future réforme du droit *sui generis* devrait garantir l'accès, *ex ante*, aux bases de données contenant des données provenant d'objets connectés ou de service

[916] CJUE, 9 nov. 2004, *The British Horseracing Board, Ltd a. c/ William Hill Organization Ltd,* préc. ; VIVANT M., « L'investissement, rien que l'investissement », *op. cit.*, n°104, p. 41., FERAL-SCHUHL C., SS. dir., *Cyberdroit, op. cit*., n°341.43.
[917] CPI, art. L. 342-3, 2e.
[918] BERTRAND, A., « Droit d'auteur », *Dalloz action*, 2010, n°201.39.

lié aux utilisateurs et aux tiers. De même, un accès *ex post* peut être garanti en faveur des concurrents en cas d'abus de position dominante. Cette possibilité est néanmoins théorique s'agissant du secteur agricole puisqu'il ne semble pas, pour l'heure, qu'un des acteurs ait acquis une position dominante sur le marché.

302- **Conclusion du chapitre.** Le législateur protège le producteur ou le créateur d'une base de données agricoles puisque celui-ci peut réserver l'accès aux seuls utilisateurs qui auront accepté les conditions d'accès. Ceci réduit considérablement l'accessibilité et la circulation des données contenues dans ces bases et s'assimile à une appropriation des données. Néanmoins, le législateur a proposé l'ouverture des données contenues dans les bases lorsqu'elles sont produites au moyen d'objets connectés, en faveur du générateur de la donnée. La protection des bases de données n'est pas l'unique outil de réservation, d'autres moyens permettent une forme d'appropriation des données agricoles privées par leurs détenteurs.

Chapitre 2. La réservation de l'accès aux données agricoles non protégées

303- Dans le secteur agricole, les sociétés de prestation de services telles que SMAG, ITK ou encore Ekylibre, traitent et enrichissent les données brutes collectées sur les exploitations afin de fournir de l'aide à la décision et des informations utiles aux exploitants agricoles[919]. Afin de protéger leur savoir-faire, conserver leur avantage concurrentiel et sécuriser les données qu'elles détiennent, ces sociétés en réservent l'accès. Toutefois, lorsque les bases de données ne répondent pas aux conditions de protection du droit de la propriété intellectuelle, c'est par le contrat que les entreprises organisent les conditions et les modalités d'accès aux données. Ainsi, la liberté contractuelle leur permet d'aller au-delà de la protection qu'elles auraient pu obtenir avec le droit d'auteur et le droit *sui generis*. Si le droit de propriété intellectuelle sur les bases de données ne constitue pas un obstacle à la circulation des données[920], les clauses de confidentialité, elles, imposent de les garder secrètes et en empêchent la circulation. Mais aussi, afin de protéger les données contre les attaques extérieures, des outils techniques permettent de les sécuriser. Par conséquent, afin d'étudier les outils juridiques et techniques à la disposition des sociétés de l'agriculture numérique pour la réservation des données en dehors des droits de propriété intellectuelle, il faut, tout d'abord, envisager la réservation contractuelle de l'accès aux données agricoles (**Section 1**), pour, ensuite, s'intéresser à la sécurisation technique de ces données (**Section 2**).

Section 1. La réservation contractuelle de l'accès aux données agricoles

304- Il convient d'envisager le contenu du principe de la liberté contractuelle appliqué aux contrats de l'agriculture numérique (**§1**) avant d'analyser la réservation d'informations agricoles confidentielles par le contrat (**§2**).

[919] Voir *supra*, n°138.
[920] Voir *supra*, n°267 et s.

§1. *Le contenu du principe de la liberté contractuelle appliqué aux contrats de l'agriculture numérique*

305.- L'étude de la liberté contractuelle appliquée aux contrats de l'agriculture numérique suppose d'en envisager le principe (**I**), ainsi que ses limites (**II**).

I. Le principe de la liberté contractuelle appliqué aux contrats de l'agriculture numérique

306.- Tout d'abord, la jurisprudence a reconnu que l'accès aux bases de données non protégées pouvait être limité par la liberté contractuelle[921] (**A**). Par conséquent, les parties sont libres de prévoir les contrats qu'elles souhaitent sur les bases de données non protégées (**B**).

A. Le principe de la liberté contractuelle sur les bases de données non protégées

307.- Dans le secteur agricole, les sociétés prestataires de services qui fournissent de l'aide à la décision obtiennent de nombreuses données grâce aux technologies de collecte de données (objets connectés, capteurs, etc.). Ces données sont ensuite stockées dans des bases de données, des entrepôts de données (*Datawarehouse*) ou encore dans des lacs de données (*Datalake*) sans qu'un travail de structuration soit nécessairement effectué ou qu'il y ait un apport intellectuel. Le travail d'enrichissement ne vient alors que postérieurement pour le traitement des données. Par conséquent, ces sociétés ne peuvent pas revendiquer le bénéfice de la protection des bases de données que ce soit au titre du droit d'auteur ou du droit *sui generis*. La question se pose donc de savoir si l'accès à ces données peut être limité et sur quel fondement cette limitation peut reposer. Sur cette question, tout d'abord, les juges ont apporté des éléments de réponse dans la décision *Ryanair c/PR Aviation* qu'il convient d'analyser (**1**). Ensuite, il sera nécessaire d'envisager le bénéfice de la liberté contractuelle sur l'accès aux bases de données non protégées (**2**).

[921] CJUE, 15 janv. 2015, n° C-30/14, *Ryanair Ltd c/ PR Aviation BV*, *JurisData*, n°2015-002578 ; *RIDA*, 2015/2, p. 319 et p. 301, obs. SIRINELLI, P. ; *Auteurs et medias*, 2015, p. 181, obs. LAMBRECHT, M. ; *PI*, 2015, n°55, p. 211, obs. BERNAULT, C. ; *RLDI*, mars 2015, n°3685, obs. CASTETS-RENARD, C. ; *Prop. Industr*., 2015, comm. 71, note LARRIEU, J.

1. L'affaire Ryanair c/PR Aviation

308- **L'étendue de l'application du droit des bases de données.** La Cour de justice de l'Union européenne (CJUE) a été saisie d'une question préjudicielle dans un litige opposant *Ryanair Ltd c/PR Aviation BV*. Il s'agissait d'interpréter la directive 96/9/CE du 11 mars 1996 concernant la protection juridique des bases de données[922] au regard de sa portée sur les bases de données ne répondant pas aux conditions de la protection. Dans cette affaire, la société « *Pr Aviation exploit[ait] un site internet sur lequel les consommateurs pouv[aient] faire des recherches dans des données de vol de compagnies aériennes à bas coût, comparer les prix et, moyennant le paiement d'une commission, réserver un vol* ». À cette fin, *PR Aviation* obtenait les données à partir d'un recueil couplé au site internet *Ryanair*, également accessible aux utilisateurs. L'utilisation de ce site était, néanmoins, soumise à l'acceptation de Conditions générales d'utilisation qui interdisaient notamment d'autres sites à vendre des vols ou de l'utiliser à des fins commerciales. Aussi, pour justifier l'usage exclusif de leurs données, la société *Ryanair* invoquait le bénéfice de la directive 96/9/CE. La question se posait alors de savoir si la directive du 11 mars 1996 s'étendait aux bases de données qui ne sont pas protégées, que ce soit par le droit d'auteur ou par le droit *sui generis* et si la liberté d'utiliser une base de données non protégée pouvait être limitée contractuellement. La CJUE[923] a répondu, le 15 janvier 2015, que *« la directive 96/9/CE doit être interprétée en ce sens qu'elle n'est pas applicable à une base de données qui n'est protégée ni par le droit d'auteur ni par le droit sui generis en vertu de cette directive, si bien que les articles 6, paragraphes 1, 8 et 15 de ladite directive ne font pas obstacle à ce que le créateur d'une telle base de données établisse des limitations contractuelles à l'utilisation de celle-ci par des tiers, sans préjudice du droit national applicable* ». Les exceptions au droit des bases de données contenues aux articles 6 et 8 de la directive ne s'appliquent donc qu'aux bases de données protégées. Il apparaît que de telles exceptions sont « *sans pertinence s'agissant d'une base de données non protégée dont le créateur ne jouit, en vertu de la directive nº 96/9, d'aucun des droits susmentionnés* »[924]. Les juges ont, ainsi, d'une part rejeté l'argument de *Ryanair* invoquant une protection de leur base sur le fondement de la directive, au motif que la base de données ne répondait ni aux conditions du droit d'auteur ni aux conditions du droit *sui generis*. D'autre part, ils ont affirmé que rien n'empêche en revanche les créateurs d'une base de données non protégée de limiter l'accès à

[922] *JO* L 77/20 du 27 mars 1997.
[923] *Ibid.*
[924] CASTETS-RENARD, C., « La liberté contractuelle et la réservation de l'information des bases de données non protégées devant la CJUE », *RLDI*, n°113, 1er mars 2015.

leur base par la technique contractuelle au-delà des exceptions prévues par la loi au droit *sui generis*. Par conséquent, « *le droit sui generis prévu par la directive 96/9/CE du 11 mars 1996 sur les bases de données ne peut trouver à s'appliquer dans la mesure où ces données ne sauraient être protégées en tant que telles par le droit sui generis de la base. C'est dès lors le contrat qui en régit l'usage […]* »[925].

2. Le bénéfice de la liberté contractuelle sur l'accès aux bases de données

309- Les sociétés du secteur agricole qui ne peuvent bénéficier du droit de propriété intellectuelle sur leurs bases de données peuvent en limiter l'accès avec le contrat. Aussi, il semblerait qu'il soit plus avantageux de ne pas bénéficier de la protection et de prévoir contractuellement les accès à une base de données non protégée que de revendiquer un droit de propriété intellectuelle sur la base de données. En effet, le producteur bénéficie du principe de la liberté contractuelle pour régir l'accès à sa base, il peut donc prévoir, librement et sans contraintes, les conditions d'accès et les modalités d'utilisation de celle-ci[926]. Exempt des exceptions du droit *sui generis*, le producteur n'est plus soumis à l'obligation d'accorder l'accès à sa base aux tiers. En outre, la clause de secret[927] offre la possibilité au producteur d'imposer à l'autre partie, l'utilisateur, la confidentialité des informations contenues dans la base de données. Le non-respect de cette clause est sanctionné par des dommages et intérêts[928].

B. Les effets de la liberté contractuelle sur les bases de données non protégées

310- En premier lieu, il est nécessaire d'étudier le contenu de la liberté contractuelle (**1**) pour, en second lieu, envisager les conséquences sur l'accès aux bases de données (**2**).

1. Le contenu de la liberté contractuelle

311- **Le siège de la liberté contractuelle**. Le principe de la liberté contractuelle réside à l'article 1102 du Code civil qui dispose que « *chacun est libre de contracter ou de ne pas*

[925] ZOLYNSKI, C., « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », *op. cit.*
[926] CHATRY, S., « Droit des producteurs de bases de données », *J-Cl. Propriété littéraire et artistiques*, fasc. 1650, n°7.
[927] Voir *infra*, n°339 et s.
[928] C. civ., art. 1142.

contracter, de choisir son cocontractant et de déterminer le contenu et la forme du contrat dans les limites fixées par la loi. La liberté contractuelle ne permet pas de déroger aux règles qui intéressent l'ordre public ». Ainsi, selon le principe de l'autonomie de la volonté, les parties sont libres de déterminer le contenu du contrat en l'absence de régime spécifique applicable. Ce contrat tient ensuite lieu de loi à ceux qui l'ont fait[929]. La liberté contractuelle constitue une nouvelle limite à la liberté de circulation des données qui s'ajoute au régime légal de protection.

2. Les conséquences de la liberté contractuelle sur l'accès aux bases de données

312- **L'intérêt de conserver la protection légale des bases de données en présence de la liberté contractuelle.** Dans l'affaire *Ryanair c/PR aviation*, la Cour a reconnu la possibilité pour le créateur d'une base de données non protégée d'imposer les conditions qu'il souhaite dans le contrat pour l'accès à sa base. Les observateurs se sont alors interrogés sur l'opportunité de conserver la protection légale des bases de données par le droit d'auteur et par le droit *sui generis* si la liberté contractuelle s'avère plus efficace pour les créateurs. Néanmoins, la Cour a répondu à cette problématique, dans l'arrêt précité, en affirmant que cette possibilité « *n'est pas de nature à réduire l'intérêt de revendiquer la protection juridique par ladite directive en ce que le créateur d'une base de données protégée par cette même directive ne jouirait pas, à la différence du créateur d'une base de données non protégée par celle-ci, de la liberté contractuelle de limiter les droits des utilisateurs de sa base* »[930]. En effet, la Cour rappelle dans le considérant suivant qu'il existe un véritable intérêt juridique et économique à revendiquer la protection de la directive puisqu'il s'agit d'un régime de protection automatique, harmonisé dans les États membres, que le créateur ou le producteur de la base peut, à ce titre, se réserver le droit de faire, d'autoriser ou d'interdire les actes visés dans la directive[931]. De plus, afin d'obtenir cette protection, le producteur ou le créateur de la base de données ne doit accomplir aucune formalité administrative ni arrangement conventionnel préalable[932].

313- **Une balance des avantages/inconvénients de chaque protection.** Chacune des protections contient son lot d'inconvénients. Comme l'explique Mme la professeure C. Bernault, « *dans un cas, on peut jouir pleinement de la liberté contractuelle, mais on subit les limites de l'effet relatif des conventions alors que, dans l'autre, on perd un peu de cette liberté, mais on dispose*

[929] C. civ., art. 1103 : « *Les contrats légalement formés tiennent lieu de loi à ceux qui les ont faits* ».
[930] CJUE, 15 janv. 2015, n° C-30/14, *Ryanair Ltd c/ PR Aviation BV*, cons. 41.
[931] Voir *supra*, n°232.
[932] CJUE, 15 janv. 2015, n° C-30/14, *Ryanair Ltd c/ PR Aviation BV*, cons. 42.

d'un droit opposable erga omnes »[933]. Ainsi, tandis que les droits de propriété intellectuelle fournissent un régime de protection « clé en main » opposable à tous, au producteur de la base de données, la liberté contractuelle offre, certes, plus d'amplitude au créateur afin de régir l'accès à sa base, mais elle n'est opposable qu'au contractant.

314- **Les voix dissidentes sur la liberté contractuelle appliquée aux bases de données**. Certains auteurs, à l'image de M. le professeur J. Passa, remettent en cause la limite contractuelle d'une liberté d'exploitation pour un objet incorporel. Ceci en raison du fait que le législateur, en créant un régime de protection, recherche un équilibre entre les différents intérêts en jeu. Selon cet auteur, l'équilibre ainsi recherché est exclu des contrats qui favorisent au contraire la loi du plus fort. Aussi, le contrat qui fixerait des interdits non prévus dans la loi ne devrait être valable qu'au nom d'un intérêt supérieur. Par conséquent, il ne devrait donc pas être possible de limiter contractuellement l'accès à une base de données lorsque celle-ci ne peut pas bénéficier du droit *sui generis*. Il ne devrait donc pas être possible de le limiter en raison de l'exception légale de protection conférée par le droit dont fait l'objet la base[934].

II. Les limites de la liberté contractuelle sur les contrats de l'agriculture numérique pour l'accès aux données

315- La liberté contractuelle comporte des limites auxquelles il faut apporter une attention particulière. Tout d'abord, les acteurs doivent respecter les obligations liées à l'exécution du contrat (**A**). Ensuite, les contrats ne doivent pas connaître un déséquilibre significatif (**B**).

A. Les obligations liées à l'exécution du contrat

316- L'objectif du droit des contrats est d'assurer la « *loyauté des contractants et l'équilibre de leur relation, conditions d'une confiance que juristes et économistes s'accordent à juger favorable au bon fonctionnement du marché* »[935]. Pourtant, la protection et la circulation des données agricoles par le truchement du contrat s'avèrent laborieuses. Aussi, il convient d'analyser, en

[933] BERNAULT, C., « Base de données : à défaut de propriété intellectuelle, le recours au contrat », *L'Essentiel, Droit de la propriété intellectuelle*, n°03, p. 3, 2015 : « *L'exploitation d'une base de données non protégée par un droit de propriété intellectuelle peut être limitée par un contrat sans que les exceptions prévues par la directive n°96/9/CE soient applicables* ».
[934] PASSA, J., « La limitation par contrat de l'exploitation d'un objet non protégé par un droit de propriété intellectuelle », *RDC*, n°02, 2015, p. 348.
[935] *Ibid.*

premier lieu, le principe du devoir de loyauté dans les contrats de l'agriculture numérique (**1**). En second lieu, il faudra s'intéresser à l'étendue de ce devoir (**2**).

1. Le principe du devoir de loyauté dans les contrats de l'agriculture numérique

317- **Principes irriguant le droit des contrats.** Tout d'abord, le contrat doit être exécuté de bonne foi, au titre de l'article 1104 du Code civil, ce qui suppose un devoir de loyauté des co-contractants[936]. À cette fin, le principe de transparence vient compléter cet arsenal juridique afin d'assurer les principes de loyauté et de bonne foi dans l'exécution du contrat. La transparence est le fait de « *laisser voir ce qui se trouve dans le contenu même du contrat projeté, pour mieux le négocier* »[937].

318- **Manquements dans l'exécution des contrats de l'agriculture numérique**. Il faut pointer du doigt que, bien souvent, les contrats de l'agriculture numérique manquent de transparence. Comme le relève Mme H. Juillet-Régis[938], les entreprises de l'*AgTech* n'informent pas toujours les exploitants agricoles des tiers qui auront accès aux données non personnelles, de la manière dont elles seront conservées, partagées, à quelles fins, etc. En outre, les principes de loyauté et de bonne foi imposent que les données ne soient pas utilisées dans l'intérêt contraire de l'exploitant agricole. Par exemple, les données communiquant des informations sur les récoltes de l'année précédente ne doivent pas permettre, aux distributeurs ou aux entreprises de l'agroalimentaire, de spéculer sur les prix pour l'année suivante.

2. L'étendue du devoir de loyauté dans les contrats de l'agriculture numérique

319- **Renforcement par le législateur des principes irriguant l'exécution des contrats.** Tout d'abord, la bonne foi, comme principe fondamental du droit des contrats, est aujourd'hui prise en compte dans l'analyse concurrentielle[939]. Ensuite, afin de rendre effectives ces exigences de loyauté et de transparence, plusieurs réglementations sont venues régir les contrats conclus à distance et les contrats du numérique.

---

[936] BERTIER-LESTRADE (de), B., « La bonne foi dans la réforme française des contrats », in LE GALLOU, C. et MARMISSE-D'ABBADIE D'ARRAST, A., ss. dir., *Le contrat dans tous ses États*, Presses de l'Université Toulouse 1 Capitole, pp. 141 à 160.

[937] AUBIN-BROUTE, R.-J., « Le contrat pour la maîtrise des données agricoles », *Droit rural*, n°49, janv. 2020, coll. 3.

[938] JUILLET-REGIS, H., « Quelle régulation pour les données agricoles ? », *op. cit.*

[939] MALAURIE-VIGNAL, M., HEINTZ, D. et LECOLE, M., « Comment appréhender les abus et l'utilisation des données dans la relation d'une plateforme avec ses partenaires contractuels ? » *CCC*, n°12, déc. 2020.

En premier lieu, l'ordonnance n°2016-131 du 10 février 2016[940] « *a consacré l'obligation de loyauté et d'information au cours du processus de formation de l'acte et, d'autre part, emprunté au droit du marché, son interdiction du déséquilibre significatif* »[941] et ce afin « *de promouvoir l'efficacité économique du droit commun des contrats* »[942]. Sur la forme, la réforme du droit des contrats est venue régir les conditions de conclusion des contrats électroniques figurant aux articles 1125 à 1127-4 du Code civil. Mais aussi, les conditions générales de vente (CGV) et les conditions générales d'utilisation (CGU) doivent répondre à certaines obligations afin d'assurer les conditions de la confiance entre les acteurs, elles doivent être diffusées dans un format accessible et lisible sur le site internet[943], être connues et acceptées[944] et elles ne doivent pas venir en contradiction avec les conditions particulières.

En second lieu, il faut noter l'adoption par le législateur européen de la directive 2019/770 du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques[945]. L'objectif, ici, est d'harmoniser plusieurs aspects des contrats conclus entre un professionnel et un consommateur portant sur la fourniture de contenus et de services numériques. Elle prévoit également les recours offerts aux consommateurs et leurs modalités en cas de non-conformité, ainsi que les conditions visant à limiter les possibles modifications, par le professionnel, du contenu ou du service numérique au cours de la période de fourniture du contenu ou service numérique. Cette directive s'applique « *à tout contrat par lequel le professionnel fournit ou s'engage à fournir un contenu numérique ou un service numérique au consommateur et le consommateur s'acquitte ou s'engage à s'acquitter d'un prix* »[946]. Il est remarquable de constater que l'activité agricole ne figure pas dans la définition de « consommateur » retenue par le législateur européen[947]. Néanmoins, l'ordonnance n°2021-1247 du 28 septembre 2021[948] a réintroduit l'activité agricole dans la liste

[940] Ord. n°2016-131 du 10 févr. 2016 portant réforme du droit des contrats, du régime général et de la preuve des obligations : *JORF* n°0035 du 11 févr. 2016.
[941] PILLET, G., « L'efficacité du droit français des contrats face aux géants de l'internet », *RTD com.* 2018, p. 273.
[942] *Ibid.*
[943] C. com., art. L. 441-6.
[944] C. civ., arts. 1119 et 1120.
[945] *JOUE* L 136 du 22 mai 2019.
[946] *Ibid.*, art. 3.
[947] En droit français, est considérée comme un consommateur « *toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale, libérale ou agricole* » (art. liminaire du C. consom.).
[948] Ord. n°2021-1247 du 29 sept. 2021 relative à la garantie légale de conformité pour les biens, les contenus numériques et les services numériques : *JORF* n°0228 du 30 sept. 2021. Cette ordonnance transpose les directives n°2019/770 du 20 mai 2019 relative à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques, et n°2019/771 du 20 mai 2019 relative à certains aspects concernant les contrats de vente de biens.

des activités professionnelles. Ainsi, en France, cette directive n'est pas applicable aux exploitants agricoles dans le cadre de leur activité.

En outre, par un panel de réglementations et de directives, le législateur européen souhaite contrôler en amont le respect des obligations de bonne foi, de loyauté et de transparence dans les contrats du numérique. Ce contrôle amont est complété par un contrôle aval.

B. Le contrôle du déséquilibre significatif dans les contrats de l'agriculture numérique

320- Le contrôle du déséquilibre significatif peut reposer sur le terrain de trois branches de droit que sont le droit commun des contrats, le droit des pratiques restrictives de concurrence et le droit de la consommation. Ainsi, afin, dans un second temps, de clairement identifier le droit applicable aux contrats de l'agriculture numérique (**2**), il faut, dans un premier temps, envisager le domaine d'application de chacune de ces branches (**1**).

1. Le domaine d'application des droits spéciaux et du droit commun du déséquilibre significatif

321- Le déséquilibre significatif dans le droit des contrats de consommation. La directive 93/13 du 5 avril 1993 concernant les clauses abusives dans les contrats conclus avec les consommateurs[949] s'applique dans les contrats conclus entre professionnels et consommateurs. Le consommateur est défini à l'article liminaire du Code de la consommation, comme « *toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale, libérale ou agricole* ». L'activité agricole a été ajoutée à la liste des activités professionnelles par l'ordonnance n°2016-301 du 14 mars 2016[950]. Par conséquent, les exploitants agricoles qui souscrivent des contrats afin d'obtenir la réalisation d'une prestation de services ou l'achat d'outils agricoles agissent dans le cadre de leur activité professionnelle. Ils ne pourront, donc, pas agir sur le fondement du droit de la consommation.

322- Le déséquilibre significatif dans le droit commun des contrats. Si le contrôle du déséquilibre significatif était auparavant restreint au droit de la consommation[951] et aux pratiques restrictives

[949] *JOUE* L 95/29 du 21 avr. 1993.
[950] Ord. n°2016-301 du 14 mars 2016 relative à la partie législative du code de la consommation : *JORF* n°0064 du 16 mars 2016.
[951] C. conso., art. L. 212-1.

de concurrence[952], la loi n°2018-287 du 20 avril 2018 portant réforme du droit des contrats, du régime général et de la preuve des obligations[953] a introduit la notion dans le droit commun des contrats à l'article 1171 du Code civil. Ainsi, « *toute clause non négociable déterminée à l'avance par l'une des parties qui crée un déséquilibre significatif entre les droits et les obligations sera réputée non écrite* »[954]. Tous les contrats d'adhésion conclus après le 1er octobre 2018 sont donc soumis au contrôle du déséquilibre significatif, peu importe la qualité des parties[955]. En effet, en principe, le contrat est la loi des parties. Néanmoins, si en théorie l'autonomie des volontés innerve le droit des contrats, ce n'est pas le cas dans les contrats d'adhésion. Certains contrats, définis à l'article 1110 du Code civil, sont donc soustraits de la négociation, il s'agit des contrats *« […] qui comporte[nt] un ensemble de clauses non négociables, déterminées à l'avance par l'une des parties* ». Par conséquent, en principe, pour l'achat d'un logiciel, la souscription d'un abonnement ou la demande d'accès à une plateforme, l'exploitant agricole, qui n'a d'autre choix que d'adhérer aux termes du contrat fixé par l'entreprise, pourrait se tourner vers le droit commun des contrats pour faire constater un déséquilibre significatif. En effet, les contrats auxquels il adhère prennent la forme de Conditions générales de vente (CGV) — contrats en ligne par lesquels les professionnels proposent la vente de biens ou la fourniture de service — ou de Conditions générales d'utilisation (CGU), qui régissent l'utilisation des différentes fonctionnalités proposées par la plateforme ou le site internet aux utilisateurs.

323- **Le déséquilibre significatif dans le droit des pratiques restrictives de concurrence.** Le droit spécial sanctionne le déséquilibre significatif dans le cadre de la négociation commerciale, de la conclusion ou de l'exécution d'un contrat[956]. C'est ainsi que l'article L. 442-1 du Code de commerce issu de l'ordonnance n°2019-359 du 24 avril 2019 relatif à la transparence, aux pratiques restrictives de concurrence et aux autres pratiques prohibées[957], sanctionne la partie au contrat *« qui obtient ou tente d'obtenir de l'autre partie un avantage ne correspondant à aucune contrepartie ou manifestement disproportionné au regard de la valeur de la contrepartie consentie ; Qui soumet ou tente de soumettre l'autre partie à des obligations créant un déséquilibre significatif dans les droits et obligations des parties ».* Cette branche du droit s'applique donc aux contrats commerciaux conclus entre une personne exerçant des

[952] C. com., art. L. 442-6, I, 2e.
[953] *JORF* n°0093 du 21 avr. 2018.
[954] C. civ., art. 1171, al. 1.
[955] C. civ., art. 1171, al.1.
[956] C. com., art. L. 442-1.
[957] *JORF* n°0097 du 25 avr. 2019.

activités de production, de distribution ou de services et l'autre partie au contrat, son cocontractant, agissant également dans le cadre de l'une de ces activités[958]. Par conséquent, le droit des pratiques restrictives de concurrence peut également s'appliquer aux contrats de l'agriculture numérique, puisque les exploitants agricoles souscrivent des contrats dans le cadre de leur activité de production agricole, auprès de sociétés qui proposent des prestations de services ou la vente de matériels agricoles. L'ensemble de ces acteurs agissent par conséquent dans le cadre de relations commerciales.

324- Articulation du droit commun avec le droit des pratiques restrictives de concurrence. La question se pose alors de savoir en cas de cumul lequel du régime commun des contrats et celui du droit des pratiques restrictives de concurrence trouve à s'appliquer dans les contrats entre professionnels de l'agriculture numérique. Aux termes de l'article 1105 du Code civil, les règles générales s'appliquent sous réserve des règles particulières à certains contrats. Aussi, il semble que, dans cette situation, le droit commun des contrats doive s'effacer au profit du droit des pratiques restrictives de concurrence. Par conséquent, les exploitants agricoles qui souscrivent des contrats pour la réalisation de prestation de services ou pour l'achat d'outils de collecte de données, par exemple, seront soumis de manière spécifique aux règles du Code de commerce.

2. Le contrôle du déséquilibre significatif dans les contrats de l'agriculture numérique

325- Caractérisation du déséquilibre significatif quant à l'accès aux données. La problématique réside dans le fait de caractériser le déséquilibre significatif dans les contrats commerciaux. Le Code de la consommation a établi des listes noire et grise[959] permettant de présumer qu'une clause est abusive dans les contrats conclus avec des consommateurs ou des non professionnels. Mais, dans les autres cas, lorsque le contrat est conclu entre professionnels, le Code civil et le Code de commerce ne prévoient pas un tel dispositif. C'est donc au juge que revient la tâche « *de déterminer [si] la clause litigieuse est génératrice d'un déséquilibre ou non* »[960].

326- Appréciation du déséquilibre contractuel. Tout le problème réside dans la caractérisation du déséquilibre puisque « *la mise à disposition des données permet […] au cocontractant de*

[958] Rapport au Président de la République relatif à l'ord. n°2019-359 du 24 avr. 2019 portant refonte du titre IV du livre IV du code de commerce relatif à la transparence, aux pratiques restrictives de concurrence et aux autres pratiques prohibées : *JORF* n°0097 du 25 avr. 2019.
[959] C. conso, arts. R. 212-1 et R. 212-2.
[960] VINGIANO-VIRICEL, I., « Les obligations précontractuelles d'information lors de la vente d'un objet connecté [contrat de vente] », ét. 6, *CCC*, déc. 2019.

disposer d'un pouvoir informationnel ou financier sur l'exploitant agricole » qui résulte *« de l'analyse et de l'agrégation des données* »[961] et non de leur simple détention. Aussi, afin d'apprécier le déséquilibre significatif, l'article L. 442-1 du Code de commerce précise que « *le déséquilibre significatif ne porte ni sur l'objet principal du contrat ni sur l'adéquation du prix à la prestation* ». Néanmoins, l'économie des contrats du numérique est souvent ambiguë. Il a été mis en évidence, en ce sens, que le « *point commun à toutes les grandes entreprises de l'économie numérique est l'intensité de l'exploitation des données issues du suivi régulier et systématique de l'activité de leurs utilisateurs* »[962]. En effet, celui qui détient les données peut en tirer un avantage concurrentiel et organiser l'économie de son activité autour de celles-ci[963]. Cependant, le droit peine à se saisir d'une économie structurée autour des données qui sont immatérielles et difficilement évaluables. Aussi, lorsque l'agriculteur souscrit un contrat pour l'obtention d'outils d'aide à la décision, l'accès à une plateforme, l'utilisation d'un logiciel ou encore l'achat de matériels agricoles, le contrat ne porte pas sur les données elles-mêmes. Or, l'entreprise tire un avantage concurrentiel des données collectées sur les exploitations agricoles *via* le contrat, sans qu'il y ait nécessairement de contrepartie pour l'agriculteur. De ce constat, « *il en résulte une perte de maîtrise [sur les données] pour l'utilisateur que le contrat peine à recréer* »[964].

Aussi, l'entreprise de l'*AgTech* détient un pouvoir sur l'agriculteur en raison du fait qu'elle peut fixer les conditions d'utilisation de son logiciel ou de son application dans des clauses non négociables qu'elle détermine à l'avance. Par conséquent, l'entreprise qui fournit le service contrôle l'accessibilité et la disponibilité des données issues des exploitations agricoles, tandis que l'agriculteur se soumet aux conditions de l'entreprise pour l'accès à ce service. Les entreprises de l'agriculture numérique pourraient donc voir leur responsabilité engagée en cas de déséquilibre significatif dans les contrats qu'ils concluent avec les agriculteurs. Par exemple, dès lors que la valeur des données collectées et traitées par l'entreprise est supérieure à la valeur du service obtenu, il pourrait y avoir un déséquilibre significatif entre les parties. Mais la valeur des données est le plus souvent résiduelle, c'est l'information qui en est tirée qui est évaluable. Il sera donc très difficile de démontrer un tel

[961] DOUVILLE, Th., « Contrat et données agricoles », *op. cit.*, n°6, p. 3.
[962] COLLIN, P. et COLIN, N., *Mission d'expertise sur la fiscalité de l'économie numérique*, Synthèse, janv. 2013, p. 2.
[963] PILLET G., « L'efficacité du droit français des contrats face aux géants de l'internet », *op. cit.*, n°12, p. 273 : « *Celui qui détient ces données et sait les exploiter se trouve en mesure d'améliorer ses produits ou ses services, de créer des applications pertinentes, de mieux cibler sa clientèle, de prendre de meilleures décisions stratégiques ou encore de valoriser ces données auprès de tiers qui deviennent concessionnaires de leur utilisation* ». Voir spéc. COLLIN, P. et COLIN, N., Mission préc., p. 2.
[964] PILLET, G., *idem*., n°13, p. 273.

déséquilibre entre les droits et les obligations des parties en se basant sur la seule valeur des données. Néanmoins, le déséquilibre significatif pourrait se fonder sur d'autres éléments, tels que la limitation de l'accès. En effet, le fournisseur de services ou de matériels qui traite et exploite les données exerce un pouvoir considérable sur l'accès aux données qui peut se manifester dans les contrats. Certains contrats prévoient par exemple qu'en cas de cessation de paiement de l'abonnement, l'accès au service sera suspendu, à charge pour le cocontractant de faire la demande de récupération des données brutes dans un délai défini (souvent trente jours). Cette clause qui limite de fait l'accès aux données pour l'agriculteur pourrait être constitutive d'un déséquilibre significatif dans la mesure où la charge de la réversibilité des données pèse sur l'utilisateur et non pas sur le fournisseur de services. Aussi, les entreprises détentrices des données limitent souvent leur responsabilité en cas de défaut d'accès si les manquements ne leur sont pas totalement imputables. Par exemple, l'entreprise peut partager sa responsabilité avec d'autres intervenants dans l'accessibilité des données, tels que le fournisseur de réseau internet. C'est un moyen efficace de dégager sa propre responsabilité. Constitue donc un déséquilibre contractuel, la clause « *portant sur la perte et le transfert des données agricoles insérées par le vendeur d'un bien ou le prestataire de service* »[965] ou quand cette clause « *favorise manifestement l'auteur du contrat d'adhésion conclu par l'exploitant au titre des données agricoles* »[966].

327- **Répression judiciaire du déséquilibre significatif.** Il ne semble pas exister pour l'heure de jurisprudence faisant application du déséquilibre significatif dans des contrats conclus entre fournisseur de services ou de matériels et collecteur de données. C'est le juge qui devra donc apprécier au cas par cas le caractère abusif d'une clause litigieuse dans les contrats de l'agriculture numérique. Tout porte à croire qu'une clause limitant de fait l'accès aux données collectées sur l'exploitation ou qui impose des conditions techniques trop contraignantes pour leur récupération par l'exploitant par exemple serait susceptible de caractériser un déséquilibre significatif entre les droits et les obligations des parties au contrat. Il est déjà admis que l'exploitation disproportionnée des données peut être source de déséquilibre à en croire l'assignation de la DGCRRF à l'encontre des sociétés Apple et Google. La DGCCRF considère, en effet, que de telles clauses caractérisent un déséquilibre significatif à l'encontre des développeurs de contenus et d'application. Ces clauses permettent en effet « *la libre [ré-] utilisation des informations, par Google ou Apple, notamment technologiques, communiquées*

[965] BEGUIN-FAYNEL, C., « La problématique de l'appropriation des données agricoles », *Droit rural*, n°479, janv. 2020, coll. 2, n°9.
[966] *Ibid.*

par les développeurs, sans réciprocité »[967]. Dans ce sens, le Tribunal de commerce de Paris a condamné dans une décision du 28 mars 2022[968], la société Google à une amende de 2 millions d'euros et l'a contrainte à réécrire dans un délai de trois mois plusieurs clauses jugées déséquilibrées du contrat de distribution proposé aux développeurs français sur le fondement de l'ancienne version de l'article L. 442-6, I, 2e du Code de commerce. Cet article interdisait en effet « *de soumettre ou de tenter de soumettre un partenaire commercial à des obligations créant un déséquilibre significatif dans les droits et obligations des parties* ».

328- **Responsabilisation du cocontractant.** Dans le cas où un déséquilibre significatif serait démontré, l'auteur de tels agissements engagerait sa responsabilité et devrait réparer le préjudice causé à son cocontractant. Depuis l'ordonnance n°2019-359[969], les victimes professionnelles des pratiques répréhensibles peuvent demander eux-mêmes l'annulation des clauses excessives sur le fondement de l'article L. 442-4 du Code de commerce. Ils ne sont donc plus obligés d'attendre l'action du ministère de l'Économie et des Finances pour agir en leur nom.

§2. *Le contenu du contrat, la réservation d'informations confidentielles*

329- De nombreuses données sont collectées sur les exploitations agricoles puis traitées afin de fournir de l'aide à la décision et des informations utiles pour l'agriculteur. Ces données peuvent contenir des informations considérées comme sensibles commercialement à la fois pour l'exploitant agricole et pour les entreprises de l'*AgTech*. En effet, d'une part, qu'elles soient personnelles ou non personnelles, les données agricoles peuvent contenir des informations sur les techniques agricoles, informations considérées comme sensibles pour les exploitants. Ces données peuvent révéler leur savoir-faire et ont un intérêt économique certain. Également, d'autres acteurs peuvent collecter des données qui une fois couplées à celles des exploitants agricoles peuvent révéler un grand nombre d'informations à propos de l'exploitation, elle-même et de ses activités[970]. C'est le cas notamment du gouvernement qui collecte des données

[967] AN, *Les plateformes numériques*, Rapport d'information n°3127, 24 juin 2020 ; MALAURIE-VIGNAL, M., HEINTZ, D. et LECOLE, M., « Comment appréhender les abus et l'utilisation des données dans la relation d'une plateforme avec ses partenaires contractuels ? », *CCC*, n°12, déc. 2020.

[968] T. com. Paris, 28 mars 2022, n°2018017655 ; comm. *Actualités du droit*, BERLEMONT, J., avr. 2022 ; AUGAGNEUR, L.-M., *Actualités du droit*, comm. mars 2022.

[969] Ord. relative à la transparence, aux pratiques restrictives de concurrence et aux autres pratiques prohibées : *JORF* n°0097 du 25 avr. 2019.

[970] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, *Farm Data Management, Sharing and Services for Agriculture Development,* Unit 2. Data Sharing Principles, Lesson 2.2: Challenges for Smallholders in Data Value Chains, oct./nov. 2019, p. 6.

concernant l'exploitation au cours du recensement agricole, ou encore, des centres de recherche qui collectent des données satellitaires ou des données géospatiales[971].

C'est ainsi que « *des données de production peuvent être utilisées par les partenaires acheteurs pour mettre l'agriculteur en position de faiblesse lors de la négociation. Ces données peuvent influencer les marchés des matières agricoles* »[972]. De même, « *la divulgation de certaines informations peut […] nuire au secret de la stratégie de l'exploitation comme des informations sur les relations partenariales de l'agriculteur ou encore l'accès à sa comptabilité* »[973]. Les données phytosanitaires par exemple révélant les produits utilisés et leur quantité pourraient être détournées pour nuire à l'image des agriculteurs. De même, aux États-Unis, certaines entreprises partagent les données des agriculteurs ayant les meilleurs rendements avec d'autres agriculteurs moins efficaces dans le but d'améliorer leurs propres rendements[974]. Il faut soulever également que les agriculteurs peuvent avoir « *la crainte que la diffusion de certaines informations facilite des vols de productions ou de matériels* »[975]. C'est le cas notamment en ce qui concerne les apiculteurs utilisant des ruches connectées qui souhaitent conserver la confidentialité des données de géolocalisation de leurs ruches afin d'éviter tout vol par leurs concurrents[976] ou par d'autres personnes. D'autre part, les entreprises de l'*AgTech* qui traitent et analysent les données ont développé des algorithmes et des méthodes de traitement afin de fournir de l'aide à la décision aux agriculteurs. Ainsi, en vue de la protection de leur savoir-faire et en raison de leurs investissements intellectuels, financiers et matériels, les données traitées recouvrent également un caractère sensible pour ces entreprises, en raison de leur intérêt commercial. À ce titre, elles souhaitent également conserver la confidentialité de ces données. Par conséquent, dans un premier temps, il est nécessaire d'envisager le principe de la protection des informations sensibles (**I**). Dans un second temps, il faudra s'intéresser plus spécialement au régime du secret des affaires (**II**).

---

971 *Ibid.*
972 BRUN, F., « Quelles opportunités et craintes sur les échanges de données agricoles ? Point de vue des agriculteurs », Projet Multipass, 14 janv. 2019 ; https://numerique.acta.asso.fr/multipass-1-opportunites-craintes-data-agri/.
973 *Ibid.*
974 Voir *infra*, n°596.
975 BRUN, F., « Quelles opportunités et craintes sur les échanges de données agricoles ? Point de vue des agriculteurs », *op. cit.*
976 Voir *infra*, n°703.

I. Le principe de la protection des informations sensibles

330- Si la loi offre plusieurs régimes de confidentialité qui s'avèrent, après analyse, limités (**A**), les parties peuvent toutefois toujours convenir d'organiser la confidentialité de certaines informations dans leur contrat, au moyen d'une clause de confidentialité (**B**).

A. La protection légale limitée des informations sensibles

331- Tout d'abord, le droit pénal offre une protection à certaines informations (**1**). La responsabilité civile permet également d'engager la responsabilité de ceux qui ne respecteraient pas la confidentialité de certaines informations (**2**). Enfin, les données à caractère personnel bénéficient de leur propre régime de protection (**3**).

1. Les secrets pénalement répréhensibles

332- **Secrets traités.** Le droit pénal offre plusieurs régimes de protection pour des informations spécifiques. Dans le cadre des données de l'agriculture numérique, seulement certains de ces régimes doivent être développés afin de traiter ceux qui touchent de près ou de loin ce secteur. Il s'agit du secret professionnel, du secret de fabrique et du secret statistique. En revanche, les secrets portant sur les informations relevant de la défense nationale ne seront pas traités. En effet, les acteurs du secteur agricole n'ont, en principe, pas vocation à traiter d'informations pouvant porter atteinte à la préservation des intérêts fondamentaux de la Nation, telles que la défense et la sécurité nationale. De même, le secret médical ne sera pas traité, puisque le secteur agricole n'a pas vocation à exploiter des données portant sur des informations collectées par des professionnels de santé. Enfin, les acteurs de l'agriculture numérique ne sont pas, non plus, concernés par le secret des correspondances concernant la confidentialité des informations contenues dans les courriers postaux et électroniques.

333- **Secret professionnel.** L'article 226-13 du Code pénal dispose que « *la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une condition ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 euros d'amende* ». Cette protection est limitée aux seules professions réglementées telles que les professions médicales. Par conséquent, elle ne peut pas s'appliquer aux personnes qui ne sont pas visées directement par la loi ou par la jurisprudence.

Ainsi, l'infraction de violation du secret professionnel est inefficace pour la reproduction et l'utilisation frauduleuse de données d'une entreprise privée.

334- **Secret de fabrique.** En droit de la propriété intellectuelle, les articles L.1227-1 du Code du travail et L.621-1 du CPI sanctionnent la violation d'un secret de fabrique. Ce dispositif est limité aux informations qui portent sur le savoir-faire technique de l'entreprise et exclut le savoir-faire commercial. Les personnes concernées par cette infraction de divulgation d'un secret de fabrique ne peuvent être sanctionnées qu'en cas de divulgation de ce secret. Ainsi, un simple usage personnel du savoir-faire ne pourra pas faire l'objet d'une sanction. De plus, les conditions de la répression de la violation d'un secret de fabrique exigent que le secret soit révélé par le salarié ou par le dirigeant de l'entreprise. Or, les relations de l'agriculture numérique développées ici concernent surtout celles qui lient un vendeur de matériel ou un fournisseur de services avec son client, agriculteur. Par conséquent, le secret de fabrique ne trouve pas à s'appliquer dans les relations d'affaires du secteur de l'agriculture numérique.

335- **Secret statistique.** C'est la loi n°51-711 du 7 juin 1951 sur l'obligation, la coordination et le secret en matière de statistique qui encadre le secret statistique. Afin de préserver les informations ayant trait à la vie personnelle et familiale, les renseignements individuels collectés par les services de la statistique dans les questionnaires ne peuvent être communiqués avant un délai de soixante-quinze ans suivant la date de réalisation de l'enquête ou de vingt-cinq ans à compter de la date de décès de l'intéressé. Il existe néanmoins une exception relative à une demande effectuée à des fins de statistiques publiques ou de recherche scientifique et historique sur décision de l'administration des archives et après avis du Comité du secret statistique[977]. De même, les renseignements d'ordre économique ou financier ne peuvent faire l'objet d'aucune communication, avant l'expiration d'un délai de vingt-cinq ans à compter de la date de réalisation de l'enquête, sauf décision contraire de l'administration des archives et après avis du Comité du secret statistique. Aussi, les services de la statistique qui réalisent des enquêtes auprès des agriculteurs doivent respecter le secret statistique et ne pas divulguer d'informations portant sur la vie privée ou d'ordre économique et financier sauf dans certaines conditions prévues par la loi. Il est à noter que ces informations ne peuvent jamais être utilisées à des fins de contrôle fiscal ou de répression économique.

[977] Pour un ex., voir *supra*, n°161 et s., spéc. 163.

2. L'obligation civile de confidentialité

336. **Préjudice de la violation du secret.** En l'absence de contrats, les litiges concernant la protection d'un secret se règlent sur le terrain de la responsabilité civile[978]. Au titre de l'article 1240 du Code civil, « *tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer* ». La responsabilité civile permet donc de sanctionner sur le fondement de la théorie de la responsabilité précontractuelle « *une prise de substance des résultats des efforts intellectuels ou matériels d'autrui afin d'économiser les investissements* »[979]. Il s'agit là encore d'un cas particulier ne permettant pas de conserver l'exclusivité des données. Le législateur a tenu compte de ces difficultés et a notamment inséré dans le Code civil, l'article 1112-2 qui permet d'engager la responsabilité de la personne qui utilise ou divulgue une information confidentielle relevant de la période des négociations précontractuelles.

337. **Difficultés probatoires.** La charge de la preuve est lourde pour la personne créancière du secret divulgué : elle doit démontrer que l'information révélée constitue un secret, que son débiteur n'est pas autorisé à la divulguer, que c'est bien ce débiteur qui l'a divulguée et que cette divulgation non autorisée lui cause un préjudice[980]. Aussi, la responsabilité civile sera difficile à mettre en œuvre dans le cadre de l'agriculture numérique. La personne qui se prétend victime d'une obtention illicite de données devra donc démontrer qu'il y a bien eu une fuite de données et trouver son origine, ce qui est, en pratique, un exercice difficile. Cette contrainte probatoire distingue la confidentialité des droits de la propriété intellectuelle, ce qui « *risque de réduire l'effectivité de la protection des données et d'affaiblir l'utilisation pratique de la violation du secret des affaires* »[981].

3. L'obligation de sécurité des données à caractère personnel

338. La loi de 1978 dispose que « *les données doivent être traitées de façon à garantir une sécurité appropriée, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, ou l'accès par des personnes non*

[978] TESTU, F.-X., « Responsabilité civile et propriété des idées en matière de brevets et de savoir-faire », *RCA*, n°5, mai 2017, dossier 8.
[979] CHARDEAUX, M.-A., *Les choses communes*, LGDJ, n°67, p. 70.
[980] GALLOIS, J., « La clause de confidentialité (ou de secret) », *CCC*, n°5, mai 2021, dossier n°12.
[981] BOIZARD, M., « La valorisation des données numériques par la protection juridique des algorithmes », *Dalloz IP/IT*, 2018, p. 99.

autorisées, à l'aide de mesures techniques ou organisationnelles déterminées »[982]. Aussi, le Règlement n°016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (RGPD)[983] offre un cadre protecteur à ces données[984]. En substance, les traitements des données à caractère personnel doivent être justifiés en raison d'une finalité prévue par la loi ou avoir reçu le consentement de la personne physique[985]. L'accès aux données à caractère personnel est donc limité par la loi. De plus, le responsable du traitement doit mettre en œuvre « *des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au[x] risque[s]* »[986], concernant les droits et libertés des personnes physiques. Il peut ainsi mettre en place « *les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement* »[987]. Les données à caractère personnel doivent donc à ce titre être maintenues confidentielles.

B. La clause de confidentialité

339. La protection du secret des affaires, malgré une définition inexistante, est une priorité pour les acteurs économiques. Le cas le plus parlant est celui de la recette du Coca-cola[988]. Jusqu'à récemment, aucune infraction ne permettait de sanctionner un secret d'affaires. Néanmoins, plusieurs textes législatifs et réglementaires encadraient la confidentialité des informations[989]. Le secret peut donc être protégé par le contrat (**1**) à travers la rédaction d'une clause de confidentialité (**2**).

[982] LIL, art. 4, 6° ; RGPD, art. 5, 1°, f).
[983] *JOUE* L 119/1 du 4 mai 2016.
[984] Voir *infra*, n°711 et s.
[985] Pour un développement sur la sécurité des données personnelles, voir *infra*, n°786 et s.
[986] Règl. n°2016/679, préc., art. 32.
[987] *Ibid.*
[988] GALLOUX, J.-C., « La directive sur le secret des affaires », *RTD com.*, 2017, p. 59.
[989] GALLOUX, J.-C, « Droit sur les créations nouvelles », *RTD com.*, 2014, p. 87.

1. Le secret protégé par le contrat

340- Contexte. Un grand nombre de savoir-faire sont conservés par le truchement des clauses de confidentialité[990]. Ces clauses permettent de garder une information secrète et « *[d'] ériger en faute la divulgation d'une information* »[991]. Le débiteur a, dès lors, « *un devoir de se taire* »[992].

341- Objet. La clause de confidentialité a vocation à conserver secrètes toutes les informations ayant une valeur économique ou un intérêt stratégique, non protégeables par ailleurs. Il peut s'agir, par exemple, de l'interdiction de révéler des connaissances techniques transmises dans les contrats de recherche (Licence de *Know-How*).

La clause doit déterminer la nature des informations faisant l'objet du secret, elle doit préciser les modalités de l'interdiction de circulation des informations ainsi que lister les débiteurs de l'obligation de garder le secret. Il est à noter que les entreprises peuvent organiser des *Data Rooms* qui permettent aux parties d'organiser la diffusion de l'information pour les opérations importantes de manière sécurisée[993].

342- Validité. L'obligation de confidentialité ne peut porter que sur des informations confidentielles. Il n'y a pas de limite de durée, la jurisprudence a admis une « *obligation sans terme dès lors que le procédé susceptible de protection n'est pas tombé dans le domaine public* »[994]. C'est pourquoi, une clause de confidentialité universelle et perpétuelle tant qu'elle ne porte pas sur « *des branches spécifiques de la profession du débiteur* »[995] semble envisageable. Néanmoins, il faut prendre en compte l'article 1210 du Code civil qui prohibe les engagements perpétuels et qui pourrait être soulevé par le débiteur de l'obligation de confidentialité. Il pourrait ainsi être judicieux de rédiger une clause limitée dans le temps, dont la durée serait déterminée selon la nature de l'information et selon la personne du débiteur[996].

343- Limite. L'obligation de garder le secret ne peut être absolue. Certaines catégories d'informations peuvent d'ailleurs être exclues. De même, la clause ne sera pas licite dans le cas où elle favorise une restriction de la concurrence. Par exemple, dans l'arrêt *Pronuptia*[997], la

---

[990] Aussi appelée clause de secret, de non-divulgation, de discrétion ou de non-communication.
[991] CASEAU-ROCHE C., « La clause de confidentialité », *AJCA*, 2014, p. 119.
[992] VIVANT, M., « Les clauses de secrets. Les principales clauses conclues par les professionnels », Colloque de l'IDA, *PUAM*, 1991, p. 101.
[993] DANDERN, B. et HAUSSMANN, C., « Les *Data Rooms* : une pratique vue sous un angle théorique », *Droit et patrimoine*, n°175, 2018.
[994] CASEAU-ROCHE, C., « La clause de confidentialité », *op. cit.*
[995] *Ibid.*
[996] GALLOIS, J., « La clause de confidentialité (ou de secret) », *op. cit.*.
[997] CJUE, *Pronuptia de Paris GmbH c/ Pronuptia de Paris Irmgard Schillgalis*, aff. 161/84, 61984J0161, 28 janv. 1986.

CJUE a estimé que « *le franchiseur doit pouvoir communiquer aux franchisés son savoir-faire et leur apporter l'assistance voulue pour les mettre en mesure d'appliquer ses méthodes, sans risquer qu'il profite, ne serait-ce qu'indirectement, à des concurrents* »[998]. Dès lors que le savoir-faire tombe dans le domaine public, il ne peut plus être imposé à moins de se rendre coupable d'une atteinte à la concurrence. Il n'est pas possible non plus de protéger une information illicite ou d'ordre public ou faisant l'objet d'un devoir de divulgation. Une protection disproportionnée d'une information ou la protection d'une information confuse et imprécise seraient aussi de nature à rendre nulle la clause de confidentialité[999].

344- **Mise en œuvre**. La mise en œuvre de la clause de confidentialité consiste à démontrer la faute qui permet d'engager la responsabilité contractuelle du débiteur. Cette preuve peut néanmoins être parfois difficile à apporter. Par ailleurs, les dommages et intérêts sont fixés dans une clause pénale ou bien le juge du fond peut, lui-même, les évaluer. Les créanciers peuvent, en outre, obtenir sous astreinte la cessation de toute publication des éléments confidentiels. Ils peuvent également solliciter en référé l'allocation d'une provision sur les dommages et intérêts et engager la responsabilité délictuelle du tiers complice qui a obtenu les informations en connaissance de cause et qui les a exploitées. Les créanciers de l'obligation de confidentialité peuvent enfin obtenir la résolution du contrat.

2. La rédaction de la clause de confidentialité

345- Afin de produire ses effets, la clause doit être correctement rédigée. Elle ne doit pas être trop large ou trop imprécise. En premier lieu, elle doit viser le destinataire de l'information qui peut être contraint de faire lui-même respecter la clause de confidentialité par ses collaborateurs, salariés et clients. Cette clause peut éventuellement être assortie d'une clause pénale. En second lieu, la clause doit être suffisamment précise pour appréhender les informations qui font l'objet de l'obligation de confidentialité, mais également suffisamment large pour ne pas faire l'impasse sur des informations confidentielles. Ainsi, la clause peut contenir une définition générale de la notion d'information confidentielle à laquelle est ajoutée une liste soit des informations sensibles en précisant que « *notamment ces informations sont considérées comme confidentielles* », soit au contraire, elle peut contenir une liste des informations qui ne sont pas confidentielles en précisant la mention « *par exception, ne sont pas considérées comme confidentielles* ». Par exemple, la clause peut être rédigée ainsi : « *les parties s'engagent, tant*

[998] *Ibid.*
[999] GALLOIS, J., « La clause de confidentialité (ou de secret) », *op. cit.*

pour leur compte que celui de leurs salariés, préposés et conseils, dont elles se portent fort, et ce, pour dix ans, à ne pas divulguer les documents et informations (les lister), à quelques personnes et sous quelque forme que ce soit, et à ne pas les exploiter à des fins personnelles et/ou en dehors des négociations et de l'exécution du présent accord, sauf autorisation expresse, préalable et écrite de l'autre partie ou sur injonction de justice ou d'une autorité administrative ou de contrôle »[1000].

II. La reconnaissance légale du secret des affaires

346- Aucune réglementation sur la protection du secret des affaires n'existait jusqu'à récemment. Plusieurs propositions de loi avaient été envisagées, mais n'ont jamais abouti, telles que la proposition de loi n°3985 de 2012 sur la violation du secret des affaires et la proposition de loi n°2139 de 2014 sur la protection du secret des affaires. Finalement, c'est l'Union européenne qui a franchi le cap[1001] en adoptant la directive n°2016/943/UE le 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués contre l'obtention, l'utilisation et la divulgation illicites[1002]. Aussi, il convient d'envisager la protection du secret des affaires (**A**) avant de s'intéresser à sa mise en œuvre (**B**).

A. La protection du secret des affaires

347- Le secret des affaires est une notion nouvelle (**1**) qui a fait l'objet d'une récente évolution réglementaire (**2**).

1. Une notion nouvelle

348- La notion de secret des affaires renvoie à l'immatérialité du patrimoine et à son caractère secret. Cette expression est reprise dans de nombreux textes législatifs et réglementaires[1003], mais

[1000] *Ibid.*
[1001] Pour une approche critique, voir LE STANC, C., « Secret d'affaires – Chut ! », *Propr. industr.*, n°6, juin 2016, repère 6 ; MARQUET, V., « Directive Secret des affaires : quand la liberté d'expression devient une exception, ou une vision européenne de la transparence », *Légipresse*, 2016, n°334, pp. 3 à 4 ; ARTIGUELONG, M. et GUIBERT, D., « Directive européenne "Secret d'affaires" : une menace pour les libertés ! », *Légipresse*, 2015, n°328, pp. 323 à 324.
[1002] *JOUE*, L 157/1 du 15 juin 2016, COM(2013) 813 final.
[1003] Loi n°2011-852 du 20 juill. 2011 relative à la régulation du système de distribution de la presse : *JORF* n°0167 du 21 juill. 2011, art. 4 ; Loi n°2010-476 du 12 mai 2010 relative à l'ouverture à la concurrence et à la régulation

aucun n'en donnait pour autant de définition[1004]. La jurisprudence française faisait également défaut en la matière. Finalement, quelques décisions de l'Union européenne avaient développé cette notion en la définissant comme « *les informations dont non seulement la divulgation au public, mais également la transmission à un sujet de droit différent de celui qui a fourni l'information peut gravement léser les intérêts de celui-ci* »[1005]. Dans un arrêt, le TPICE retenait, également, que « *sont secrètes les informations "chiffrées ou techniques" relatives notamment à "la position commerciale et à la position concurrentielle de la partie demanderesse ou du tiers qu'elles concernent" et que "dans la mesure où de telles informations sont spécifiques, précises et récentes, elles sont par nature des secrets d'affaires"* »[1006].

2. La récente réglementation portant sur les secrets d'affaires

340- Adoption de la directive sur le « secret des affaires ». La directive 2016/943/UE a été adoptée par le Parlement européen le 8 juin 2016 et désigne directement la protection du secret des affaires. Son objectif vise à mieux protéger les entreprises européennes réputées vulnérables face à l'espionnage économique et industriel. Cette directive porte donc « *sur la protection des savoir-faire et des informations commerciales non divulguées (secret d'affaires) contre l'obtention, l'utilisation et la divulgation illicites* ». Elle a fait l'objet d'une proposition de loi par les députés à l'assemblée en première lecture le 28 mars 2018, qui a été adoptée par la Commission mixte paritaire (CMP), le 24 mai 2018. Le texte ainsi proposé a été soumis au Sénat le 21 juin 2018 et finalement adopté définitivement par la loi n°2018-670 du 30 juillet 2018 relative à la protection du secret des affaires[1007].

350- Extension de la notion de secret des affaires. La directive retient une définition extensive de la notion de « *secret d'affaires* » inspirée de l'accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC). En transposant cette directive, le législateur français a consacré la définition du secret d'affaires à l'article L. 151-1 du Code de commerce, il s'agit de toutes les informations, quelle que soit leur nature (technique, commerciale, etc.), dès lors, qu'elles « *sont secrètes* », qu'elles ont une « *valeur commerciale parce qu'elles sont secrètes* », et qu'elles « *ont fait l'objet, de la part de la personne qui en a le contrôle de façon*

---

du secteur des jeux d'argent et de hasard en ligne : *JORF* n°0110 du 13 mai 2010, art. 43 ; Loi n°2008-776 du 4 août 2008, de modernisation de l'économie : *JORF* n°0181 du 5 août 2008.

[1004] BOURGEOIS, M., *Droit de la donnée*, *op. cit.*, n°1592, p. 370.

[1005] TPICE, 18 sept. 1996, n° T-353/94, *Postbank*, *RTD eur.* 1997. 459, chron. BLAISE, J.-B. et IDOT, L.

[1006] TPICE, 22 févr. 2005, n° T-383/03, *Hynix Semiconductor* ; GALLOUX, J.-C., « Droit sur les créations nouvelles », *op. cit.*, p. 87.

[1007] *JORF* n°0174 du 31 juill. 2018.

licite, de dispositions raisonnables, compte tenu des circonstances destinées à les garder secrètes ». Ainsi, la protection du secret d'affaires contient deux éléments[1008]. Le premier est objectif, c'est-à-dire que les informations doivent être inaccessibles au public puisque « secrètes » et elles doivent avoir une valeur commerciale. De ce fait, l'obligation de ne pas divulguer consiste en l'organisation de l'inaccessibilité par des mesures techniques ou juridiques. L'information n'est donc pas portée à la connaissance du public et n'est pas dans le domaine public. La valeur commerciale de l'information résulte pour Mme A. Robin de « *l'avantage concurrentiel que la maîtrise de l'information procure* »[1009]. Le second élément de la protection du secret des affaires est subjectif, il concerne la désignation des informations que les personnes considèrent comme confidentielles. Au vu de ces éléments de définition, devrait pouvoir être protégé par le secret des affaires un grand nombre d'informations telles qu'une recette, un procédé de fabrication, des données techniques ou industrielles, les listes de clients, des méthodes de ventes, etc. Cette définition permet ainsi de « *faciliter les recours juridiques des entreprises pour obtenir réparation suite au vol ou à l'abus des données relevant du secret des affaires* »[1010]. C'est un véritable outil offert aux acteurs qui peuvent mettre en place des méthodes de protection des informations confidentielles dans le cadre de cette loi. Le secret des affaires permet donc de conserver la confidentialité de tout renseignement commercial qui donne à une entreprise un avantage concurrentiel. Selon M. Y. Padova, « *le droit du secret des affaires peut faciliter les transactions tout en garantissant un certain niveau de confidentialité conférant de la valeur à la donnée ainsi protégée* ». Il ajoute que « *la protection par le secret des affaires assurerait ainsi une forme de sécurité juridique aux entreprises entrant dans les relations contractuelles avec d'autres afin d'échanger des données qu'elles détiennent* »[1011]. En effet, le secret des affaires organise les recours juridiques en faveur du détenteur légitime du secret en cas d'atteinte par une action en responsabilité civile[1012]. Cette action se prescrit par cinq ans à compter du jour où le détenteur légitime du secret des affaires a connu ou aurait dû connaître le dernier fait qui en est la cause[1013].

[1008] ROBIN, A., *Droit des données de la recherche. Science ouverte, innovation, données publiques*, Larcier, 2022, n°134, pp. 109-110.
[1009] *Ibid*.
[1010] QUEMENER, M., *Le droit face à la disruption numérique. Adaptation des droits classiques*, Émergence de nouveaux droits, Gualino, 2018, n°1222, p. 284.
[1011] PADOVA, Y., « Entre patrimonialité et injonction au partage : la donnée écartelée ? (Partie I) », *RLDI*, n°155, 2019.
[1012] C. com., art. L. 152-1.
[1013] C. com., art. L. 152-2.

B. La mise en œuvre du secret des affaires

351- Tout d'abord, il est nécessaire de se demander quelles sont les conditions d'application du secret des affaires (**1**), pour ensuite envisager les effets de la violation du secret des affaires (**2**).

1. Les conditions d'application du secret des affaires

352- Identification des informations confidentielles. Avant toute chose, il faut déterminer les informations confidentielles pouvant faire l'objet d'un secret des affaires. La directive sur les secrets d'affaires prévoit que la définition du secret d'affaires doit « *couvrir les savoir-faire, les informations commerciales et les informations technologiques* »[1014]. En revanche sont exclues « *les informations courantes et l'expérience et les compétences obtenues par des travailleurs dans l'exercice normal de leurs fonctions* ». La directive « *exclut également les informations qui sont généralement connues de personnes appartenant aux milieux qui s'occupent normalement du genre d'informations en question, ou qui leur sont aisément accessibles* »[1015].

353- Conditions du secret d'affaires. Les conditions pour établir un secret d'affaires sont prévues à l'article 2 de la directive sur les secrets d'affaires et ont été reprises dans le Code de commerce. L'article L. 151-1 du Code de commerce issu de la loi de transposition de la directive prévoit trois critères applicables à ces informations[1016].

Premièrement, l'information *« n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ces éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité* ». Par conséquent, l'information ne doit pas être connue et facilement accessible, elle doit être conservée secrète. Les données sont collectées et conservées, généralement, dans des réseaux fermés que ce soient des *Datacenter* ou dans des bases de données fermées. Ainsi, il n'est pas facile d'y accéder et tout le monde n'en a pas connaissance. Les détenteurs des données sont également incités à en assurer la sécurité.

Deuxièmement, l'information « *revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret* ». Ainsi, la loi dispose que l'information a une valeur commerciale parce qu'elle est secrète. Cette préposition suppose que toute chose gardée secrète peut avoir

---

[1014] Dir. 2016/943, préc., cons. 14.
[1015] *Ibid.*
[1016] LAPOUSTERLE, J., « La directive (UE) 2016/943 du 8 juin 2016 sur la protection des secrets d'affaires : apports et perspectives de transposition », *Dalloz IP/IT*, n°493, 2016 ; MILCHIOR, R. et FOURGOUX, V., « Directive sur les secrets d'affaires : création d'un nouveau droit de propriété intellectuelle », *AJCA*, n°391, 2016.

une valeur commerciale. Mais leur valeur peut aussi provenir d'ailleurs. La directive propose « *de considérer la valeur commerciale intrinsèque d'une information* »[1017], du moment que *« leur obtention, utilisation ou divulgation illicite est susceptible de porter atteinte aux intérêts de la personne qui en a le contrôle de façon licite en ce qu'elle nuit au potentiel scientifique et technique de cette personne, à ses intérêts économiques ou financiers, à ses positions stratégiques ou à sa capacité concurrentielle* »[1018].

Enfin, l'information « *fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret* ». Cette dernière condition incite la personne qui détient les informations de manière légitime à mettre en œuvre des protections raisonnables pour conserver le secret.

Par conséquent, à la lecture de ces conditions, il apparaît que la notion de secret des affaires recouvre un grand nombre d'informations. Le secret des affaires peut ainsi porter sur des informations très diverses, il peut s'agir « *des informations ou des secrets d'ordre technique » ou « des informations ou des secrets d'ordre commercial* »[1019]. Les premières recouvrent le « *savoir-faire et les données techniques* », les secondes comprennent quant à elles « *les fichiers de clients et de fournisseurs, les méthodes et stratégies commerciales, et les informations sur les coûts et les prix, mais aussi les projets de développement, les sinistres, les études de marché, etc.* »[1020].

354 **Identification du détenteur du secret des affaires.** Le détenteur légitime du secret des affaires est défini à l'article 2 de la directive « *comme toute personne physique ou morale qui a licitement le contrôle d'un secret d'affaires* ». L'article L. 151-2 du Code de commerce reprend cette définition : « *Est détenteur légitime d'un secret d'affaires, celui qui en a le contrôle de façon licite* ». L'article L. 151-3 du Code de commerce précise ce qui constitue des modes d'obtention licite du secret d'affaires, il s'agit « *1°, d'une découverte ou une création indépendante ; 2°, l'observation, l'étude, le démontage ou le test d'un produit ou d'un objet qui a été mis à la disposition du public ou qui est de façon licite en possession de la personne qui obtient l'information, sauf stipulation contractuelle interdisant ou limitant l'obtention du secret* ». Le secret d'affaires ne reconnaît pas un titre ou un droit exclusif de propriété à son détenteur, mais la loi encadre l'action en justice dont le détenteur légitime bénéficie[1021].

[1017] ROBIN, A., « Secret d'affaires et liberté d'expression : l'exercice d'équilibrisme de la directive », *RLDC*, 2016.
[1018] Dir. 2016/943, préc., cons. 14.
[1019] GALLOUX, J.-C, « Droit sur les créations nouvelles », *RTD com.*, 2014, p. 87.
[1020] *Ibid.*
[1021] ROBIN, A., *Droit des données de la recherche, op. cit.*, n°135, pp. 110 et 111.

Dans les textes tant européens que français, cependant, rien n'indique précisément les règles spécifiques qui permettent de déterminer le détenteur légitime. Ceci s'explique par le fait que le secret d'affaires est protéiforme[1022] : il recouvre un très grand nombre de situations et de types d'informations qu'il aurait été difficile de concentrer dans une seule et unique acception. Par conséquent, « *la détermination du détenteur légitime dépend notamment des circonstances de développement ou d'obtention du secret d'affaires ainsi que l'objet même du secret d'affaires* »[1023]. Aussi, dans le cas d'un cumul avec un droit spécial, comme un droit de propriété intellectuelle par exemple, ce sont les règles spéciales qui s'appliqueront au détriment du secret d'affaires. Par conséquent, en présence d'un logiciel ou d'une base de données, le détenteur des droits est celui qui est désigné par le droit de la propriété intellectuelle. En l'absence de règles spéciales, toutefois, c'est le contrat qui désigne le détenteur légitime du secret. La désignation du détenteur légitime permet de le distinguer à la fois des tiers qui n'ont pas connaissance des informations tenues secrètes, mais aussi, des personnes en ayant connaissance, mais qui ne détiennent aucun droit ou prérogative sur celles-ci et enfin des détenteurs qui ont connaissance du secret et qui sont tenus d'une obligation de ne pas divulguer aux tiers vis-à-vis du détenteur légitime. Le contrat permet donc de régler ces différentes situations.

Dans le secteur de l'agriculture numérique, bien souvent, les entreprises de l'*AgTech* qui ont investi pour l'obtention et le traitement des données afin de fournir de l'aide à la décision et des informations utiles aux exploitants agricoles peuvent revendiquer un secret d'affaires sur les données mises à disposition. C'est ainsi que la société Weedec, par exemple, a inclus dans ses contrats une clause de confidentialité afin, notamment, d'interdire la divulgation des données échangées dans le cadre de la mise en œuvre du service qu'elle propose avec l'utilisateur de la plateforme. Dans cette situation, Weedec est donc le détenteur légitime du secret et leurs clients, les utilisateurs de la plateforme, sont détenteurs du secret, mais ne peuvent utiliser les données qui en font l'objet à d'autres fins que ce qui est prévu par le contrat.

365- **Détenteur légitime du secret d'affaires et détenteur des données.** Il faut distinguer d'ores et déjà les notions de détenteur légitime du secret d'affaires et le détenteur des données prévu dans le règlement n°2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données[1024]. En effet, ces deux notions ne portent pas sur le même objet. Le secret d'affaires porte sur des informations qui ont fait l'objet de mesures techniques et juridiques de

[1022] BOUVET, T., « Détermination du détenteur légitime des droits sur un secret d'affaires », *Rev. Prop. Ind.*, 2018.
[1023] *Ibid.*
[1024] *JOUE* L 152/1 du 3 juin 2022.

confidentialité. En revanche, le détenteur des données[1025] est désigné dans le règlement sur la gouvernance des données comme « *[la] personne morale ou [la] personne concernée qui, conformément au droit de l'Union ou au droit national applicable, a le droit de donner accès à certaines données à caractère personnel ou à caractère non personnel qu'elle contrôle ou de les partager* »[1026]. La Proposition de règlement sur les données de février 2022[1027] propose de retenir une définition similaire[1028]. Ces deux notions ne sont donc pas synonymes et peuvent se cumuler. En effet, le détenteur de données qui contrôle l'accès aux données qu'il détient est souvent également celui qui met en place les mesures techniques et juridiques du secret. Ainsi, ce sont les entreprises de l'agriculture numérique qui détiennent les données dans le secteur agricole et ce sont elles aussi qui organisent la confidentialité de ces données.

356- **Identification des mesures de protection.** Les mesures de protection sont de plusieurs ordres, il peut s'agir de mesures techniques, de mesures juridiques ou encore de mesures juridictionnelles. S'agissant des mesures techniques, il peut s'agir de code d'accès, de verrouillage informatique, « *Data centralisation room, cryptage, cahiers de laboratoire, traçabilité, restrictions d'accès, contrôle des communications avec l'extérieur, mesures de prévention*[1029] »[1030] ou bien encore, M. O. de Maison Rouge préconise de classer les données confidentielles de l'entreprise constitutives d'un avantage concurrentiel, ainsi que de délimiter les personnes qui ont accès à ces données[1031]. Parmi les mesures juridiques, il faut noter que la loi sur le secret des affaires ne chasse pas le contrat, bien au contraire, ce dernier permet de mettre en œuvre le secret[1032]. Il peut donc s'agir de « *clauses de confidentialité des contrats de travail, de sous-traitance, d'accords de confidentialité, etc.* »[1033]. Il est donc possible de prévoir une clause de confidentialité[1034] dans les contrats afin de contraindre les cocontractants au secret. Enfin, les articles L. 152-3 et suivants du Code de commerce prévoient désormais des mesures juridictionnelles pour prévenir et faire cesser une atteinte au secret des affaires. Le juge

[1025] Voir *supra*, n°22.
[1026] Règlement sur la gouvernance des données, préc., art. 2.
[1027] Proposition de règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données), COM/2022/68 final.
[1028] *Ibid.*, art. 2 : « *Une personne morale ou une personne physique qui, conformément au présent règlement, aux dispositions législatives applicables de l'Union ou à la législation nationale mettant en œuvre le droit de l'Union, a le droit ou l'obligation ou, dans le cas de données à caractère non personnel et par le contrôle de la conception du produit et des services liés, a la possibilité, de rendre disponibles certaines données à caractère personnel* ».
[1029] Voir sur les précautions en matière informatique, le site de l'ANSSI.
[1030] *Ibid.*
[1031] MAISON-ROUGE (de), O., « Le secret des affaires : Une protection juridique des données stratégiques », *sur le site de Village de la justice*, 2 août 2018.
[1032] GARINOT, J.-M., « Secret des affaires : la loi ne chasse pas le contrat », *AJCA*, 2018, p. 412.
[1033] *Ibid.*
[1034] Voir *supra*, n°339 et s.

peut, en effet, « *sans préjudice de l'octroi de dommages et intérêts, prescrire, y compris sous astreinte, toute mesure proportionnée de nature à empêcher ou à faire cesser une telle atteinte* »[1035]. Les conditions d'application du secret des affaires sont relativement larges et seule la mise en œuvre de mesures préventives raisonnables permet de bénéficier du régime de protection du secret d'affaires. Mais, en l'absence de mise en conformité avec la directive du secret d'affaires, les détenteurs légitimes du secret ne pourront se prévaloir de sa protection[1036].

357- **Exceptions.** Aujourd'hui, la question se pose de savoir quelle est la limite entre le secret et la divulgation de l'information ? En effet, certaines personnes ont payé le prix fort dans leur guerre contre le secret. C'est le cas par exemple de Julian Assange poursuivi depuis 2010 par les États-Unis pour avoir diffusé des informations classées confidentielles du gouvernement américain sur les guerres d'Afghanistan et d'Irak *via* son site *Wikileaks* au nom de la transparence. Aussi, afin de trouver un équilibre entre liberté d'expression, droit à l'information et secret, la directive n°2016/943 prévoit des dérogations au secret des affaires en son article 5. Ces exceptions permettent de protéger la liberté d'expression et le droit à l'information ainsi que de révéler une faute, un acte répréhensible ou une activité illégale dans un intérêt public général ou encore d'agir aux fins de la protection d'un intérêt légitime reconnu par le droit de l'Union ou le droit national. Ainsi, les dérogations au secret des affaires permettent dans certaines circonstances de divulguer ou de diffuser des données confidentielles. En outre, pour divulguer ces informations, encore faut-il y avoir préalablement accès[1037]. Seule la contrainte permet d'obliger le détenteur d'un secret à diffuser les informations qu'il détient. C'est pourquoi des réflexions sont aujourd'hui menées afin d'obliger certains opérateurs privés à mettre à disposition leurs données dans certaines situations[1038]. C'est le cas notamment des données environnementales encadrées par la Convention d'Aarhus de 2018. À ce titre, les données phytosanitaires pourraient à terme être concernées par l'obligation de diffusion par des personnes privées au nom du droit à l'information[1039]. Néanmoins, il faut rappeler que même les données publiques sont soumises au secret des affaires[1040]. Cette difficulté d'accès aux données conduit certaines associations et certains journalistes à employer des moyens illégaux pour obtenir des informations confidentielles. Il appartient donc aux juges de délimiter les atteintes au secret.

[1035] MATTATIA, F., *Droit d'auteur et propriété intellectuelle dans le numérique*, Eyrolles, 2e éd., 2019, p. 42.
[1036] PUËLL, P., « Secret des affaires : Une mise en conformité nécessaire », *Expertises*, nov. 2020, n°462, p. 371.
[1037] GALLOUX, J.-C., « Libres propos sur le droit d'accès aux données », *op. cit*., p. 14.
[1038] ROBIN, A, *Droit des données de la recherche, op. cit*., p. 174.
[1039] Pour un exemple concret, voir *supra*, n°159 et s.
[1040] Voir *supra*, n°116.

358- Plusieurs affaires récentes peuvent servir d'illustration pour l'articulation entre plusieurs droits et libertés fondamentaux. En effet, afin de dénoncer les conditions de traitement des animaux dans certains élevages des journalistes et des associations n'hésitent pas à pénétrer sans autorisation dans des locaux privés afin de capter des images dans le but de les diffuser et d'informer le grand public sur le non-respect du bien-être animal. Aussi, dans une affaire opposant l'association Red Pill (ex-DXE) en tant que lanceuse d'alerte, la société Konbini en tant que média, et la société EARL Nantel en tant qu'éleveuse de volailles, s'est posé la question de l'articulation entre le droit à l'information et le droit de propriété. Dans cette affaire, les membres de l'association et une équipe de tournage avaient pénétré dans les locaux de l'éleveur dont les portes n'étaient pas fermées et avaient tourné des images sans autorisation. L'éleveur avait été informé de l'existence de cette vidéo et avait demandé sa suppression sur le fondement d'un trouble manifestement illicite constitué par une atteinte au droit de propriété, une violation de domicile et le non-respect de la réglementation sanitaire. L'association et le média avaient alors opposé leur liberté d'expression et leur droit d'informer et avaient souligné le caractère nécessaire et proportionné des moyens employés. Ils considéraient que ces moyens étaient légitimes afin d'informer le débat public et d'alerter les consommateurs. Néanmoins, dans un arrêt rendu en référé, la Cour d'appel de Rennes[1041], confirmant le jugement du tribunal de Saint-Malo, avait fait droit à la demande de la société Nantel et avait condamné solidairement l'association Red Pill et le média Konbini pour atteinte à l'image et au droit de propriété de l'éleveur. Ainsi, les juges ont considéré que le droit à l'information et la liberté d'expression ne justifiaient pas une atteinte au droit de propriété en retenant qu'aucune circonstance ne justifiait que la liberté d'information ne soit opposée au droit de propriété de l'exploitant. Néanmoins, cette décision pourrait être annulée en raison d'une jurisprudence récente de la Cour de cassation. En effet, dans une autre affaire dont les faits étaient similaires, cette même association avait également été condamnée par la Cour d'appel de Rennes dans un arrêt du 17 mars 2020[1042]. Les juges avaient retenu que « *la liberté d'expression ne pouvait, à l'évidence être opposée sérieusement au droit de propriété de l'exploitant et que le juge des référés n'avait pas à rechercher un équilibre entre le droit de propriété et le droit d'informer ou encore à vérifier le caractère proportionné des moyens utilisés pour l'information du public dès lors que l'association avait pénétré dans les locaux de celle-ci sans y être autorisée ni par la propriétaire ni par le juge* ». Mais, le 2 février 2022, la Cour de cassation[1043] a cassé et annulé

[1041] CA Rennes, 1ère ch., 14 déc. 2021, n°20/03118.
[1042] CA Rennes 1ère ch., 17 mars 2020, n°19/06749.
[1043] C. cass, 1ère civ., 2 févr. 2022, n°20-16.040, *Association Red Pill.*

cet arrêt en retenant, en vertu d'une jurisprudence constante de la Cour européenne des droits de l'homme, qu'en présence de deux droits conventionnellement protégés, le juge national devait toujours procéder à une mise en balance des intérêts en présence afin de rechercher un équilibre entre les droits en concours et le cas échéant, privilégier la solution la plus protectrice de l'intérêt le plus légitime[1044]. Or, les restrictions à la liberté d'expression devaient nécessairement répondre à un besoin social impérieux, en particulier lorsqu'elles concernent un sujet d'intérêt général, tel que la protection des animaux[1045]. Aussi, la Cour d'appel de Rennes qui n'avait pas fait la balance entre la liberté d'expression contenue à l'article 10 de la Convention européenne des droits de l'homme (CEDH) et le droit au respect des biens reconnu à toute personne physique ou morale de l'article 1er du protocole additionnel de la CEDH a vu son arrêt cassé. La Cour de cassation a rappelé l'obligation des juges du fond d'effectuer un contrôle de proportionnalité lorsque des droits et libertés d'égale valeur entrent en conflit. Le droit à l'information n'est donc pas systématiquement inférieur au droit de propriété ou au droit à l'image. Au vu de ces éléments, dans le cas de la formation d'un pourvoi en cassation par l'association Red Pill et le média Konbini l'arrêt de la Cour d'appel de Rennes rendu le 14 décembre 2021 pour des faits similaires pourrait donc également faire l'objet d'une cassation pour cette même raison.

Par conséquent, désormais, lorsque des données confidentielles seront divulguées, sur le fondement d'une dérogation comprise à l'article 5 de la directive n°2016/943, le juge devra opérer un contrôle de proportionnalité entre les droits et les libertés concernés.

2. Les effets de la violation du secret des affaires

359- **Comportements répréhensibles.** La directive sur le secret des affaires a pour objectif de sanctionner « *l'obtention, l'utilisation ou la divulgation d'un secret d'affaires* », mais aussi, « *la commercialisation de biens en infraction* »[1046].

D'abord, l'article L. 151-3 du Code de commerce définit ce qu'est l'obtention licite d'un secret des affaires. Il doit s'agir d'une « *découverte* » ou « *[d'] une création indépendante* » ou « *l'observation, l'étude, le démontage ou le test d'un produit ou d'un objet qui a été mis à la*

[1044] CEDH, 5 janv. 2000, *Beyeler c/ Italie*, n°33202/96, pt 107 ; CEDH, 16 juill. 2014, *aliae et autres c/ Bosnie-Herzégovine, Croatie, Serbie, Slovénie et l'ex-République yougoslave de Macédoine*, n°60642/08, pt 108.
[1045] CEDH, 30 juin 2009, *Verein gegen Tierfabriken Schweiz* c/ *Suisse [GC]*, n°32772/02, pt 92 ; CEDH, 22 avr. 2013, *Animal Defenders International* c/ *Royaume-Uni [GC]*, n°48876/08, pts 103 à 105.
[1046] BOURGEOIS, M., *Droit de la donnée, op. cit*., n°1601, p. 373 ; Dir. n°2016/943, préc., art. 2, 4.

disposition du public ou qui est de façon licite en possession de la personne qui obtient l'information, sauf stipulation contractuelle interdisant ou limitant l'obtention du secret ».

Ensuite, l'article L. 151-4 du Code de commerce précise que l'obtention du secret des affaires est illicite « *lorsqu'elle est réalisée sans le consentement de son détenteur légitime et qu'elle résulte : 1o D'un accès non autorisé à tout document, objet, matériau, substance ou fichier numérique qui contient le secret ou dont il peut être déduit, ou bien d'une appropriation ou d'une copie non autorisée de ces éléments ; 2o De tout autre comportement considéré, compte tenu des circonstances, comme déloyal et contraire aux usages en matière commerciale* ».

De même, l'utilisation ou la divulgation est illicite lorsqu'elle résulte d'une violation d'une obligation de ne pas divulguer le secret ou de limiter son utilisation[1047].

L'obtention, l'utilisation ou la divulgation est encore illicite lorsque la personne savait ou aurait dû savoir au regard des circonstances, que ce secret avait été obtenu, directement ou indirectement, d'une personne qui l'utilisait ou le divulguait de façon illicite[1048].

Enfin, l'obtention, l'utilisation ou la divulgation de façon illicite des secrets d'affaires du fournisseur au sens de la directive n°2016/943 est une pratique commerciale déloyale interdite. C'est ce que rappelle notamment la Directive n°2019/633 du 17 avril 2019 sur les pratiques commerciales déloyales dans les relations interentreprises au sein de la chaîne d'approvisionnement agricole et alimentaire[1049].

360- **Sanctions de l'atteinte à un secret des affaires.** Les États membres mettent en place des procédures permettant d'obtenir une réparation[1050]. En outre, la directive précise que « *ces mesures peuvent consister, notamment, le cas échéant, à allouer des dommages et intérêts au défendeur, à imposer des sanctions au demandeur ou à ordonner la diffusion d'informations relatives à une décision* »[1051]. Ainsi, les sanctions sont laissées à l'appréciation des États membres, il peut s'agir de mesures provisoires et définitives et/ou de dommages et intérêts. Mais encore, l'article 1 de la loi n°2018-670 du 30 juillet 2018 a introduit un certain nombre de sanctions. C'est ainsi que toute atteinte au secret des affaires engage la responsabilité de son auteur[1052]. Les actions sont prescrites par cinq ans à compter du jour où le détenteur légitime du secret des affaires a connu ou aurait dû connaître le dernier fait qui en est la cause[1053]. Le

[1047] C. com., art. L. 151-5.
[1048] C. com., art. L. 151-6.
[1049] *JOUE* L 111/59, 25 avr. 2019.
[1050] Dir. n°2016/943, préc. art. 6.
[1051] *Ibid*., art. 7, 2.
[1052] C. com., art. L. 152-1.
[1053] C. com., art. L. 152-2.

juge peut, sans préjudice de l'octroi de dommages et intérêts, prescrire, y compris sous astreinte, toute mesure proportionnée de nature à empêcher ou à faire cesser une telle atteinte[1054]. Elle peut ordonner des mesures provisoires et conservatoires[1055] et ordonner le versement d'une indemnité à la partie lésée[1056]. Pour fixer les dommages et intérêts, la juridiction prend en compte les conséquences économiques négatives de l'atteinte au secret des affaires, le préjudice moral et les bénéfices réalisés par l'auteur de l'atteinte au secret des affaires[1057]. Enfin, la juridiction peut ordonner toute mesure de publicité de la décision relative à l'obtention, l'utilisation ou la divulgation d'un secret des affaires[1058].

361- **« Droit de propriété embryonnaire ».** La réservation exclusive d'une chose peut s'apparenter à un droit de propriété. Par conséquent, certains auteurs avancent l'idée que les données font l'objet d'une emprise possessoire[1059]. Ce qui se traduit finalement par la possibilité de conserver secrètes des données ou d'imposer un accès aux tiers. Pour une autrice, Mme M.-A. Chardeaux, « *toute valeur non appropriée dont le droit organise la réservation et la commercialisation grâce à une technique imitant la propriété, puisée dans le droit commun des contrats, le droit pénal ou dans les actions en responsabilité civile, constitue un bien et est de manière corrélative soustraite à la catégorie des choses communes, en l'absence de catégorie tierce* »[1060]. Par conséquent, la possibilité de réservation des données par le secret des affaires les ferait entrer dans la catégorie des biens. Ainsi, une loi ne serait pas toujours nécessaire pour faire d'une chose un bien[1061]. C'est ce que retient, en tout cas, une partie de la doctrine[1062]. M. le professeur P. Catala évoque, à ce sujet, la notion de « *propriété embryonnaire* »[1063].

362- **Apparente corrélation entre propriété et confidentialité.** En ce qui concerne les données, si une telle analyse leur était applicable, la propriété ne pourrait jamais être pleine et entière. Le détenteur de données ne semble, en effet, pas pouvoir obtenir les mêmes prérogatives qu'un propriétaire. Pour illustrer ce propos, l'article 2276 du Code civil organise un droit de suite pour

---

[1054] C. com., art. L. 152-3 (L. n°2018-670 du 30 juill. 2018, art. 1er).
[1055] C. com., art. L. 152-4.
[1056] C. com., art. L. 152-5.
[1057] C. com., art. L. 152-6.
[1058] C. com., art. L. 152-7.
[1059] THINK TANK GENERATION LIBRE, *Mes Data sont à moi. Pour une patrimonialité des données personnelles*. Rapport, 2018, pp. 57 à 58 ; BINCTIN, N., « Données et secret des affaires », Colloque – Circulation des données et propriétés intellectuelles, *PI*, avr. 2020, n°75, p. 41.
[1060] CHARDEAUX, M.-A., *Les Choses communes, op. cit.*, n°67, p. 69.
[1061] *Ibid.*
[1062] ZENATI, F. et REVET, TH., *Les biens*, 2e éd., refondue, PUF, 1997, n°7, p. 22 : « *Dès lors qu'un objet apparaît utile et appropriable, qu'il entre peu ou prou dans le commerce, il devient objectivement un bien et devrait être considéré comme tel quoi qu'en dise – surtout : que n'en dise pas – la loi* ».
[1063] CATALA, P., « La propriété de l'information », in MARTY G., ss. dir., *Mélanges offerts à P. RAYNAUD*, Paris, *D.S.*, 1985, p. 97, spéc. n°31, p. 110.

le propriétaire qui lui permet de revendiquer la chose pendant trois ans à compter du jour de la perte ou du vol contre celui dans les mains duquel il la trouve. Or, lorsque les données ou les informations sont divulguées, le détenteur légitime ne peut pas revendiquer un droit de suite opposable aux tiers. En effet, si un tel droit existe pour les œuvres de l'esprit avec le droit d'auteur, les données ne semblent pas pouvoir en bénéficier. Il paraît impossible d'obtenir une telle prérogative sur les données puisqu'elles ont pour caractère justement d'être non-exclusives et non-rivales. Ces caractères qui leur sont intrinsèques empêcheraient donc toute revendication dessus après leur diffusion. Ainsi, il n'y a pas de continuité du droit de propriété sur les données. Le droit de propriété sur l'information par le secret d'affaires est donc très limité, voire inexistant. C'est pourquoi d'ailleurs la loi n'évoque pas de droit de propriété, mais bien une détention légitime sur les données. Il s'agit seulement d'un fait juridique non opposable, contrairement au droit de propriété[1064] qui est opposable à tous. Ainsi, « *intimement liée à des comportements fautifs connus, la violation du secret des affaires ne s'apparente, ni de près ni de loin, à la violation d'un droit de propriété* »[1065].

Par conséquent, il est possible de convenir que le secret d'affaires consacre une réservation privative de l'information qui devient dès lors un actif incorporel susceptible d'une détention ou d'une possession exclusive. Le secret des affaires permet donc d'envisager la patrimonialité des données[1066].

363- **Conclusion de la section.** Les données collectées sur les exploitations agricoles peuvent faire l'objet d'une réservation privative au moyen du contrat associé à des mesures techniques. Le détenteur légitime du secret qui se trouve bien souvent être le détenteur des données, lui-même, c'est-à-dire l'entreprise de l'*AgTech,* assure ainsi la non-divulgation des données qu'elle détient aux tiers au contrat. Cette réservation peut aussi assurer aux collecteurs de données, bien souvent, les agriculteurs, la non-divulgation des informations concernant leur méthode de travail ou leur savoir-faire sur leur élevage ou leur exploitation. Néanmoins, des limites à la réservation de l'information servent de garde-fou et permettent de diffuser des données ou des informations qui démontreraient des activités illégales ou encore des actes répréhensibles. La divulgation doit donc servir l'intérêt général ou l'intérêt légitime tel que le respect de

[1064] ROBIN, A., « Agriculture numérique, données et droit : topographie juridique de l'"écosystème informationnel vert" », *Sciences Eaux & Territoires*, 2019, p. 40.
[1065] ROBIN, A., « Secret d'affaires et liberté d'expression : l'exercice d'équilibrisme de la directive », *op. cit.*
[1066] PADOVA, Y., « Entre patrimonialité et injonction au partage la donnée écartelée (Partie I et II) », *op. cit.*

l'environnement ou le bien-être animal. Dans ce cas, c'est le juge qui opère le contrôle de constitutionnalité entre les droits et libertés en présence.

Section 2. La sécurisation technique de l'accès aux données agricoles contre les actions des tiers

364- Les entreprises et les établissements publics qui détiennent les données des agriculteurs mettent en œuvre des mesures juridiques et techniques afin de les protéger contre les éventuelles atteintes et intrusions des tiers dans les systèmes informatiques de réservation. Il convient donc tout d'abord d'envisager le principe légal de la protection contre les atteintes aux données (**§1**), pour ensuite s'intéresser au régime de protection applicable à ces atteintes (**§2**).

§1. *Le principe légal de la protection contre les atteintes aux données*

365- En premier lieu, il faut s'intéresser à la répression pénale des atteintes aux données (**I**) pour, en second lieu, envisager la reconnaissance légale des atteintes spécifiques aux données (**II**).

I. La répression pénale de l'atteinte aux données

366- En droit pénal, deux délits permettent de sanctionner le détournement et la soustraction des données dans certaines circonstances, d'abord, par l'abus de confiance (**A**), ensuite, par le vol (**B**).

A. L'abus de confiance

367- L'étude de l'abus de confiance suppose d'envisager son incrimination (**1**) ainsi que le délit de détournement des données (**2**).

1. L'incrimination de l'abus de confiance

368- **Fondement.** L'abus de confiance est sanctionné au titre des articles 314-1 et suivants du Code pénal, c'est « *le fait par une personne de détourner au préjudice d'autrui, des fonds, des valeurs ou un bien quelconque qui lui ont été remis et qu'elle a acceptés à charge de les rendre, de les*

représenter ou d'en faire un usage déterminé ». L'abus de confiance est sanctionné de cinq ans d'emprisonnement et de 375 000 euros d'amende.

369- **Conditions.** Pour qu'il y ait abus de confiance, la chose doit avoir été remise volontairement et à titre précaire[1067]. Ce qui signifie qu'il ne doit pas y avoir de transfert de propriété. L'abus de confiance permet donc de sanctionner le détournement d'une chose qui aura été remise volontairement et à titre précaire à une personne à charge pour lui de le restituer, de le représenter ou d'en faire un usage déterminé.

2. La prise en compte des choses corporelles

370- **Évolution jurisprudentielle.** Si avant 2000, la jurisprudence de la Cour de cassation faisait une nette distinction entre les biens corporels et incorporels pour l'application du délit d'abus de confiance[1068], elle a renversé sa jurisprudence par un arrêt du 14 novembre 2000[1069]. Dans cette décision, la Cour de cassation a jugé que « *constitue un abus de confiance le fait de détourner le numéro de carte bancaire communiqué par un client pour un paiement déterminé et par là même, d'en faire un usage non convenu entre les parties* ». Désormais, tout bien quelconque peut faire l'objet d'un détournement qu'il soit corporel ou incorporel, tel qu'un numéro de carte bancaire ou des informations comme celles portant sur la clientèle[1070]. Ainsi, dans une seconde décision, du 22 octobre 2014, la chambre criminelle de la Cour de cassation[1071] a retenu que celui qui s'est rendu coupable du détournement de données après une remise volontaire et précaire pourra être sanctionné au titre de l'abus de confiance. Dans cette affaire, le prévenu a été reconnu coupable d'abus de confiance pour avoir « *en connaissance de cause, détourné en les dupliquant, pour son usage personnel, au préjudice de son employeur, des fichiers informatiques contenant des informations confidentielles et mis à disposition pour un usage professionnel* ». Aussi, le seul fait de dupliquer des données qui ont été remises volontairement peut être sanctionné au titre de l'abus de confiance. Pour une partie de la doctrine, cette décision permet de reconnaître « *implicitement la qualification des données comme un "bien" de l'entreprise* »[1072]. Or, il ne faut pas se tromper d'objet dans cette affaire. Ce sont les informations contenues dans les données qui ont été détournées, c'est-à-dire les

[1067] Crim., 5 avr. 2018, pourvoi n°17-81.085, *Bull. crim.* 2018, n°62.
[1068] Crim., 9 mars 1987, pourvoi n°84.91-977, *Bull. crim.* 1987, n°11.
[1069] Crim., 14 nov. 2000, pourvoi n°99-84.522, *Bull. crim.*
[1070] Crim., 16 nov. 2011, pourvoi n°10- 87.866, *Bull. crim.* 2011, n°233 ; Crim., 22 mars 2017, pourvoi n°15-85.929, *Bull. crim.* 2017, n°78.
[1071] Crim. 22 oct. 2014, pourvoi n°13-82.630, : JurisData n°2014-024941.
[1072] PADOVA, Y, « Entre patrimonialité et injonction au partage, la donnée écartelée ? (partie I) », *op. cit.*

informations portant sur la clientèle. La jurisprudence reconnaît la clientèle comme ayant une valeur patrimoniale qu'elle soit civile[1073] ou commerciale[1074]. En effet, la clientèle est considérée comme objet de droit de propriété protégé par l'article 1er du Protocole n°1 de la CEDH[1075]. Par conséquent, ce ne sont pas les données en elles-mêmes qui forment les biens de l'entreprise, mais les informations concernant la clientèle.

Également, avant que le secret des affaires soit reconnu par la loi, l'abus de confiance avait pu être mobilisé dans plusieurs affaires. En effet, un ancien salarié de Michelin avait été condamné à deux ans d'emprisonnement avec sursis et à une amende de 5000 euros[1076] pour avoir proposé à plusieurs sociétés concurrentes de la société Michelin de leur vendre des données confidentielles. De même, dans l'affaire Valeo, une ancienne stagiaire chinoise avait téléchargé sur son disque dur des fichiers confidentiels de l'équipementier automobile Valeo et avait été condamnée pour abus de confiance[1077]. Néanmoins, l'abus de confiance est difficile à mobiliser dans le cadre des données puisqu'il faut, nécessairement, une remise préalable de la chose qui s'inscrit généralement dans une relation contractuelle. Il n'est pas suffisamment efficace pour sanctionner toutes les violations du secret des affaires.

B. Le vol de données

371- Si le vol était à l'origine conditionné par la soustraction d'un élément matériel (**1**), la Cour de cassation a fait évoluer sa jurisprudence pour finalement reconnaître le vol de données sans support (**2**).

1. La condition initiale de soustraction d'un élément matériel

372- Évolution jurisprudentielle sur le vol de données avec soustraction de support matériel. La jurisprudence pénale a pu laisser entendre que les données entraient dans la catégorie des biens en qualifiant de vol la simple soustraction de données. En effet, pour que la qualification de « vol » soit retenue en droit pénal, l'article 311-1 du Code pénal exige « *la soustraction frauduleuse de la chose d'autrui* ». La doctrine et la jurisprudence reconnaissent que le droit pénal est d'interprétation stricte et que cette formulation suppose l'aspect tangible de la chose.

[1073] Civ. 1re, 7 nov. 2000, n°98-17.731, *Bull.* 2000, n°283, p. 183.
[1074] C.E.D.H., Cour (pleinière), 26 juin 1986, aff. *Van Marle et autres c/ Pays-Bas*, n°8543/79 et autres.
[1075] C.E.D.H., 16 nov. 2018, aff., req. n°21623/13, *Könyv-Tar KFT et autres c/ Hongrie*.
[1076] TGI Clermont-Ferrand, ch. corr., 21 juin 2010 : Dr. pén. 2010, comm. 116, M. Véron.
[1077] TGI Versailles, 18 déc. 2007, n°0511965021, *L. c/ Valéo* : *CCE*. 2008, comm. 62, CAPRIOLI, É.

Ce n'est qu'à partir de la fin des années 1980 que la jurisprudence a assoupli sa position en admettant le vol d'informations à la seule condition qu'il y ait soustraction, même momentanée, d'un support matériel (disquette, document, etc.) contenant les informations soustraites[1078]. Il faut noter que pour Mme M.-P. Lucas de Leyssac, « *une telle interprétation ne méconnaît pas les principes fondamentaux de la matière pénale* »[1079]. En effet, « *la façon d'appréhender une chose varie nécessairement avec la nature de celle-ci, et la chambre criminelle l'a expressément admis depuis longtemps, précisément, en matière de vol* »[1080].

Dans le domaine informatique, plusieurs décisions d'espèce ont admis la reconnaissance du vol de données sur ce même fondement, dès lors qu'il y a « soustraction » d'un élément matériel contenant les données (fichier, document ou encore support)[1081]. La donnée peut se présenter sous diverses formes (papier, numérique, etc.), « *mais elle est en tout état de cause matérialisée ou fixée sur un support* »[1082]. Cela supposait de bien distinguer la chose sur laquelle sont fixées les données des données elles-mêmes en tant « *[qu'] élément[s] immatériel[s] distinct[s] de tout support de stockage* »[1083].

2. Le vol de données sans support matériel

373- **Revirement de jurisprudence.** Si, par la suite, plusieurs décisions ont admis le vol de données sans support[1084], ce n'est qu'en 2015, dans l'affaire *Bluetouff*[1085], que la Cour de cassation a véritablement entériné le vol de données. Dans cet arrêt du 20 mai 2015, le prévennou s'était introduit sur le site extranet d'une agence de l'État, à la suite d'une défaillance technique. Après avoir constaté l'existence d'un contrôle d'accès, il s'était maintenu frauduleusement dans le

---

[1078] Crim., 12 janv. 1989, n°87-82.265 ; Crim. 1er mars 1989, n°88-82.815.
[1079] ROCHFELD, J., *La propriété dans la jurisprudence de la Cour de cassation*, La documentation française, ét. annuelle 2019, p. 29.
[1080] LUCAS DE LEYSSAC, M.-P., « L'arrêt Bourquin, une double révolution : un vol d'information seule, une soustraction permettant d'appréhender des reproductions qui ne constitueraient pas des contrefaçons », *RSC*, n°3, juill. - sept. 1990, pp. 507 à 520.
[1081] Crim 8 janv. 1979, aff. *Logabax*, n°77-93038, *Bull. crim.* n°13 ; *D.* 1979, p. 509, note CORLAY, P ; Cass. crim., 12 janv. 1989, aff. *Bourquin*, n°87-82265, *Bull. crim*. n°14 ; JurisData n°1989-700634 ; *RSC* 1990, p. 346, obs. BOUZAT, P. et 507, obs. LUCAS DE LEYSSAC, M.-P. ; *RTD com.* 1990, p. 143, obs. BOUZAT, P. ; *Bull. crim*. 1989, n°14 ; *DIT*. 1989, p. 34, obs. DEVEZE J. ; *Gaz. Pal.*, 14/15 juill. 1989, p. 23, obs. DOUCET ; *Expertises* 1989, p. 269 ; Cass. crim., 1er mars 1989, aff. *Antonioli*, n°88-82815, *Bull. crim.* n°100 ; JurisData n°1989-001418 ; *D.* 1990, p. 330, note HUET, J. ; *RSC* 1990, p. 346, obs. BOUZAT, P. et 507, obs. LUCAS DE LEYSSAC, M.-P. ; *RTD com.* 1990, p. 142, obs. BOUZAT ; P. ; *D.* 1990, somm. p. 230, obs. HUET, J. ; *JCP E* 1990, II, 15761, obs. VIVANT, M. et LUCAS, A. ; *Gaz. Pal.* 12 nov. 1989, n°306, jur. p. 18 ; JC*P G* 1989, n°21, IV, p. 186 ; *JCP E*, 1989, n°21, I, p. 141 ; *D.* 1990, n°37, p. 330.
[1082] *Ibid.*
[1083] AN, *Rapport n°2173, renforçant les dispositions relatives à la lutte contre le terrorisme*, 22 juill. 2014, art. 11 bis (nouveau).
[1084] Crim., 9 sept. 2003, n°02-87.098 ; Crim., 4 mars 2008, n°07-84.002 ; Crim., 27 avril 2011, n°10-86.233.
[1085] Crim., 20 mai 2015, n°14-81.336, préc.

site, avait téléchargé des données puis les avait transmises à des tiers. La Cour de cassation a retenu la qualification de vol pour le maintien dans un système de traitement automatisé protégé. Le prévenu a alors été sanctionné pour avoir soustrait les données et les avoir utilisées sans le consentement de leur propriétaire.

374- **Discussion du choix de qualification.** Il peut paraître, de prime à bord, étonnant que les juges aient retenu la qualification de vol dans cette affaire alors même que la loi du 13 novembre 2014 relative à la lutte contre le terrorisme, modifiant l'article 323-3 du Code pénal[1086] était déjà entrée en vigueur. Cette loi est en effet venue modifier la loi Godfrain de 1988 relative à la fraude informatique[1087], qui condamnait l'introduction, la soustraction ou la modification frauduleuse de données dans un Système de Traitement Automatisé de Données (STAD), mais ne permettait pas de sanctionner la copie des données. Ce choix avait été fait à l'époque de ne pas tenir « *compte de la captation sans droit de données ou programmes enregistrés au motif précisément que de tels faits paraissaient constituer un vol* »[1088]. Ainsi, la loi du 13 novembre 2014[1089] a ajouté cette possibilité et l'article 323-2 du Code pénal sanctionne désormais le délit d'intrusion et d'entrave au fonctionnement d'un système automatisé de données. Depuis son entrée en vigueur, cet article permet de sanctionner l'extraction et la reproduction de données sans avoir recours à l'incrimination de vol. Néanmoins, les faits de l'affaire *Bluetouff* étant antérieurs à la promulgation de la loi du 13 novembre 2014, ils ne pouvaient être appliqués au cas d'espèce. Il faut gager donc que le vol n'aura pas souvent l'occasion d'être retenu dans le futur puisque l'incrimination des atteintes aux systèmes de traitement automatisé de données est un texte spécifique, plus sévère, d'application suffisamment large pour prendre en compte l'ensemble des cas de soustraction de données.

375- **Téléchargement d'informations personnelles sur le serveur d'une entreprise.** Dans une affaire plus récente, du 28 juin 2017, les juges ont dû se prononcer sur la soustraction d'informations sans atteinte à un STAD. Ici, la Cour de cassation a retenu la qualification « *[d']appropriation frauduleuse* » (en lieu et place de « *soustraction frauduleuse* » qui qualifie le vol) par tout moyen de production, d'informations personnelles sur un réseau informatique

[1086] ROBIN A., « Le statut juridique ambivalent du fichier : de l'appropriation de la compilation à la réservation de l'information », *in* EDAZZI, F. et MAUCLAIR, S., ss. dir., *Le fichier*, Actes du colloque organisé à la Faculté de Droit d'Orléans, 26 & 27 nov. 2015, *LGDJ*, 2016.p°215.
[1087] Loi n°88-19, 5 jan. 1988, relative à la fraude informatique (loi Godfrain) : *JORF* du 6 janv. 1988.
[1088] ROCHFELD, J., « La propriété dans la jurisprudence de la Cour de cassation », *op. cit.*, p. 36.
[1089] Loi n°2014-1353 du 14 nov. 2014 renforçant les dispositions relatives à la lutte contre le terrorisme : *JORF* n°0263 du 14 nov. 2014.

d'une entreprise[1090]. Dans les faits, il n'y avait pas eu d'atteinte à un système de traitement automatisé de données puisque l'affaire concernait deux avocats d'une même société civile professionnelle (SCP) qui partageaient un système informatique interne au cabinet. Le prévenu, dans le cadre d'un litige l'opposant à l'un de ses associés, avait remis au bâtonnier des doubles de correspondances et des copies de courriers adressés et destinés à son associée contre le gré de celle-ci et à des fins étrangères à la SCP. Le prévenu, dans le cadre de son pourvoi, contestait les décisions de première et seconde instance qui retenaient la qualification de vol au motif, notamment, qu'il avait librement accès aux informations depuis un terminal de l'entreprise sans passer par un mot de passe ce qui constituait une preuve de leur appartenance à l'entreprise. La Cour de cassation a rejeté le pourvoi en retenant que l'associée n'avait pas entendu donner au prévenu « *la disposition des documents personnels dont elle était propriétaire* » et que « *le libre accès à des informations personnelles sur un réseau informatique d'une entreprise n'est pas exclusif de leur appropriation frauduleuse par tout moyen de reproduction* ». Néanmoins, si cette jurisprudence reconnaît le « *vol d'informations partagées* »[1091], il faut observer le fait que cette décision concernait des informations personnelles. Une partie de la doctrine s'est interrogée sur la qualification de vol dans cette affaire. Elle se demandait si en raison de l'absence de protection des données et du libre accès, ces informations n'avaient pas été librement remises aux tiers emportant de fait la qualification d'abus de confiance. Or, « *au regard de la jurisprudence, il apparaît que la remise d'informations à un tiers et la détention qui en résulte impliquent soit que le propriétaire lui ait donné l'autorisation de les utiliser dans un cadre donné (c'est l'hypothèse du détournement des numéros de carte bancaire évoqué ci-dessus), soit que ces données aient été reproduites sur un support (physique ou informatique), lui-même détenu par ce tiers* »[1092]. Ainsi, « *la simple possibilité de prendre connaissance librement d'une information n'emporte donc ni sa remise ni sa détention* »[1093]. En revanche, pour retenir l'appropriation frauduleuse, il doit y avoir une duplication des informations qui nécessite une « *reproduction, matérielle ou immatérielle* »[1094]. En effet, ce qui est sanctionné ce n'est pas le fait d'accéder aux données dans le STAD, mais de les reproduire sur un autre espace de l'ordinateur ou du réseau. Ici encore, les faits étaient antérieurs à la promulgation de

[1090] Crim., 28 juin 2017, n°16-81.113, BEAUSSONIE, G., *D.* 2017. 1885, DESGENS-PASSANAU, G., *Dalloz, IP/IT*, 2017. 663, ROUJOU DE BOUBEE, G., *D.* 2017. 2501 ; SAENKO, L., *RTD. com.* 2017. 713 ; MATSOUPOULOU, H., *RSC* 2017. 752.
[1091] ROCHFELD, J., « La propriété dans la jurisprudence de la Cour de cassation », *op. cit.*, p. 37.
[1092] *Ibid.*, p. 41.
[1093] *Ibid.*
[1094] LASSERRE CAPDEVILLE, J., « Nouvelle solution favorable au vol d'informations », obs. Cass. crim., 28 juin 2017, n°16-81.113, *AJ Pénal*, 2017, p. 448.

la loi du 13 novembre 2014. Par conséquent, les juges ne pouvaient faire application de la réglementation sur l'extraction des données d'un STAD.

Si ces deux décisions ont entériné le vol d'information, ce n'est que par anticipation de l'entrée en vigueur de la loi du 13 novembre 2014. Aussi, en vertu de la maxime, *specialia generalibus derogant*, l'adoption d'un texte spécifique sur les atteintes aux STAD aura pour effet de réduire la portée de ces arrêts d'espèce.

II. La reconnaissance légale de l'atteinte spécifique aux données

376- Le législateur a reconnu l'intrusion et l'entrave à un système de traitement automatisé de données comme étant répréhensibles (**A**). Cette infraction a ensuite été étendue au délit d'extraction de données (**B**).

A. La répression de l'intrusion et de l'entrave à un STAD

377- Il faut, d'abord, envisager le contexte de la répression de l'intrusion et de l'entrave à un STAD (**1**) pour ensuite étudier la reconnaissance légale de la répression de l'intrusion et de l'entrave à un STAD (**2**).

1. Le contexte de la répression de l'intrusion et de l'entrave à un STAD

378- Jusqu'en 1988, aucun dispositif juridique ne permettait de sanctionner l'intrusion dans un système de traitement de données. Certaines données très sensibles pouvaient donc être piratées sans qu'aucune sanction n'existe. L'absence de sanction laissait planer un sentiment d'impunité pour ces infractions dématérialisées. Pourtant, les nouvelles technologies offrent un véritable terrain de jeux pour les cybercriminels et la cybercriminalité a pris de l'ampleur au cours de ces dernières décennies. Il n'existe, d'ailleurs, aujourd'hui, plus une semaine sans que des cyberattaques fassent les titres des journaux.

2. La reconnaissance légale de la répression de l'intrusion et de l'entrave à un STAD

379- Le législateur a pris en compte assez tôt ce phénomène facilité par le développement d'Internet et de l'informatique et a réprimé, pour la première fois, spécifiquement, les atteintes à un

système de traitement automatisé de données dans la loi n°88-19 du 5 janvier 1988. Celle-ci a été codifiée aux articles 323-1 et suivants du Code pénal. Aujourd'hui, ces articles répriment l'ensemble des atteintes à un système informatique, « *mais aussi le fait d'entraver ou de fausser le fonctionnement de ces systèmes, d'altérer les données et de mettre à disposition d'autrui un équipement permettant d'accomplir ces infractions* »[1095]. De plus, l'article 323-1, alinéa 1er du Code pénal, dispose que « *le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie, d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 euros d'amende* ». Par la suite, une compilation de textes est venue s'ajouter à cette réglementation. D'abord, le législateur est venu réprimer les infractions commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État par une loi du 27 mars 2012[1096]. Ensuite, la loi du 24 juillet 2015 a augmenté les peines de cette infraction[1097]. Ainsi, cette incrimination permet de clore le débat sur la question du vol de données[1098]. Mais, la loi de modification qui doit retenir l'attention est celle du 13 novembre 2014 qui a permis de reconnaître le délit d'extraction des données, avec ou sans copie.

B. L'extension de la répression de l'atteinte à un STAD au délit d'extraction des données

380- Le législateur a reconnu le délit d'extraction frauduleuse des données (**1**) afin de réprimer les comportements délictueux en matière de données (**2**).

1. Répression de l'extraction de données

381- Le législateur a renforcé le délit d'intrusion et d'entrave au fonctionnement d'un STAD en réprimant le fait d'extraire frauduleusement des données informatiques avec la loi du 24 novembre 2014 relative à la lutte contre le terrorisme, codifié à l'article 323-3 du Code pénal. Ainsi, il n'est plus besoin de démontrer une soustraction frauduleuse d'un bien matériel pourtant condition du délit de vol ou la remise d'une chose prévue contractuellement pour

[1095] FILIPPI (De), P. et DULONG DE ROSNAY, M., « Le piratage informatique, un explorateur des courants juridiques du réseau », *Revue de Sciences humaines Tracés*, n°26, 2014.
[1096] Loi n°2012-410 du 27 mars 2012, relative à la protection de l'identité : *JORF* n°0075 du 28 mars 2012, art. 9.
[1097] Loi n°2015-912 du 24 juill. 2015, relative au renseignement (1) : *JORF* n°0171 du 26 juill. 2015, art. 4.
[1098] ROBIN, A., « Secret d'affaires et liberté d'expression : l'exercice d'équilibrisme de la directive », *op. cit.*

l'abus de confiance afin de démontrer l'atteinte à des données contenues dans un système d'information. Cette reconnaissance permet d'éviter l'écueil du vol de données.

2. Répression des comportements délictueux en matière de données

382- Un groupement d'experts (CYBERLEX et CECyF) a analysé la répression des comportements délictueux en matière de données. Ils ont conclu que l'article 323-3 du Code pénal dans sa nouvelle formule permet de couvrir l'ensemble de ces comportements « *sous réserve de l'absence d'interprétation restrictive des tribunaux* »[1099]. En effet, l'article 323-3 du Code pénal sanctionne le fait d'introduire des données frauduleusement dans un système de traitement automatisé, mais aussi, le fait d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données. Le groupement d'experts s'est interrogé également sur la définition de l'extraction et a conclu qu'il s'agissait de la même définition que celle appliquée aux bases de données[1100].

§2. *Le régime juridique de la protection contre les atteintes aux données*

383- Une fois que les données sont contenues dans un système informatique, la loi prévoit désormais des sanctions à l'encontre de ceux qui tenteraient d'y accéder sans autorisation, de les extraire ou bien encore de les modifier. Ce dispositif offre une protection pour les agriculteurs dont les données sont protégées par des systèmes informatiques. Cette protection pourrait, néanmoins, se retourner contre eux, à l'image des agriculteurs du Nebraska[1101] contraints de pirater leur propre matériel agricole afin de les réparer eux-mêmes à moindre coup. En effet, des constructeurs de machines agricoles, tels que *John Deere*, implantent des logiciels dans leurs machines qui sont accessibles seulement par les concessionnaires agréés. Aussi, les agriculteurs sont obligés de passer par eux afin de réparer leur tracteur à des prix prohibitifs et dans des délais très longs. Les agriculteurs peuvent se transformer alors en pirate informatique pour accéder aux données des logiciels intégrés dans leurs machines au moyen de logiciels pirates ukrainiens, afin de les réparer eux-mêmes. En outre, l'infraction d'atteinte à un STAD suppose d'identifier le STAD lui-même (**I**), avant d'envisager la répression des atteintes à ce STAD (**II**).

[1099] CYBERLEX et CECyF, *Code pénal et lutte contre la cybercriminalité : Proposition pour une efficacité juridique renforcée*, Rapport, 25 janv. 2017, p. 10.
[1100] Sur la notion d'extraction, voir *supra*, n°255.
[1101] EUDES Y., « Les agriculteurs hackeurs du Nebraska », *op. cit.*

I. L'identification d'un système de traitement automatisé de données

384. Dans un premier temps, il convient d'analyser la notion de STAD (**A**) pour, dans un second temps, caractériser le STAD lui-même (**B**).

A. La notion de STAD

385. La notion de STAD suppose que soient envisagés d'abord sa définition (**1**) puis son contenu (**2**).

1. La définition d'un STAD

386. **Absence de définition légale et propositions doctrinales.** Avant tout développement juridique, il convient d'envisager ce à quoi fait référence la notion de système de traitement automatisé de données (STAD). Le Code pénal n'en propose aucune définition, il en va de même pour les lois relatives aux STAD[1102].

La doctrine, quant à elle, se réfère à la définition qui avait été proposée lors des débats parlementaires de la loi n°88-19 du 5 janvier 1988 (dite loi « Godfrain »)[1103], dans un rapport rédigé, le 22 décembre 1987, par le sénateur Jacques Thyraud. Selon ce rapport, le STAD correspond à « *tout ensemble composé d'une ou plusieurs unités de traitement, de mémoires, de logiciels, de données, d'organes d'entrées-sorties, et de liaisons qui concourent à un résultat déterminé, cet ensemble étant protégé par des dispositifs de sécurité* »[1104]. Certains auteurs relèvent que cette définition exige l'existence de dispositifs de sécurité alors que cette condition n'est pas attendue par la loi[1105].

387. **Validation prétorienne.** Malgré les critiques, cette définition a été reprise par la jurisprudence et, notamment, dans l'affaire *Kerviel* par les juges de la Cour d'appel de Paris le 24 octobre

[1102] Loi n°88-19, 5 janv. 1988, préc. ; Loi n°2015-912, 24 juill. 2015 préc. ; Loi n°2014-1353, 13 nov. 2014, préc. ; Loi n°2012-410 du 27 mars 2012, préc.
[1103] Loi n°88-19 du 5 janvier 1988, préc.
[1104] THYRAUD, J., Rapport n°3 fait au nom de la commission des lois, Doc. Sénat, 1987-88., p. 52.
[1105] LEPAGE, A., « Un an de droit pénal des nouvelles technologies (oct. 2012-oct. 2013) », *Dr. pén*. 2013, chron. 11, cité par STASIAK F., « L'affaire K. vue avec un peu de recul », *RLDA*, n°97, 1er oct. 2014.

2012[1106]. Dans cet arrêt, les juges précisent que la définition ainsi posée est « *immédiatement intelligible* » et ne pose pas de « *difficulté d'interprétation* ».

388- **Universalité de fait.** Quelques auteurs retiennent la notion d'universalité de fait, à l'image de M. le Professeur. R. Gassin dans son article « *la protection pénale d'une nouvelle "universalité de fait" en droit français : les systèmes de traitement automatisé de données* »[1107]. Ainsi, les éléments informatiques attaqués doivent être intégrés à un système pour que la sanction puisse s'appliquer[1108]. C'est pour cela qu'un disque dur, qui est donc un élément externe, n'est pas retenu comme un STAD par la jurisprudence[1109].

2. Les contours de la notion de STAD

389- La jurisprudence a défini les contours de la notion au fil des décisions. Un grand nombre de systèmes intègrent aujourd'hui la notion : c'est le cas par exemple du réseau informatique d'un cabinet d'avocats[1110], d'un système bancaire[1111], du service informatique d'un CHU[1112]. Il peut aussi s'agir « *[d']une puce électronique de carte de paiement, de téléphone mobile, un site internet, une base de données ou un autocommutateur téléphonique* »[1113]. La Cour de cassation a également pu reconnaître « *[l']usage et la détention d'un keylogger matériel* »[1114] comme un STAD (il s'agit d'un enregistreur de frappe installé en douce et qui permet la capture des caractères frappés sur le clavier). Dans cette affaire, le médecin incriminé avait pu, par le biais de ce système, prendre connaissance de la messagerie de ses confrères[1115].

[1106] CA Paris, pôle 5, ch. 12, 24 oct. 2012, n° RG : 11/00404, *Jérôme Kerviel c/ ministère public*, *JCP E* 2012, 1702, note MORTIER, R., Bull. Joly Bourse 2013, p. 87, note RONTCHEVSKY, N., *RSC*, 2013, p. 381, obs. STASIAK, F., *JCP G* 2012, 1371, note LASSERRE CAPDEVILLE, J.

[1107] GASSIN, R., « La protection pénale d'une nouvelle "universalité de fait" en droit français : les systèmes de traitement automatisé de données », *ALD*, 16 févr. 1989.

[1108] VIVANT, M., WARUSFEL, B., MALLET-POUJOL, N. et COSTES, L., *Le Lamy droit du numérique*, 2019, n°2513.

[1109] CA Douai, ch. Corr., 21 oct. 2008, *Juris-Data*, n°2008-374086.

[1110] Crim., 10 mai 2017, *Juris-Data*, n°2017-008826.

[1111] CA Paris, Pôle 5, 12e ch., 24 oct. 2012, préc.

[1112] Crim. 16 janv. 2018, *Juris-Data*, n°2018-000269.

[1113] QUEMENER, M., *Le droit face à la disruption numérique*, *op. cit.*, n°317, p. 98.

[1114] https://www.nextinpact.com/news/106061-la-cour-cassation-precise-infractions-entourant-lusage-et-detention-dun-keylogger.htm.

[1115] Crim. 16 janv. 2018, préc. : « *qu'en effet, se rend coupable de l'infraction prévue à l'article 323-1 du code pénal la personne qui, sachant qu'elle n'y est pas autorisée, accède, à l'insu des victimes, à un système de traitement automatisé de données* ».

B. La caractérisation des STAD

390- Afin de caractériser un STAD, il faut seulement démontrer son existence (**1**). Toutefois, l'existence de dispositifs de sécurité n'est pas exigée pour reconnaître le délit d'intrusion et d'entrave au fonctionnement d'un STAD (**2**).

1. Les caractéristiques du STAD

391- Existence. La caractérisation du STAD est un préalable évident à la reconnaissance du délit incriminé. Afin de le caractériser, les tribunaux reconnaissent aujourd'hui une acception large de la notion[1116]. Il suffit qu'un système soit protégé par des mesures techniques dans le but de produire un résultat déterminé pour démontrer son existence. Le système est un ensemble composé d'éléments tels que des unités de traitements, de mémoire, de logiciels, de données ou encore d'organes d'entrées et de sorties. Les « éléments » sont toute technologie, dispositif, composant qui empêche ou limite les utilisations non autorisées, tels qu'un code d'accès, un procédé de protection tel qu'un cryptage, un brouillage ou toute autre transformation de l'objet de la protection ou d'un mécanisme de contrôle de la copie qui a atteint cet objectif de protection[1117]. Le résultat déterminé est le traitement automatisé de données.[1118] Ainsi, ont été reconnus comme STAD par les tribunaux, le réseau du GIE cartes bancaires[1119], un logiciel considéré isolément[1120], le réseau « France Télécom »[1121], etc. Par exemple, un logiciel intégré à un tracteur dont l'accès est réservé au moyen d'un mot de passe forme un STAD.

2. Le dispositif de sécurité non exigé

392- L'ensemble d'éléments techniques ayant pour finalité le traitement des données peut être protégé par des dispositifs de sécurité[1122], mais la jurisprudence ne subordonne pas l'application de l'article 323-1 du Code pénal à l'existence d'un tel dispositif. L'infraction est constituée dès le moment où l'agent n'avait pas le droit d'accéder ou de se maintenir dans le système de

[1116] TGI Nîmes, 28 juin 2013, n°13/1677, CAPRIOLI, E., *CCE*, n°1, janv. 2014, comm. 11.
[1117] CPI, art. L. 331-5.
[1118] CPI, art. L. 331-5 ; Loi n°2021-1382 du 25 oct. 2021 relative à la régulation et à la protection de l'accès aux œuvres culturelles à l'ère numérique (1) : *JORF* n°0250 du 26 oct. 2021, art. 1.
[1119] TGI Paris, 13e ch., 25 févr. 2000 : JurisData n°2000-134655 ; *D.* 2000, p. 219.
[1120] CA Douai, 7 oct. 1992 : JurisData n°1992-49432.
[1121] TGI Paris, 12e ch., 26 juin 1995 : *LPA* 1996, n°27, p. 4, note ALVAREZ.
[1122] CA Paris, 30 oct. 2002, *Kitetoa c/ Sté Tati*, *CCE*, 2003.

traitement automatisé de données[1123]. Il suffit que le maître du système matérialise son intention d'en restreindre l'accès aux seules personnes autorisées[1124]. L'entreprise n'a donc pas l'obligation de mettre en œuvre un dispositif de sécurité sur son système pour faire reconnaître une atteinte.

II. La répression des atteintes au STAD

393- L'étude des atteintes au STAD suppose d'analyser, dans un premier temps, les comportements répréhensibles (**A**), pour envisager, dans un second temps, la sécurisation des données par les prestataires de services de l'agriculture numérique (**B**).

A. Les comportements répréhensibles sur les STAD

394- L'élément matériel de l'infraction peut se matérialiser de plusieurs manières : par l'accès ou le maintien frauduleux dans un STAD[1125] (**1**), par l'atteinte ou l'entrave au fonctionnement d'un STAD[1126] (**2**), par l'action frauduleuse commise sur les données d'un STAD, à savoir le fait « *d'introduire (…), d'extraire, de détenir, de produire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient* »[1127] (**3**), ou enfin, par la détention ou l'offre d'un dispositif permettant la réalisation d'une atteinte à un STAD[1128] (**4**).

1. L'accès ou le maintien frauduleux dans un STAD

395- L'article 323-1 du Code pénal sanctionne « *le fait d'accéder ou de se maintenir, frauduleusement, dans toute ou partie d'un système de traitement automatisé de données* », ce délit est puni de deux ans d'emprisonnement et de 60 000 euros d'amende[1129]. Cette sanction est aggravée à trois ans d'emprisonnement et 100 000 euros d'amende lorsqu'il en est résulté « *la suppression ou la modification des données contenues dans le système* »[1130]. Ainsi, le simple fait d'accéder et/ou de se maintenir dans un STAD sans autorisation permet de constituer

[1123] ROBACZEWSKI, C., « Atteinte aux systèmes de traitement automatisé de données », *J-Cl. Pénal*,19 févr. 2010.
[1124] CA Paris, 5 avr. 1994, *JCP E*, 1995, I, 461, obs. VIVANT, F. et Le STANC, C.
[1125] C. pénal, art. 323-1.
[1126] C. pénal, art. 323-2.
[1127] C. pénal, art. 323-3.
[1128] C. pénal, art. 323-3-1.
[1129] C. pénal, art. 323-1, al.1.
[1130] C. pénal, art. 323-1 c., al. 2.

l'infraction[1131]. Dès lors que cette infraction est commise à l'encontre d'un STAD mis en œuvre par l'État, la peine est de cinq ans d'emprisonnement et de 150 000 euros d'amende.

2. L'atteinte ou l'entrave à un STAD

396- De manière autonome, l'article 323-2 du Code pénal dispose qu'est puni de cinq ans d'emprisonnement et de 75 000 euros d'amende « *le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données* ». L'atteinte peut consister en un déni de services distribués lorsque l'attaque à l'encontre d'un serveur, par exemple, empêche les utilisateurs d'accéder au site ainsi bloqué. Le tribunal correctionnel de Paris a dans ce sens jugé que l'intéressé a accédé frauduleusement à tout ou partie d'un STAD, au serveur hébergeant le site internet de la société EDF, ou s'y est maintenu frauduleusement et a « *entravé ou faussé le fonctionnement d'un STAD, en l'espèce en participant à une attaque par déni de services distribués contre le serveur hébergeant le site internet de la société EDF (http://www.edf.com) ayant conduit à son blocage* »[1132]. Ces atteintes ont donné lieu à une condamnation de six mois d'emprisonnement avec sursis et de 29 000 euros de dommages et intérêts en faveur de la société EDF.

L'entrave à un système de traitement automatisé de données peut consister en des faits matériels comme « *un sabotage, vol d'une carte ou de l'introduction d'un virus* »[1133]. Il faut que l'acte ait « *pour effet d'entraver le fonctionnement du système informatique* »[1134]. C'est le cas notamment « *[lorsqu']un individu détourne les internautes et les revenus publicitaires générés sur un site internet* » comme l'a jugé la Cour d'appel de Paris dans un arrêt du 14 novembre 2017[1135].

[1131] CA Paris, pôle 4, 10e ch., 5 févr. 2014, www.legalis.net : « *La cour d'appel de Paris a condamné pour maintien frauduleux à un système automatisé de données et vol de fichiers un journaliste qui s'était introduit dans l'extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (Anses) et y avait récupéré des documents dont l'accès n'était pas protégé* » ; QUEMENER M., *Le droit face à la disruption numérique*, *op. cit.*, n°317, p. 98.

[1132] TGI, Paris, 13e ch. corr. 1, 28 sept. 2016.

[1133] QUEMENER, M., *Le droit face à la disruption numérique, op. cit.*, n°322, p. 100.

[1134] *Ibid.*

[1135] CA Paris, pôle 5, ch. 14, 14 nov. 2017 : « *M. X. ne peut raisonnablement invoquer l'erreur de droit pour prétendre à la licéité de l'introduction d'un lien hypertexte dans le site internet exploité par Up To Ten, alors que cette introduction n'avait d'autre fin que de capter à son profit, l'ensemble des ressources engendrées par la consultation du site par les internautes ; Qu'il a ainsi sciemment entravé en le faussant, le fonctionnement normal du système de traitement automatisé mis en œuvre par UpToTen* ».

3. L'action frauduleuse sur les données d'un STAD

397. La Loi n°2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme a modifié l'article 323-3 du Code pénal. Cette infraction « v*ise à sanctionner les destructions de fichiers ou de bases de données, la modification de données bancaires ou comptables qui permettent par exemple des détournements de fonds importants* »[1136]. L'affaire *Kerviel*[1137] évoquée précédemment en est une illustration. Aussi, le fait de pouvoir sanctionner l'extraction de données met un terme au débat sur la potentialité de sanctionner un « vol » de données. Dorénavant en présence d'un délit d'extraction, de détention, de reproduction, de transmission, de suppression ou de modification de données, les juges se fonderont sur l'article 323-3 du Code pénal et non plus sur celui de l'article 311-1 qui sanctionne le vol.

4. La détention ou l'offre d'un dispositif permettant la réalisation d'une atteinte à un STAD

398. L'article 323-3-1 du Code pénal sanctionne « *le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3* ». Il s'agit là de sanctionner la production ou la détention de virus, mais aussi la publication de faille informatique qui permettraient de porter atteinte à un STAD. C'est en ce sens que s'est prononcée, la chambre criminelle de la Cour de cassation dans un arrêt du 27 octobre 2009[1138].

De plus, il faut noter que l'article 323-4 du Code pénal prévoit les sanctions lorsque ces infractions sont commises par groupement ou lors d'une entente établie. Il s'agit « *des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée* »[1139]. Par exemple, un arrêt de la chambre criminelle de la Cour de cassation du 7 novembre 2017[1140] a

---

[1136] QUEMENER, M., *op. cit.*, n°324, p. 100.
[1137] Crim., 19 mars 2014, n°12-87.416.
[1138] Crim., 27 oct. 2009, n°09-82.346 : « *La constatation qu'il a agi sans motif légitime et en connaissance de cause établit l'intention coupable de celui qui, en violation de l'article 323-3-1 du code pénal, importe, détient, offre, cède ou met à disposition un moyen ou une information conçue ou spécialement adaptée pour commettre une infraction d'atteinte aux systèmes de traitement automatisé de données. Justifie sa décision la cour d'appel qui retient qu'un prévenu ne pouvait arguer d'un motif légitime tiré de la volonté d'information dès lors que, du fait de son expertise, il savait qu'il diffusait des informations présentant un risque d'utilisation à des fins de piratage* ».
[1139] C. pénal, art. 323-4.
[1140] Crim., 7 nov. 2017, n°16-84918.

rejeté le pourvoi qu'une personne avait formé à l'encontre de l'arrêt de la Cour d'appel de Paris du 30 juin 2016 qui l'avait condamné « *pour participation à une entente établie en vue de la préparation d'une entrave au d'un fonctionnement d'un système automatisé de données* ». Il faut également souligner que la simple tentative est elle aussi punissable des mêmes peines que les infractions elles-mêmes, au titre de l'article 323-7 du Code pénal. Des peines complémentaires sont fixées à l'encontre des personnes physiques à l'article 323-5 du Code pénal[1141] et des personnes morales à l'article 323-6 du Code pénal[1142].

L'élément intentionnel se déduit des circonstances matérielles de la réalisation de l'infraction. La jurisprudence ne punit pas les erreurs de manipulation informatique non intentionnelles[1143]. Néanmoins le fait pour l'auteur d'une telle erreur de se maintenir ensuite dans le système une fois qu'il a réalisé qu'il n'était pas autorisé à le faire constitue l'élément intentionnel. Il faut donc caractériser la volonté du contrevenant[1144].

B. La responsabilisation des entreprises de l'agriculture numérique sur la question de la sécurisation des données

399- Les entreprises de l'agriculture numérique ont une responsabilité légale de sécuriser les données agricoles qu'elles détiennent (**1**) qui consiste en une obligation de sécurisation (**2**).

1. La responsabilité légale

400- Les personnes morales doivent mettre en œuvre les sécurités suffisantes afin d'éviter que des failles de sécurité permettent la pénétration par des cyberattaquants dans les systèmes de

[1141] C. pénal, art. 323-5 : « *Les personnes physiques coupables des délits prévus au présent chapitre encourent également les peines complémentaires suivantes : 1° L'interdiction, pour une durée de cinq ans au plus, des droits civiques, civils et de famille, suivant les modalités de l'article 131-26 ; 2° L'interdiction, pour une durée de cinq ans au plus, d'exercer une fonction publique ou d'exercer l'activité professionnelle ou sociale dans l'exercice de laquelle ou à l'occasion de laquelle l'infraction a été commise ; 3° La confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit, à l'exception des objets susceptibles de restitution ; 4° La fermeture, pour une durée de cinq ans au plus, des établissements ou de l'un ou de plusieurs des établissements de l'entreprise ayant servi à commettre les faits incriminés ; 5° L'exclusion, pour une durée de cinq ans au plus, des marchés publics ; 6° L'interdiction, pour une durée de cinq ans au plus, d'émettre des chèques autres que ceux qui permettent le retrait de fonds par le tireur auprès du tiré ou ceux qui sont certifiés ; 7° L'affichage ou la diffusion de la décision prononcée dans les conditions prévues par l'article 131-35* ».

[1142] C. pénal, art. 323-6 : « *Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39. L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise* ».

[1143] CA Paris, 30 oct. 2002, *Kitetoa c/ Sté Tati* : *CCE*, 2003, 5.

[1144] Crim., 20 mai 2015, n°14-81.336.

traitement automatisé[1145]. En effet, tout d'abord, la directive « Sécurité » du 6 juillet 2016 a pour objectif d'établir des mesures visant à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union afin d'améliorer le fonctionnement du marché intérieur[1146]. Elle vise les opérateurs de services essentiels et les fournisseurs de services numériques. Ces derniers doivent donc répondre à des exigences en matière de sécurité et de notification dès lors qu'ils utilisent des réseaux et des systèmes d'information définis à l'article 4 de la directive[1147]. Ces réseaux doivent par conséquent être sécurisés. Ensuite, la directive relative aux attaques contre les systèmes d'information du 12 août 2013[1148] prévoit qu'à défaut de mise en œuvre d'une protection suffisante contre les cyberattaques, la responsabilité des entreprises prestataires de services peut être engagée. Également, sur le plan civil, l'entreprise peut engager sa responsabilité pour faute[1149], pour négligence ou imprudence[1150].

2. L'obligation de sécurisation

401- **Le secteur agricole, nouvelle cible des cyberattaques.** Avec l'ampleur que prennent les nouvelles technologies dans le secteur agricole, la question de la sécurisation des données devient un problème majeur[1151]. Si ce secteur était jusqu'à présent épargné par les cyberattaques, il ne l'est plus désormais[1152]. Plusieurs attaques ont en effet pu être identifiées. Par exemple, des cyberattaquants peuvent utiliser des rançongiciels qui permettent de voler des données et d'exiger une rançon en échange d'un avantage concurrentiel. Également, des failles de sécurité peuvent potentiellement permettre à des individus malintentionnés de falsifier des données pour perturber les marchés du secteur agricole. De même, des données peuvent être récupérées dans le but d'endommager les cultures en modifiant les ordres donnés aux objets

[1145] FERAL-SCHUHL, C., ss. dir., *Cyberdroit, op. cit.*, n°511.11.
[1146] Dir. n°2016/1148 du 6 juill. 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union : *JOUE* L 194/1 du 19 juill. 2016, art. 1.
[1147] « *Réseau et système d'information : a) un réseau de communications électroniques au sens de l'article 2, point a), de la directive 2002/21/CE; b) tout dispositif ou tout ensemble de dispositifs interconnectés ou apparentés, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques; ou c) les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b) en vue de leur fonctionnement, utilisation, protection et maintenance* ».
[1148] Dir. n°2013/40/UE du 12 août 2013, relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil : *JOUE* L 218/8 du 14 août 2013.
[1149] C. civ., art. 1240.
[1150] C. civ., art. 1241.
[1151] SAINT-ARNAUD, P., « L'informatisation de l'agriculture ouvre la porte à la cybercriminalité », La Presse Canadienne, *L'actualité*, 25 avr. 2021.
[1152] PAYSAN BRETON, « Le cyber-risque désormais présent dans le secteur agricole », *Paysan Breton, Hebdomadaire Technique Agricole*, 26 mars 2021.

connectés, en perturbant à distance ces objets ou encore en les mettant hors service. Notamment, des animaux sensibles aux conditions climatiques pourraient être victimes du piratage d'un système de régulation de la température en échange d'une rançon, ce qui aurait, pour effet, la perte des animaux et du chiffre d'affaires.

402- Par conséquent, les détenteurs de données devraient toujours être tenus de sécuriser les données agricoles spécifiquement afin d'éviter toute cyberattaque ou toute perte des données, à l'image de la sécurisation des données personnelles[1153]. D'ailleurs, la *Soft Law* prévoit une obligation de protection et de sécurisation des données à l'encontre de l'entreprise qui collecte/fournit les données. En effet, tant la Charte Data-Agri que le Code de conduite de l'Union européenne relatif au partage des données agricoles par accord contractuel incitent les parties à définir dans leur contrat les responsabilités de chacun. En effet, le premier texte encourage à prévoir « *les responsabilités en matière de sécurité et d'atteinte à la confidentialité des données* »[1154] tandis que le second incite à prévoir « *de manière explicite les responsabilités en matière de sécurité et de confidentialité de l'utilisateur / du fournisseur de données* »[1155].

403- **Conclusion de la section.** Le droit reconnaît la possibilité pour les entreprises de sécuriser l'accès aux données qu'elles détiennent. Cette possibilité de sécurisation est à la fois une aubaine pour l'agriculteur puisqu'elle permet de protéger les données de son exploitation contre les attaques extérieures. Mais cette sécurisation représente également un risque pour l'agriculteur de se voir imposer des limites à l'accès aux données des objets connectés qu'il utilise sur son exploitation.

404- **Conclusion du chapitre.** Les outils juridiques et techniques à la disposition des entreprises agricoles leur permettent de réserver les données qu'elles détiennent, parfois au préjudice des agriculteurs qui perdent alors la maîtrise de l'accès aux données qu'ils génèrent. Ainsi, les entreprises de l'*AgTech* peuvent à partir de ces données améliorer les services et les outils qu'elles développent pour le secteur et conserver un monopole sur certaines informations. En outre, elles devraient toujours être tenues de respecter une obligation de sécurisation sur ces données.

[1153] Voir *infra*, n°767 et s.
[1154] Charte Data-Agri, préc., art. 11.
[1155] Code de conduite de l'Union européenne relatif au partage des données agricoles par accord contractuel, préc., p. 11.

405- **Conclusion du titre.** Tant le droit des bases de données que le contrat et la loi permettent, aujourd'hui, aux acteurs de l'agriculture numérique d'organiser un monopole, à la fois, sur le résultat de leurs investissements — les bases de données — et sur les données elles-mêmes. Ainsi, l'organisation de la réservation des données agricoles privées limite l'accès à ces données et leur circulation entre les acteurs du secteur agricole. Une distorsion peut se créer toutefois entre les droits et les obligations des parties au contrat entre les agriculteurs et leurs fournisseurs de matériels et de services quant à la maîtrise de l'accès aux données. Les agriculteurs sont en effet souvent soumis à la volonté de leurs cocontractants, bien que, en France, les entreprises de l'*AgTech* aient, en grande majorité, pris en compte les intérêts de leurs clients afin de protéger les intérêts du secteur agricole. Dans une autre mesure, théoriquement, le contrôle de l'accès pourrait avoir pour effet une distorsion de la concurrence en cas d'abus de position dominante pour les entreprises considérées comme des « contrôleurs d'accès ». Quoi qu'il en soit, la tendance de la politique européenne tend vers une ouverture et une circulation des données. Aussi, le droit *sui generis*, avec la réforme en cours, devrait perdre de la force au moins en ce qui concerne les données industrielles.

406- **Conclusion de la partie.** Pour le moment, l'économie de l'agriculture numérique est encore dynamique. Les entreprises adoptent des comportements plutôt réservataires sur les données qu'elles détiennent afin d'en conserver la maîtrise de l'accès. Par conséquent, les agriculteurs n'ont pas véritablement la maîtrise de l'usage des données qu'ils génèrent au moyen des objets connectés qu'ils utilisent sur leur propre exploitation. Or, l'accès est le préambule mais aussi la clef de la maîtrise de l'usage des données. Sans accès aux données, il n'y a pas de maîtrise. Ce n'est qu'en y ayant accès que les agriculteurs pourraient en effet décider si les données qu'ils ont générées peuvent être diffusées, dans quelles mesures elles peuvent l'être, à quelles conditions, qui peut les exploiter, etc.

Partie II. La maîtrise de l'usage des données agricoles

407.- L'étude de la maîtrise ou du contrôle de l'usage des données agricoles oblige à déplacer le curseur de manière plus spécifique sur les seules données issues de l'exploitation agricole et non plus sur l'ensemble des données de l'agriculture numérique. L'objectif était de protéger l'agriculteur en recherchant s'il est possible de lui octroyer la capacité de contrôler l'usage des données de son exploitation, il ne peut donc espérer avoir un contrôle que sur les données qu'il a lui-même générées par son activité. En effet, nous avons démontré dans la partie précédente que les entreprises de l'agriculture numérique, telles que SMAG ou ITK détiennent les données des agriculteurs et en contrôlent l'accès au moyen d'outils juridiques et techniques. Les agriculteurs se retrouvent souvent en position de faiblesse face à ces entreprises qui détiennent leurs données d'exploitation et qui ont la capacité d'en contrôler l'accès. Les agriculteurs perdent donc bien souvent le contrôle de l'usage de leurs données et se soumettent à la volonté de leurs partenaires commerciaux.

Pour donner un exemple du contrôle d'une société de l'agriculture numérique sur l'usage des données agricoles qu'elle détient, les conditions générales d'utilisation d'une application gratuite[1156] sont explicites. Cette application permet de visualiser les données collectées *via* les objets connectés de cette société ou ceux de ses partenaires. Dans la licence d'utilisation, le contenu même de l'application est désigné comme regroupant tous les éléments qui la composent de manière non limitative. Par conséquent, il est possible d'en déduire que les données mises à disposition dans l'application sont comprises dans le contenu de cette application. La société octroie, alors, selon les clauses de la licence à l'utilisateur de l'application — l'agriculteur — un droit d'utilisation sur ce contenu. Ce droit est non exclusif, révocable, non cessible, non transférable et uniquement pour ses besoins propres à l'exclusion de toute autre finalité. En revanche, l'utilisateur n'acquiert aucun droit sur le contenu de l'application, il ne peut pas non plus le reproduire, le représenter, l'adapter ou l'exploiter. De plus, dans une autre clause, l'utilisateur de l'application est désigné par la société comme étant responsable du contenu des données collectées et communiquées dans l'application ainsi que des éventuels droits des tiers. En revanche, les usages possibles sur les données sont définis par la société qui peut les utiliser afin d'améliorer ses propres services ou créer de nouveaux services gratuits ou payants sans que l'utilisateur ne puisse en demander de contrepartie financière. Cet exemple permet de constater que l'agriculteur n'a, d'une part, aucun droit sur

[1156] L'anonymisation des conditions générales d'utilisation est préservée afin de ne pas identifier la société.

les données pourtant collectées sur son exploitation et, d'autre part, qu'il n'a que des devoirs en contrepartie du service rendu. L'agriculteur, afin d'obtenir l'accès au service souhaité, se contente donc le plus souvent d'accepter les licences d'utilisation sans pouvoir les négocier, il se retrouve alors dans une situation de faiblesse vis-à-vis de l'entreprise. La société qui contrôle l'usage des données peut choisir les personnes qui y ont accès et les utilisations possibles. Elle peut également interdire d'autres usages et partages. C'est donc celle-ci qui choisit ce qu'il est possible de faire ou non des données contenues dans l'application qu'elle propose. Par conséquent, reconnaître un droit de contrôle de l'usage à l'exploitant agricole sur ses données d'exploitation doit, entre autres, lui permettre d'obtenir plus de pouvoir dans ses relations avec ses fournisseurs de services et de matériels. C'est aussi, le replacer au centre de l'économie des données agricoles et le protéger contre les utilisations des données à des fins allant à l'encontre de ses intérêts. Il faut, donc, se demander sur quels fondements peut se baser le contrôle de l'usage des données d'exploitation, quel est son contenu et quelles en sont les limites. Aussi après avoir constaté l'absence regrettée de contrôle de l'usage sur les données d'exploitation (**Titre I**), il sera nécessaire d'envisager la création d'un droit de contrôle de l'usage sur les données à caractère non personnel au profit de l'exploitant agricole afin de compléter l'existant, c'est-à-dire la protection portant sur les données à caractère personnel (**Titre II**).

Titre I. L'absence regrettée de contrôle de l'usage des données d'exploitation

408- Aujourd'hui, la tendance qui se dégage est celle de la circulation et de la valorisation des données non personnelles plutôt que leur protection. Il faut, néanmoins, dans un premier temps, constater que le droit ne permet pas à l'exploitant agricole de contrôler l'usage des données issues de son exploitation (**Chapitre 1**). Cependant, la problématique de la protection des données non personnelles de l'exploitation agricole représente des enjeux majeurs en ce qui concerne notamment la souveraineté alimentaire et l'indépendance des agriculteurs. Cette problématique fait écho à celle des ressources génétiques des pays africains exploitées par les pays européens sans leur consentement. Le protocole de Nagoya de 2010[1157], de portée internationale, entré en vigueur le 12 octobre 2014, a pour objectif de mieux protéger les espèces et les écosystèmes et à en partager plus équitablement les bénéfices. Il implique, notamment, que les pays donnent leur consentement pour l'exploitation de leurs ressources, qu'ils soient rétribués et que les savoirs qu'ils abritent soient reconnus. Cet accord est toutefois encore trop peu appliqué aujourd'hui[1158]. Par analogie, comme les pays pillés de leurs savoirs, les agriculteurs souhaitent également pouvoir donner leur consentement avant toute exploitation des données issues de leur exploitation agricole. En effet, ces données peuvent renfermer notamment des informations portant sur leur savoir-faire ou sur des informations qu'ils considèrent comme « sensibles ». C'est pourquoi une tendance parallèle à la réservation des données se développe depuis quelques années, bien que limitée, afin d'offrir la possibilité pour l'exploitant agricole de contrôler l'usage des données non personnelles de son exploitation (**Chapitre 2**).

[1157] Secrétariat de la convention sur la diversité biologique, Protocole de Nagoya sur l'accès aux ressources génétiques et le partage juste et équitable des avantages découlant de leur utilisation, relatif à la convention sur la diversité biologique, 29 oct. 2010, ratifié par la France *via* la loi n°2016-1087 du 16 août 2016 pour la reconquête de la biodiversité, de la nature et des paysages : *JORF* n°0184 du 9 août 2016.

[1158] https://www.alternatives-economiques.fr/contre-piraterie-ressources-genetiques-un-accord-international-pe/00102096

Chapitre 1. L'absence de contrôle par l'agriculteur de l'usage des données d'exploitation non personnelles

409- L'un des objectifs principaux de la collecte et de la production des données d'exploitation n'est pas de les conserver pour soi, mais au contraire de les partager afin de créer une dynamique intellectuelle, de favoriser l'innovation et la recherche et d'assurer le libre jeu de la concurrence. Aussi, l'orientation prise par le législateur ces dernières années tend vers la réutilisation et le partage des données d'exploitation. C'est pourquoi, en premier lieu, le droit pose le principe de la libre réutilisation des données d'exploitation collectées ou produites dans le cadre d'une mission de service public (**Section 1**). En second lieu, les propositions se multiplient afin de créer une gouvernance des données privées et faciliter leur partage. Toutefois, l'impossibilité de contrôler l'usage des données, une fois qu'elles sont diffusées, incite les entreprises à en limiter l'accès afin de conserver la maîtrise exclusive de leur usage (**Section 2**).

Section 1. La libre réutilisation des données publiques d'exploitation

410- Certaines données d'exploitation, telles les données phytosanitaires, que les agriculteurs saisissent dans leur logiciel de gestion deviennent publiques lorsqu'elles sont collectées et diffusées par un organisme public[1159]. Dans ce cas, les données phytosanitaires sont accessibles et réutilisables, puisque le législateur a reconnu le principe de la libre réutilisation des données publiques (**§1**), sous certaines conditions toutefois (**§2**).

§1. *Le principe de la libre réutilisation des données publiques*

411- Il convient d'envisager, dans un premier temps, l'avènement du principe de la liberté de réutilisation des données publiques (**I**), pour, dans un second temps, s'intéresser au périmètre de la liberté de réutilisation des données publiques (**II**).

[1159] Voir *supra*, n°165 et s.

I. L'avènement du principe de la liberté de réutilisation

412- La consécration du principe de la liberté de réutilisation (**A**) suppose d'en envisager le fondement (**B**).

A. La consécration du principe de la liberté de réutilisation

413- La réutilisation des données publiques a été un long processus concrétisé par la directive du 17 novembre 2003 qui a introduit la notion de réutilisation (**1**), mais il faudra attendre 2013 pour que soit admis un véritable droit à la réutilisation (**2**).

1. L'introduction de la notion de réutilisation

414- Tout d'abord, la loi n°78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'Administration et le public[1160] est le texte fondateur de l'ouverture des données. Néanmoins, à cette époque, le législateur n'avait pas encore pris la mesure du potentiel commercial des données publiques. Il faudra attendre 2003 pour que soit adoptée la Directive n°2003/98/CE du 17 novembre 2003 concernant la réutilisation des informations du secteur public (*Public Sector Information Directive* — PSI I)[1161]. Elle a pour objet la mise en place de dispositifs de licences et de redevances afin d'exploiter les externalités positives de l'*Open Data*[1162]. Mais, cette directive ne garantit pas un droit de réutilisation à tous, elle prévoit seulement les modalités de réutilisation que doivent appliquer les États membres dès lors qu'ils adhèrent au principe de réutilisation des informations publiques[1163]. La directive de 2003 a ainsi permis d'introduire la notion de réutilisation et l'a définie en son article 2.4 comme « *l'utilisation par des personnes physiques ou morales de documents détenus par des organismes du secteur public, à des fins commerciales ou non commerciales autres que l'objectif initial de la mission de service public pour lequel les documents ont été produits. L'échange de documents entre des organismes du secteur public aux seules fins de l'exercice de leur mission de service public ne constitue pas une réutilisation* ». Cette directive a été transposée en droit français par l'Ordonnance n°2005-650 du 6 juin 2005 relative à la liberté

[1160] *JORF* du 18 juill. 1978.
[1161] *JOUE* L 345/90 du 31 déc. 2003.
[1162] LALLET, A. et NGUYEN DUY, P., « Communication des documents administratifs », *Rép. cont. adm.*, n°231, juin 2019.
[1163] *Ibid.*

d'accès aux documents administratifs et à la réutilisation des informations publiques[1164]. Celle-ci a introduit un chapitre dans le CRPA intitulé « De la réutilisation des informations publiques » et a supprimé l'article 10 de la loi n°78-753 qui disposait que les documents sont communiqués « *sous réserve des droits de propriété littéraire ou artistique* » et qu'ils ne peuvent être « *reproduits, diffusés ou utilisés à des fins commerciales* ». Il y a alors eu un changement de paradigme puisque l'ordonnance crée un régime fondé sur le principe de la liberté de réutilisation. L'objectif étant de créer un marché européen de l'information[1165].

2. La création d'un véritable droit à la réutilisation

415- La Directive n°2013/37 du 26 juin 2013, concernant la réutilisation des informations du secteur public (PSI II)[1166] a révisé la Directive PSI I du 17 novembre 2003 en consacrant un véritable droit à la réutilisation des informations publiques[1167]. Cette directive a été transposée par la Loi n°2015-1779 du 28 décembre 2015 relative à la gratuité et aux modalités de la réutilisation des informations du secteur public[1168], dite loi Valter qui a instauré un principe de gratuité de la réutilisation des données publiques. La Loi n°2016-1321 du 7 octobre 2016 pour une République numérique (LRN)[1169] a, ensuite, codifié les dispositions relatives à la réutilisation dans le titre II, du livre III du CRPA. Enfin, la Directive n°2019/1024 du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public (PSI III)[1170] a refondu le régime de la réutilisation et aurait dû être transposée avant le 17 juillet 2021. Cette nouvelle directive insiste « *particulièrement sur la nécessité de fournir un accès en temps réel à des données dynamiques (flux de données) issues des capteurs électroniques de toutes sortes* »[1171]. Également, elle crée une nouvelle catégorie de données, les « données de forte valeur »[1172] qui sont « *détenues par les organismes publics ainsi que par les entreprises publiques et [leur] réutilisation est considérée comme comportant d'importants avantages*

[1164] *JORF* n°131 du 7 juin 2005.
[1165] TERESI, L., « L'Open Data et le droit de l'Union européenne (1) » *AJDA*, 2016 : « *Dans le but de permettre la création d'un marché européen de l'information a porté le discours sur l'ouverture des données publiques. Celui-ci s'est concrétisé par l'adoption d'actions normatives destinées à favoriser la disponibilité et à faciliter l'exploitation commerciale de l'information issue du secteur public* ».
[1166] *JOUE* L 175/1 du 27 juin 2013.
[1167] Pour une analyse détaillée, voir TERESI, L., « Observations sur la directive n°2013/37/UE du 26 juin 2013 sur la réutilisation de l'information du secteur public », *JCP A*, n°7, 2039, n°21, 2014.
[1168] *JORF* n°0301 du 29 déc. 2015.
[1169] *JORF* n°0235 du 8 oct. 2016.
[1170] *JOUE* L 172/56 du 26 juin 2019.
[1171] ROBIN, A., « 3 questions — Gouvernance des données : l'ambition européenne de l'espace unique numérique », *JCP E*, n°8-09, 24 févr. 2022, 180.
[1172] Voir *supra*, n°146 et s.

socio-économiques »[1173]. Néanmoins, cette directive n'a pas bouleversé le droit de la réutilisation en France puisqu'elle « *reprend un certain nombre de dispositions déjà introduites dans le droit français* »[1174]. Son article 3 prévoit toutefois que le droit à la réutilisation, commerciale ou non, des informations figurant dans les documents, relève de son champ d'application. Ainsi, « *le régime du droit à la réutilisation permet de détacher complètement l'information par rapport à l'Administration qui l'a produite (ce qui favorise de nouvelles interprétations et de nouvelles formes d'exploitation)* »[1175].

B. Le fondement économique du droit de réutilisation

416- Le principe de la transparence n'est plus le seul objectif de l'action publique, y a été ajouté le développement économique (**1**). C'est pourquoi le droit de réutilisation des données publiques est fondé sur la liberté du commerce et de l'industrie (**2**).

1. Le développement économique

417- L'accès aux documents administratifs ne repose pas sur le même fondement que celui de la réutilisation des informations publiques. Si la commercialisation des informations publiques relève d'une logique économique, l'accès aux documents administratifs est né d'une logique de transparence qui sous-tend le chapitre 1er de la Loi n°78-753 du 17 juillet 1978[1176]. Aussi, comme l'énonçait le Premier ministre le 29 mai 2006 : « *À la préoccupation de la transparence administrative qui a inspiré la loi du 17 juillet 1978, vient ainsi s'ajouter un objectif de développement de l'activité économique par une meilleure valorisation des gisements de données dont dispose l'Administration* »[1177].

2. Le fondement de la liberté du commerce et de l'industrie

418- Le fondement du droit de réutilisation repose sur la liberté du commerce et de l'industrie et de ses deux composantes : la liberté d'entreprendre et la liberté de la concurrence. La liberté d'entreprendre est définie comme la « *liberté d'accéder à une profession ou à une activité*

[1173] ROBIN, A., *op. cit.*.
[1174] LALLET, A. et NGUYEN DUY, P., « Communication des documents administratifs », *op. cit.*, n°198.
[1175] TERESI, L., « L'*Open Data* et le droit de l'Union européenne (1) », *op. cit*.
[1176] LALLET, A. et NGUYEN DUY, P., *op. cit.*, n°201.
[1177] Premier ministre, circ. n°5156/SG, 29 mai 2006, nº PM-542.

économique, mais également la liberté d'exercer cette profession ou cette activité »[1178]. Sa seconde composante est la liberté de la concurrence qui est une déclinaison du principe d'égalité[1179]. La reconnaissance du principe de la libre réutilisation des données publiques par le législateur induit une prise en compte « *de l'enjeu économique que représentent les informations publiques en raison de leur potentiel commercial* »[1180]. Le droit de réutilisation des données publiques suppose que les administrations n'ont plus le contrôle de la destination des données qu'elles produisent ou reçoivent. L'usage est, désormais, ouvert à tous. Désormais, « *un régime de principe* » a été posé qui prévoit « *un droit universel gratuit à la libre réutilisation* »[1181]. Chacun peut donc réutiliser les données à d'autres fins que celles de la mission de service public pour laquelle elles ont été produites ou reçues de manière égale entre tous les concurrents. Les objectifs du droit de réutilisation sont donc de « *faire naître des initiatives innovantes, créatrices de richesses économiques* »[1182] du secteur privé en permettant la circulation et la réutilisation des données publiques[1183].

II. Le périmètre de la liberté de réutilisation

419- Le périmètre de la liberté de réutilisation, qui est différent de celui de l'accès, doit conduire à l'étude des notions d'informations publiques (**A**) et de réutilisation (**B**).

A. Les informations publiques

420- Tout d'abord, il est nécessaire d'envisager le lien entre informations publiques et documents administratifs (**1**), pour ensuite analyser les limites de la notion d'informations publiques (**2**).

[1178] Cons. const., 30 nov. 2012, déc. n°2012-285, QPC.
[1179] CE, 2 mars 2011, déc. n°345288, *Sté Manings*.
[1180] MARTINEZ, R. et MARX, B., « La longue marche de l'information publique, de la liberté d'accès aux documents administratifs à la réutilisation commerciale des informations publiques », *Documentaliste-Sciences de l'Information*, 2007/3, (Vol.44), pp. 218 à 217.
[1181] BLAIZOT-HAZARD, C., « Données publiques et patrimoine immatériel des personnes publiques », *PI*, avr. 2020.
[1182] *Ibid.*
[1183] TERESI, L., « L'Open Data et le droit de l'Union européenne (1) », *op. cit.* : « *La politique de l'Union européenne a poursuivi une finalité relativement ambitieuse : susciter (ou structurer) l'essor de marchés européens de l'information en facilitant l'appréhension des contenus issus du secteur public* ».

1. Le lien entre informations publiques et documents administratifs

421- **Définition.** La notion d'« information publique » est définie à l'article L. 321-1 du CRPA comme toutes informations publiques « *figurant dans des documents communiqués ou publiés par les administrations mentionnées au 1er alinéa de l'article L. 300-2 […]* ». Cette notion renvoie donc à celle de « documents administratifs »[1184] et a été préférée à celle de « données publiques » à compter de la directive PSI I de 2003[1185]. L'information publique figure donc dans un document administratif. La notion étant extensive, il peut s'agir du contenu d'une base de données[1186], de photographies ou bien encore de documents audiovisuels, etc. L'article L. 312-1-1 du CRPA prévoit d'ailleurs que sont des documents administratifs les données, mises à jour de façon régulière dont la publication présente un intérêt économique, social, sanitaire ou environnemental. La directive PSI III de 2019 retient, quant à elle, une définition large et cohérente en son article 2 de la notion de document, il s'agit de « *tout contenu, quel que soit son support (papier ou format électronique, enregistrement sonore, visuel ou audiovisuel)* » ou « *toute partie de ce contenu* ».

422- **Origine des informations publiques.** Alors que dans le régime de l'accès aux documents administratifs, on distingue les données publiques des documents, faisant naître un régime d'ouverture des données publiques, le droit de réutilisation se cantonne aux informations contenues dans les documents administratifs produits par l'Administration. Aussi, le fait d'avoir retenu la notion d'informations publiques contenues dans un document administratif distingue les régimes d'accès et de réutilisation, puisque les informations publiques ne peuvent pas être produites par une personne privée contrairement aux données publiques. Les informations publiques sont nécessairement contenues dans des documents administratifs et elles sont accessibles à toute personne soit par le biais d'un droit à communication des documents garantis par la loi soit par une diffusion publique légale.

423- **Extension de la notion.** À la lecture de l'article L. 321-3 du CRPA, la notion d'information publique semble s'étendre à celle des données publiques. En effet, cet article prévoit expressément que les données de référence sont mises à disposition en vue de faciliter leur réutilisation. Cette mise à disposition constitue une mission de service public. Dans ce cas, il

---

[1184] Voir *supra*, n°28 et s.

[1185] TERESI, L., *La commercialisation des données publiques*, Thèse, dir. CHEROT, J.-Y., Aix-Marseille, 2007, n°92, p. 113.

[1186] CRPA, art. L. 312-1-1, 3e : « *Sont susceptibles de réutilisation : les bases de données, mises à jour de façon régulière, qu'elles produisent ou qu'elles reçoivent et qui ne font pas l'objet d'une diffusion publique par ailleurs en vertu de l'article L. 321-3 du CRPA* ».

apparaît que la notion d'informations publiques contenues dans un document n'a plus beaucoup de sens, puisque les données de référence peuvent elles aussi être réutilisées, à moins qu'il soit sous-entendu que ces données sont toujours contenues dans une base de données qui constituerait le document administratif. Toutefois, l'article L. 312-1-1 du CRPA suppose le contraire puisqu'il est fait nettement la différence entre les bases de données (3e alinéa) et les données (4e alinéa).

Quoiqu'il en soit, les données de référence de l'article L. 321-3 du CRPA et les données mises à jour de façon régulière dont la publication présente un intérêt économique, social, sanitaire ou environnemental (qualité de l'air, données géographiques, données financières, etc.) de l'article L. 312-1-1 du CRPA doivent être publiées dans un format ouvert afin de faciliter leur réutilisation.

Aussi, dans le secteur agricole, les données contenues dans des bases de données produites par l'Administration telles que la base de données Agreste, la table Ciqual ou encore Inspire sont librement réutilisables[1187]. De même, en ce qui concerne les données de référence[1188] (données cadastrales, parcellaires et géographiques pour ce qui intéresse le secteur agricole).

2. Les limites de la notion d'informations publiques

424 L'article L. 321-2 du CRPA exclut du champ d'application du droit de réutilisation les informations contenues dans des documents « *dont la communication ne constitue pas un droit pour toute personne en application du titre 1er ou d'autres dispositions législatives, sauf si ces informations font l'objet d'une diffusion publique [...]* », mais aussi, ceux « *sur lesquels des tiers détiennent des droits de propriété intellectuelle* »[1189]. Il est à noter que la loi pour une République numérique (LRN) a supprimé l'exclusion des informations produites ou reçues dans le cadre d'une activité de service public à caractère industriel et commercial[1190] du régime de réutilisation des informations publiques. En effet, l'article L. 321-1 du CRPA dans son ancienne version excluait les informations contenues dans des documents produits ou reçus par les administrations dans l'exercice d'une mission de service public à caractère industriel ou commercial. Mais l'article 9 de la LRN a abrogé l'article L. 321-1, 1°, b). Ainsi, dorénavant, ces informations ne sont plus exclues du champ d'application du droit de réutilisation. Par conséquent, la nature de la mission de service public n'influe plus sur le droit de réutilisation

[1187] Voir *supra*, n°56 et s.
[1188] Voir *supra*, n°49.
[1189] Pour le développement des limites au droit de réutilisation, voir *infra*, n°428 et s.
[1190] CRPA, art. L. 321-2 (ancien article).

des informations produites ou reçues au cours de cette mission. Néanmoins, les bases de données produites ou reçues par une administration dans l'exercice d'une mission de service public à caractère industriel et commercial sont exclues du droit de réutilisation au titre de l'article L. 323-1, al. 2 du CRPA. Ainsi, les intérêts de ces établissements soumis à la concurrence sont préservés, ils peuvent alors valoriser leurs bases de données[1191].

425- Les données de la recherche peuvent également être réutilisées dans le cadre de la LRN à travers un double dispositif. D'abord, celui des écrits scientifiques issus d'une activité de recherche financée au moins pour moitié sur fonds publics qui ont été rendus publics gratuitement par leur auteur dans les conditions prévues à l'article L. 533-4 du Code de la recherche. Ensuite, celui des données issues d'une activité de recherche financée au moins pour moitié sur fonds publics qui ne sont pas protégées par un droit spécifique ou une réglementation particulière telle que des droits de propriété intellectuelle, la protection des données à caractère personnel ou le respect de la vie privée et qui ont été rendues publiques par le chercheur, l'établissement ou l'organisme de recherche. Dans les deux cas, la réutilisation est libre, mis à part que le document ne peut faire l'objet d'une exploitation dans le cadre d'une activité d'édition à caractère commercial. Enfin, la Directive du 20 juin 2019 concernant les données ouvertes et la réutilisation des informations du secteur public a un champ d'application légèrement différent que ceux des textes précédents. En effet, il ne reprend pas les notions d'informations publiques ou de données publiques, mais retient celle de « *document* ». Toutefois, dans les grandes lignes, les champs d'application de ces deux notions se recoupent[1192].

B. La réutilisation

426- Il convient d'analyser le principe de la réutilisation (**1**) qui comporte néanmoins des limites quant à la protection des données et des personnes (**2**).

1. Le principe de la réutilisation

427- L'article L. 321-1 du CRPA dispose que les informations publiques peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les

[1191] ROBIN, A., *Droit des données de la recherche, op. cit.*, n°716, p. 534.
[1192] Pour aller plus loin, LALLET, A. et NGUYEN DUY, P., « Communication des documents administratifs », *op. cit.*, n°212.

besoins de laquelle les documents ont été produits ou reçus[1193], que ce soit à caractère commercial ou non[1194]. L'objectif étant « *la création de produit nouveau sur les marchés de l'information* »[1195] de la directive. C'est donc l'aspect commercial qui prime dans le régime de la réutilisation. Néanmoins, elles peuvent être réutilisées à des fins économiques, mais aussi de recherches scientifiques. La seule condition est que la réutilisation soit distincte de « *l'objectif initial de la mission de service public* ». Par conséquent, le régime de la réutilisation ne s'applique qu'au « *bénéficiaire de la communication [qui] entend faire un usage de l'information tout à fait détachable ou étranger à la mission de service public pour la satisfaction de laquelle les informations ont été collectées* »[1196]. Enfin, l'article L. 321-1 du CRPA prévoit que « *l'échange d'informations publiques entre les administrations aux fins de l'exercice de leur mission de service public ne constitue pas une réutilisation* ». Toutefois, les administrations peuvent utiliser les informations publiques produites ou reçues par une autre pour l'accomplissement de ses propres missions de service public[1197].

2. La limite de la réutilisation : la protection des données et des personnes

428- Le principe de libre réutilisation est un droit dans l'Union européenne qui doit néanmoins respecter l'intégrité des informations publiques et protéger les intérêts des personnes à qui elles se rapportent. Y font exceptions les documents dont la communication ne constitue pas un droit pour toute personne, sauf si ces informations font l'objet d'une diffusion publique, et les documents sur lesquels des tiers détiennent des droits de propriété intellectuelle[1198]. Dans le secteur de la recherche scientifique, cette deuxième exception entrave la mise en œuvre de la libre réutilisation des données scientifiques[1199]. En effet, les contrats de partenariat prévoient le plus souvent des clauses de copropriété avec des entreprises du secteur privé. Par conséquent, « *le contrat de partenariat protégera l'établissement contre l'obligation de diffusion des résultats dont la valorisation sera d'ailleurs le plus souvent assurée par l'entreprise* »[1200].

[1193] CRPA, art. L. 321-1 : « *Les informations publiques figurant dans des documents communiqués ou publiés par les administrations mentionnées au premier alinéa de l'article L. 300-2 peuvent être utilisées par toute personne qui le souhaite à d'autres fins que celles de la mission de service public pour les besoins de laquelle les documents ont été produits ou reçus* ».
[1194] CRPA, art. R. 323-3.
[1195] TERESI, L., *La commercialisation des données publiques, op. cit*., n°145 et s, p. 159.
[1196] *Ibid.*, n°149, p. 163.
[1197] LRN, art. 1er, I.
[1198] CRPA, art. L. 321-2.
[1199] ROBIN, A., « Les données scientifiques au prisme du dispositif *Open Data* », *CCE*, n°9, 2017, n°29.
[1200] ROBIN, A., « Valorisation de la recherche scientifique, propriété intellectuelle, innovation » chr., *CDST*, 7/2017.

429- De plus, la réutilisation des informations publiques est soumise à plusieurs conditions : les données ne doivent pas être altérées, leur sens ne doit pas être dénaturé et leurs sources et la date de leur dernière mise à jour doivent être mentionnées[1201]. Ainsi, l'article L. 322-1 du CRPA interdit l'altération des données et la dénaturation de leur sens. Il peut s'agir d'opérations qui affectent « *l'exactitude, l'exhaustivité et la fiabilité* »[1202] des données, telles que « *la conception d'une base de données prétendument alimentée par des données de l'Administration que le réutilisateur aurait préalablement modifiées* »[1203]. Ensuite, ce même article prévoit que doivent être mentionnées les sources et la date de leur dernière mise à jour aussi bien par le réutilisateur que par l'Administration. Cependant, ces règles peuvent être évincées par cette dernière, en effet, l'article L. 322-1 du CRPA précise que les obligations qu'il pose s'appliquent « *sauf accord de l'Administration* ». Il est peu probable néanmoins que l'Administration accorde la réutilisation de données altérées ou dénaturées. En pratique, il est plus envisageable que cet accord vise plutôt la dispense de mention des sources et de la date de la dernière mise à jour[1204]. Enfin, tant l'Administration que le réutilisateur doivent respecter la réglementation des données à caractère personnel[1205].

§2. *Les conditions de réutilisation des données publiques*

430- L'étude des conditions de réutilisation des données publiques doit conduire à rechercher les contours de la réutilisation de ces données à travers les licences d'utilisation (**I**), ainsi que par le contrôle de leur réutilisation (**II**).

I. Les contours de la réutilisation des données publiques dans les licences d'utilisation

431- Il convient d'envisager d'abord l'existence conditionnée de la licence (**A**) pour ensuite s'intéresser aux différentes licences d'utilisation (**B**).

[1201] CRPA, art. L. 322-1.
[1202] LALLET, A. et NGUYEN DUY, P., « Communication des documents administratifs », *op. cit.*, n°255.
[1203] *Ibid.*
[1204] LALLET, A. et NGUYEN DUY, P., « Diffusion et réutilisation des informations publiques : « *Open Data* » - données ouvertes », *Rép. IP/IT et comm.*, Dalloz, sept. 2020.
[1205] CRPA, art. L. 322-2.

A. L'existence conditionnée de la licence

432- L'existence de la licence d'utilisation suppose de répondre à certaines conditions (**1**), la plus importante de toutes étant le principe de gratuité de la réutilisation des données publiques (**2**).

1. Les conditions d'utilisation de la licence

433- La réutilisation des données publiques peut donner lieu à l'établissement d'une licence par les administrations afin de régir les conditions d'utilisation des données publiques[1206]. Ces licences d'utilisation peuvent être analysées en des autorisations administratives qui prennent une forme unilatérale ou contractuelle[1207]. La licence est facultative dans le cas d'une réutilisation gratuite et elle est obligatoire lorsque la réutilisation est soumise à redevance[1208]. Lorsque l'Administration fait le choix de mettre à disposition les données gratuitement sans licence d'utilisation, ce sont les règles générales de l'article L. 322-1 du CRPA qui s'appliquent. La loi leur permet toutefois de prévoir des conditions d'utilisation spécifiques de certaines données publiques même à titre gratuit en « *raison des données en cause ou de la nature de leur réutilisation* »[1209]. Enfin, il est nécessaire de préciser que dès lors que l'Administration fait le choix de subordonner la réutilisation gratuite des données publiques à la souscription d'une licence ou lorsqu'une redevance est exigée, elle doit mettre à la disposition des personnes intéressées des licences types par voie électronique[1210]. Dans une grande majorité des cas, les données publiques mises à disposition par les services déconcentrés du ministère de l'Agriculture ne sont pas soumises à des licences d'utilisation. C'est le cas des données publiées par la DRAAF[1211] ou encore Agreste. Dans ces cas, la réutilisation des données est libre pour toute personne dans la limite des conditions de l'article L. 322-1 du CRPA.

2. Le principe de la gratuité de la réutilisation des données publiques

434- **Principe : la gratuité.** Les administrations ont dorénavant l'obligation de diffuser les données publiques sans contrepartie financière. Ce parti pris résulte de la volonté de tirer les bénéfices

---

[1206] CRPA, art. L. 323-1.
[1207] TERESI, L., *La commercialisation des données publiques, op. cit.*, n°193, p. 312.
[1208] CRPA, art. L. 323-1.
[1209] TERESI, L., *op. cit*.
[1210] CRPA, art. L. 323-2.
[1211] Direction Régionale de l'Alimentation, de l'Agriculture et de la Forêt.

d'une large ouverture des données publiques pour l'économie, même si « *ce principe s'impose avec difficulté* »[1212]. La loi Valter a affirmé le principe de gratuité tout en permettant « *[d']établir une redevance de réutilisation lorsqu'elles sont tenues de couvrir par des recettes propres une part substantielle des coûts liés à l'accomplissement de leurs missions de service public* »[1213]. Il faut noter que les principes de gratuité et de libre réutilisation vont à l'encontre de l'objectif de monétisation du patrimoine immatériel pour financer le budget de la puissance publique et les progrès de la recherche[1214] : « *comme les Datas sont considérées par les économistes comme des gisements de valeur de demain, promouvoir la réutilisation gratuite du gisement considérable des données du secteur public revient de facto à abandonner pour une grande partie l'illusion selon laquelle l'immatériel public serait une source pérenne de revenus* »[1215]. Également, la directive PSI III de 2019 sur la réutilisation des informations publiques « *limite fortement les possibilités pour les entités appartenant au secteur public de se livrer à l'exploitation économique des données qu'elles produisent* »[1216].

435- **Exception : le paiement d'une redevance.** La directive PSI III dont le délai de transposition courait jusqu'au 17 juillet 2021 réaffirme une nouvelle fois le principe de gratuité ou lorsque cela est expressément prévu, la tarification au coût marginal[1217]. Ainsi, « *la directive limite fortement les possibilités pour les entités appartenant au secteur public de se livrer à l'exploitation économique des données qu'elles produisent* »[1218]. Par conséquent, l'objectif poursuivi de valorisation des données tend à être atteint grâce à la mise à disposition gratuite des données qui favorise leur libre réutilisation. Quelques exceptions sont prévues néanmoins par la loi[1219] pour des administrations lorsqu'elles « *sont tenues de couvrir par des recettes propres une part substantielle des coûts liés à l'accomplissement de leurs missions de service*

[1212] *Ibid*. : « *Dans un contexte budgétaire contraint, où les administrations cherchent davantage à valoriser leur patrimoine plutôt que de le mettre gratuitement à la disposition d'acteurs privés — parfois des multinationales en position dominante…* ».

[1213] Loi Valter, préc., art. 5 et CRPA, art. L. 324-1.

[1214] WARUSFEL, B., « Numérisation de l'action publique et *Open Data* : une révolution face à ses limites », Colloque – Circulation des données et propriétés intellectuelles, *PI*, avr. 2020, n°75, pp. 15 et s.

[1215] *Ibid.*

[1216] MULLER, E., « La libre circulation des données et la directive concernant la réutilisation des données du secteur public », *Dalloz IP/IT*, 2020, p. 424.

[1217] Dir. n°2019/1024, *op. cit.*, art. 6.1

[1218] MULLER, E., « La libre circulation et la directive concernant la réutilisation des données du secteur public », *op. cit.*, p. 424 ; Dir. n°2019/1024, préc., art. 8 - 11. 2

[1219] CRPA, art. L. 324-2 : « *La réutilisation peut également donner lieu au versement d'une redevance lorsqu'elle porte sur des informations issues des opérations de numérisation des fonds et des collections des bibliothèques, y compris des bibliothèques universitaires, des musées et des archives, et, le cas échéant, sur des informations qui y sont associées lorsque ces dernières sont commercialisées conjointement. Le produit total du montant de cette redevance, évalué sur une période comptable appropriée, ne dépasse pas le montant total des coûts de collecte, de production, de mise à disposition ou de diffusion, de conservation de leurs informations et d'acquisition des droits de propriété intellectuelle* ».

public »[1220]. Cependant, certaines administrations génèrent encore des revenus substantiels pour la réutilisation d'informations ou catégories d'informations fixées par décret[1221]. Ces informations sont soumises au paiement d'une redevance pour leur réutilisation[1222]. C'était le cas encore récemment de l'Institut national de l'information géographique et forestière (IGN) et de Météo-France. Plusieurs difficultés ont été néanmoins soulevées par le rapport au gouvernement sur les données géographiques souveraines qui a rappelé le principe de gratuité de ces données et a souligné la nécessité de les financer par la subvention pour charges de service public[1223]. En effet, la politique de tarification de la réutilisation des données conduite par l'IGN a limité la coopération avec d'autres producteurs de données, tels que les collectivités territoriales. Également, la Cour des comptes soutient dans son référé du 11 décembre 2018 que ces opérateurs, l'IGN et Météo-France notamment, ont connu une réduction des ventes de données au secteur privé en raison de plusieurs facteurs : premièrement, des plateformes sont venues les concurrencer ; deuxièmement, sont apparues sur le marché des données gratuites ou libres ; troisièmement, les opérateurs ont des difficultés à répondre aux attentes en données de qualité ; quatrièmement, les grandes entreprises sont à la fin du cycle d'acquisition des données. Aussi, le rapport Bothorel[1224] a soulevé en décembre 2020 que si l'ouverture des données remet en cause des rentes économiques et conduit à une perte de recette, elle ne fait pas, néanmoins, forcément obstacle à l'ouverture. En effet, la loi Valter de 2015 a précisément limité les redevances au cas où les administrations seraient tenues de couvrir par des recettes propres une part substantielle des coûts liés à l'accomplissement de leur mission de service public. Or, tant l'IGN que Météo-France allaient au-delà de cette part substantielle. Ainsi, le rapport Bothorel[1225] a préconisé de mener une réflexion sur l'ouverture de certaines données à compter de 2021 en concertation avec les acteurs pour une ouverture des données en 2022. De plus, sur le fondement de l'article L. 324-1 du CRPA, la circulaire du Premier ministre n°6224/SG du

---

[1220] ROBIN, A., *Droit des données de la recherche. Science ouverte, innovation, données publiques*, Larcier, 2022, n°719, p. 535.

[1221] CRPA, art. D. 324-5-1 issu du décret n°2016-1617, 29 nov. 2016, relatif aux catégories d'informations publiques de l'État et de ses établissements publics administratifs susceptibles d'être soumises au paiement d'une redevance de réutilisation : *JORF* n°0278 du 30 nov. 2016 : Les bases de données de l'Institut National de l'information Géographie et forestière, les données de Météo-France, les informations du Service hydrographique et océanographique de la marine et enfin, les informations issues des opérations de numérisation des fonds et des collections des bibliothèques.

[1222] Ord. n°2016-307, 17 mars 2016, portant codification des dispositions relatives à la réutilisation des informations publiques dans le code des relations entre le public et l'Administration : *JORF* n°0066 du 18 mars 2016, codif. CRPA, art. L. 324-5.

[1223] FAURE-MUNTIAN, V., *Rapport au Gouvernement, Les données géographiques souveraines*, juill. 2018, rec. n°24 et 25.

[1224] Mission confiée par le Premier ministre à Éric Bothorel, *Pour une politique publique de la donnée*, préc., p. 37.

[1225] *Ibid.*

27 avril 2021 prévoit notamment l'extinction, d'ici 2023, des redevances de réutilisation. Malgré des inquiétudes quant au financement de la production des données de référence avec un régime de gratuité et l'absence d'aides publiques[1226], l'IGN a anticipé cette future obligation d'ouverture et a revu sa politique de privatisation des données dans le sens de la gratuité. L'institut a, alors, fait évoluer sa mission de production-diffusion de données publiques en modifiant son organisation, son modèle économique et ses méthodes de travail, afin d'apporter un appui direct aux politiques publiques[1227]. Pour cela, il a rendu libres et gratuits l'accès et la réutilisation des données publiques concernant la topographie, les infrastructures et le relief français sous licence Etalab 2.0 depuis le 1er janvier 2021. Aussi, conformément au droit de réutilisation, désormais seules les données incluant des droits des tiers ou protégées par le droit de propriété intellectuelle sont exclues du droit de réutilisation. De plus, les données géographiques sont soumises à la directive INSPIRE[1228] qui vise à établir une infrastructure d'informations géographiques pour favoriser des politiques environnementales communautaires et des politiques ou des activités de la Communauté susceptibles d'avoir une incidence sur l'environnement. C'est pourquoi l'IGN met à disposition désormais le site Géoportail[1229]. De même, Météo-France pratiquait des prix élevés pour accéder aux données qu'ils produisaient ce qui conduisait les acteurs de l'agriculture numérique à investir eux-mêmes dans la collecte de données météorologiques afin de répondre à leurs propres besoins. Aussi, en introduisant la notion de « jeux de données à forte valeur » qui s'applique notamment au domaine météorologique et géographique, le droit de l'Union va dans un délai de deux ans imposer, à Météo-France et à IGN, d'assurer la mise en ligne de nouveaux jeux de données accessibles au moyen des API (interface de programmation d'application)[1230]. Le savoir-faire de Météo-France pourra donc être valorisé et cela permettra d'accroître ses bénéfices et il est possible à partir de l'ouverture des données météorologiques de développer de nouvelles activités et de créer de nouveaux produits à forte valeur ajoutée. Néanmoins, « *la valorisation des données publiques de l'établissement suppose des démarches d'accompagnement des utilisateurs dans l'appropriation des données météorologiques. Cet enjeu va aller croissant*

[1226] PISAN, M., « IGN : la gratuité des données en question », *Expertises*, mai 2019.
[1227] IGN, communiqué de presse, 11 déc. 2020.
[1228] Dir. n°2007/2/CE établissant une infrastructure d'information géographique dans la Communauté européenne (Inspire) : *JOUE* L 108/1 du 25 avr. 2007.
[1229] Voir *supra*, n°58.
[1230] Rapport Bothorel, préc., p. 64.

avec la dilatation du volume de données mises en ligne et reste très largement à explorer et à traiter »[1231].

B. Les licences d'utilisation

436- Parmi les licences d'utilisation, il existe des licences types (**1**) et des licences homologuées (**2**).

1. Les licences types

437- Un décret détermine les différentes licences que peuvent utiliser les administrations[1232]. Ainsi, il faut distinguer selon les licences de réutilisation à titre gratuit et les licences d'utilisation commerciales.

Tout d'abord, s'agissant des licences d'utilisation à titre gratuit, l'Administration doit choisir une des licences types figurant à l'article D. 323-2-1 du CRPA.

D'une part, l'Administration peut choisir la licence ouverte de réutilisation d'informations publiques, élaborée par Etalab qui accorde au réutilisateur une totale liberté de réutilisation. Ces licences sont, surtout, utilisées, par les services du ministère de l'Agriculture et ses services déconcentrés tels que l'IGN, mais aussi, pour certains jeux de données, par des instituts de recherche. La licence *Open Data* est une licence de référence pour les administrations organisant la publication des données publiques (Licence ouverte 2.0/LO 2,0)[1233]. Au-delà de la mise à disposition des données publiques, cette licence prévoit une libre réutilisation des données puisqu'elle autorise la reproduction, la redistribution, l'adaptation et l'exploitation commerciale des données. Elle prévoit également des obligations pour l'Administration qui est tenue d'assurer la transparence des données et de diffuser la qualité des sources en mentionnant leur paternité.

D'autre part, l'Administration peut opter pour la licence « Open Database License » (ODbL) qui est une licence avec obligation de réciprocité[1234]. Elle contraint le réutilisateur à accorder à toute personne intéressée une licence analogue pour réutiliser les informations issues de ses propres opérations de traitement. Donc, elle « *impose aux réutilisateurs de ne pas "ré-enfermer" les données libérées (enclosure), en les obligeant à utiliser la même licence pour*

[1231] CAPO-CANELLAS, V., *Météo-France*, Rapport d'information n°840 fait au nom de la commission des finances, 22 sept. 2021.
[1232] Décret n°2017-638, 27 avril 2017, relatif aux licences de réutilisation à titre gratuit des informations publiques et aux modalités de leur homologation : *JORF* n°0100 du 28 avr. 2017.
[1233] *Ibid.* ; CRPA, art. L. 323-2.
[1234] « *Share-alike* » ; CRPA, D. 323-2-1.

maintenir ouverte la base de données »[1235], sinon cela aurait pour conséquence de bloquer la réutilisation des données publiques[1236].

Ensuite, en ce qui concerne les licences de réutilisation à titre commercial, l'Administration peut utiliser la licence de son choix à condition, toutefois, de respecter les règles de réutilisation du CRPA.

2. Les licences homologuées

438- La CADA veille à l'utilisation des licences types par les administrations ou à la mise en conformité de celles qu'elles utilisaient antérieurement[1237]. Ainsi, les administrations peuvent faire homologuer leur licence[1238]. Plusieurs licences ont déjà été homologuées par les services de l'État[1239].

Tout d'abord, la Licence Libre permet de diffuser l'œuvre « *en empêchant a priori ceux qui se situent dans la chaîne contractuelle de reconstituer sur elle des droits de type propriétaires classique* »[1240]. Il s'agit d'une licence libre définie comme celle « *par laquelle l'auteur autorise la copie, la modification et la diffusion de l'œuvre modifiée ou non, de façon concurrente, sans transférer les droits d'auteur qui y sont attachés et sans que l'utilisateur ne puisse réduire ces libertés tant à l'égard de l'œuvre originelle que de ses dérivés* »[1241].

Ensuite, les licences *Creatives commons* ont été créées en 2001 par Lawrence Lessig au sein du *Stanford Law school center for International Society*. Le *Creative Commons* est un « *ensemble de solutions alternatives légales pour les personnes souhaitant libérer leurs œuvres des droits de propriété intellectuelle standards de leur pays, jugés trop restrictifs. Il consiste en plusieurs licences, connues sous le nom de licences Creatives Commons* »[1242]. Celui qui souhaite utiliser une licence *Creative commons* utilise une combinaison de pictogrammes selon

---

[1235] CLUZEL-METAYER, L., « L'ouverture des données publiques », in AFDA, ss. dir., *Le droit administratif au défi du numérique*, Dalloz, 2019, p. 14.
[1236] BERTHAULT, D., « La licence ODbL bloque la réutilisation des données publiques » *JCP A*, n°2240, 16 oct. 2017.
[1237] CADA, avis n°20190245, 27 juin 2019.
[1238] CRPA, art. D. 323-2.
[1239] Licence d'utilisation à titre gratuit de l'Institut national géographique et forestier, licence du produit gratuit issu de la Base Adresse Nationale, licence « Creative Commons Attribution – Partage dans les mêmes conditions » du service hydrographique et océanographique de la marine et deux licences de réutilisation des informations de l'Institut National de la Propriété Industrielle.
[1240] VIVANT, M. et BRUGUIERE, J.-M., *Droit d'auteur et droits voisins*, Dalloz, 4e éd., 2019, n°877, p. 865.
[1241] CLEMENT-FONTAINE, M., *Les œuvres libres*, dir. VIVANT M., Montpellier, 2006 ; CLEMENT-FONTAINE, M., *L'œuvre libre*, préf. Vivant M., Larcier, 2014..
[1242] MOUVEMENT UTOPIA, *Propriété et communs, Idées reçues et propositions*, préf. CORIAT, B., éd. Utopia, 2017, p. 102.

ce qu'il souhaite permettre ou non aux utilisateurs : « BY » oblige l'utilisateur à mentionner l'auteur de l'œuvre ; « NC » ou *No commercial* interdit toute utilisation commerciale ; « ND » ou *No derivative works* interdit toute modification ; « SA » ou *Share alike,* pour le cas où ces modifications seraient acceptées, oblige celui qui y a procédé à diffuser l'œuvre modifiée dans les termes de la licence originale. De fait, ces licences CC organisent « *un certain usage des œuvres* »[1243].

II. Le contrôle de la réutilisation des données publiques

439- Le contrôle de la réutilisation des données publiques peut se faire à travers le contrat (**A**) ou judiciairement (**B**).

A. Le contrôle contractuel

440- Afin de contrôler contractuellement la réutilisation des données publiques, la licence doit comporter certaines informations obligatoires (**1**). Aussi, l'utilisation de la licence par les administrations est limitée (**2**).

1. Le contenu des licences

441- La licence doit comporter les informations faisant l'objet de la réutilisation, mais aussi les sources de ces données et leur date de mise à disposition, sauf accord de l'Administration[1244]. Doivent également figurer le caractère commercial ou non de leur réutilisation, les droits et obligations du licencié et le cas échéant le montant de la redevance et les modalités de paiement[1245]. Le licencié peut être autorisé à reproduire, copier, publier et transmettre les données publiques à des tiers, mais aussi à les traiter et à les exploiter. Dans ce cas, la licence devra prévoir l'amplitude de ces droits et leurs modalités. Elle peut aussi obliger le réutilisateur à diffuser les données dans les mêmes conditions. Le réutilisateur devra donc prévoir la même licence lors de la diffusion des données qu'il a lui-même traitées.

[1243] VIVANT M. et BRUGUIERE J.-M., *Droit d'auteur et droits voisins*, *op. cit.*, n°886, p. 875.
[1244] CRPA, art. L. 322-1.
[1245] CRPA, art. R. 323-3.

2. Les contraintes de la licence

442- Il existe deux contraintes pour les administrations lors de l'emploi des licences à titre commercial[1246]. D'une part, les conditions d'utilisation ne peuvent restreindre la réutilisation que pour des motifs d'intérêt général et de façon proportionnée. D'autre part, ces licences ne peuvent avoir pour objet ou pour effet de restreindre la concurrence.

Dans le premier cas, « *cela signifie simplement que si l'organisme public définit des conditions relatives à l'intégrité des informations, il doit les déterminer de manière à ce que la préservation des intérêts généraux, dont il a la charge, n'affecte pas outre mesure la réutilisation, de telle sorte qu'elle soit complètement empêchée par exemple* »[1247]. L'Administration doit donc procéder à un test de proportionnalité entre les restrictions dans un objectif d'intérêt général et le droit de réutilisation. La directive PSI III de 2019 prévoit en son article 8 que ces conditions doivent être « *objectives, proportionnées, non discriminatoires et justifiées sur la base d'un objectif d'intérêt général* ».

Dans le second cas, « *les conditions de réutilisation fixées dans les licences ne doivent pas contrarier le droit de la concurrence en empêchant certains opérateurs d'accéder aux ressources détenues par les organismes publics, ou en opérant des discriminations entre les entreprises qui se trouveraient dans une situation comparable* »[1248]. Si en principe la réutilisation des données publiques ne peut pas faire l'objet d'un accord d'exclusivité avec un tiers, la loi prévoit néanmoins une exception lorsque cet accord est nécessaire à l'exercice d'une mission de service public[1249]. Cette exclusivité peut être accordée pour une période n'excédant pas dix ans et son bien-fondé doit faire l'objet d'un réexamen périodique au moins tous les trois ans[1250].

B. Le contrôle judiciaire

443- Une autorité de contrôle permet de sanctionner les réutilisateurs qui ne respecteraient pas les conditions d'utilisation des données publiques. Aussi, certains actes sont incriminés (**1**) et des sanctions peuvent être prononcées (**2**).

[1246] CRPA, art. L. 323-2.
[1247] TERESI, L., *La commercialisation des données publiques, op. cit*., p. 317.
[1248] *Ibid.*
[1249] CRPA, art. L. 325-1.
[1250] CRPA, art. L. 325-2.

1. Les actes incriminés

444- L'article L. 326-1 du CRPA prévoit les incriminations pouvant donner lieu à sanction. D'abord, il est interdit de dénaturer les informations ou d'en altérer le sens et d'omettre de citer la source et la date de dernière mise à jour, sauf accord de l'Administration[1251]. Ensuite, est sanctionné par la CADA le fait de ne pas respecter les conditions de réutilisation prévues par une licence, sous réserve que ces conditions aient été légalement instituées. Enfin, est proscrit le fait de réutiliser des informations publiques sans licence alors que celle-ci était obligatoire. Il faut noter que les sanctions visent toujours le réutilisateur et jamais l'Administration.

2. Les sanctions

445- La CADA est compétente pour infliger des sanctions aux réutilisateurs qui ne respecteraient pas les conditions de réutilisation. L'article L. 326-1 du CRPA prévoit les sanctions qui peuvent être prononcées selon les incriminations. Lorsque les données sont mises à disposition à titre gratuit et qu'elles sont réutilisées en méconnaissance de l'article L. 322-1 du CRPA ou des conditions de réutilisation prévues par une licence délivrée à cet effet ou en violation de l'obligation d'obtenir une licence, le réutilisateur est passible d'une amende de 5e classe. Lorsque les données publiques ont été réutilisées à des fins commerciales en méconnaissance des dispositions de l'article L. 322-1 du CRPA ou des conditions de réutilisation prévues par une licence délivrée à cet effet ou en violation de l'obligation d'obtenir une licence, le montant de l'amende est proportionné à la gravité du manquement commis et aux avantages tirés de ce manquement.

446- **Conclusion de la section.** Le principe de la libre réutilisation des informations publiques n'aura pas vocation à s'appliquer aux données issues des exploitations agricoles. Seulement certaines données agricoles produites par les administrations devront faire l'objet d'un droit de réutilisation (base de données Agreste, table Ciqual ou encore Inspire ainsi que les données de référence). Aussi, ces données ne font l'objet d'aucune maîtrise de leur usage puisqu'elles sont librement réutilisables. En revanche, s'agissant des données privées issues de l'exploitation agricole, la maîtrise de l'usage suppose d'avoir le contrôle de l'accès à ces données.

[1251] CRPA, art. L. 322-1.

Section 2. La maîtrise de l'usage des données privées d'exploitation par le contrôle de l'accès

447. Les entreprises qui ferment l'accès aux données privées issues de l'exploitation en contrôlent l'usage (**§1**). C'est pourquoi, aujourd'hui, le législateur européen tend vers la régulation du partage des données privées afin de favoriser leur réutilisation (**§2**).

§1. *La fermeture de l'accès aux données d'exploitation privées pour le contrôle de l'usage*

448. L'absence de régime d'ouverture des données privées contribue à l'adoption de régime réservataire par les entreprises de l'*AgTech* afin de conserver un monopole sur les données qu'elles détiennent. Les scientifiques et l'Administration ne bénéficient pas non plus *a priori* de « passe-droit » leur permettant d'accéder directement aux données des personnes morales de droit privé. Sans accès, les tiers ne peuvent avoir l'usage des données. Aussi, il faut relever l'absence de régime général d'ouverture des données privées (**I**). Néanmoins, il est possible d'organiser un système d'accès ouvert à ces données (**II**).

I. L'absence de régime d'ouverture des données d'exploitation privées

449. La loi ne prévoit pas de régime d'accès aux données d'exploitation privées (**A**). Par conséquent, l'accès aux données privées pour les tiers est somme toute restreint (**B**).

A. Le silence de la loi sur l'accès aux données d'exploitation privées

450. La question de l'accès est plus problématique lorsqu'il s'agit des tiers au contrat que pour le co-contractant. Les tiers n'ont pas de prérogatives sur les données collectées par des personnes morales de droit privé. En effet, les plus grands acteurs peuvent adopter des comportements prédateurs sur le marché qui ont pour effet de limiter les externalités positives de l'exploitation des données agricoles. La réservation des données par certaines entreprises mène à des situations de monopole sur le marché voire à des abus de position dominante. Il est donc apparu primordial pour le législateur de réguler la circulation des données. Pour cela, le législateur européen a proposé l'adoption en 2018 du Règlement 2018/1807 sur la libre circulation des

données à caractère non personnel[1252]. Il est remarquable que, plutôt que d'adopter une réglementation impérative sur la circulation des données transplateformes, le législateur ait préféré se contenter de réguler la circulation transfrontière qui ne représente pourtant pas le plus gros enjeu dans un écosystème en nuage. Il a également fait le choix de laisser une place prépondérante à l'autorégulation par les acteurs des secteurs concernés. C'est pourquoi il convient d'envisager la régulation *a minima* de la circulation des données non personnelles. Pour cela, il est nécessaire d'étudier les apports du Règlement européen au sujet de l'ouverture de l'accès aux données privées (**1**). Ensuite, il faudra s'intéresser à la mise en œuvre limitée de la circulation des données privées (**2**).

1. L'apport limité du Règlement européen au sujet de la circulation des données privées

451- **Contexte**. Les données doivent circuler afin de garantir la transparence et la loyauté de la concurrence et de l'information. La montée en puissance des technologies[1253] dépendantes des données dans l'économie européenne a fait de la libre circulation des données non personnelles un enjeu majeur. Dans ce cadre, la Commission européenne a pris plusieurs initiatives pour une économie fondée sur les données, dans sa stratégie pour un « *marché unique du numérique* »[1254]. Le législateur européen a ainsi adopté un règlement portant sur la libre circulation des données à caractère non personnel le 19 décembre 2018, afin de compléter le règlement sur la libre circulation des données à caractère personnel de 2016[1255].

452- **Objectifs du règlement**. Tout d'abord, il est question d'ouvrir la possibilité de stocker et de traiter des données non personnelles n'importe où dans l'Union européenne. Ensuite, il s'agit de « *garantir aux autorités compétentes un accès aux données traitées dans un autre État membre à des fins de contrôles réglementaires, comme l'inspection et l'audit* »[1256]. Enfin, il s'agit d'encourager « *les acteurs du marché à créer des codes de conduite afin de faciliter pour les utilisateurs professionnels le changement de fournisseur de services en nuage et le transfert*

[1252] Règl. n°2018/1807 du 14 nov. 2018, établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne : *JOUE* L 303/59 du 28 nov. 2018.
[1253] *Ibid*., cons. 9 : « *L'essor de l'Internet des objets, l'intelligence artificielle et l'apprentissage automatique* ».
[1254] CASTETS-RENARD, C., NDIOR, V. et RASS-MASSON, L., « Le marché unique numérique : Quelles réalités matérielles et conceptuelles ? », *D.*, n°956, 2019.
[1255] Règl. n°2016/679 du 27 avr. 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 : *JOUE* L 119/1 du 4 mai 2016.
[1256]http://www.europarl.europa.eu/news/fr/press-room/20180926IPR14403/libre-circulation-des-donnees-a-caractere-non-personnel-la-5e-liberte-de-l-ue.

de données vers leur propre système informatique »[1257]. Les objectifs finaux affichés sont d'éviter l'accaparement des données par un seul acteur du marché et de favoriser le droit de la concurrence et l'innovation dans les secteurs concernés. Il s'agit aussi d'harmoniser les réglementations des États membres sur la libre circulation que les données soient personnelles ou non.

453- **Suppression des barrières européennes**. Pour favoriser la libre circulation des données industrielles générées par des machines et des données commerciales[1258], la Commission européenne a fait le choix de supprimer les barrières européennes qui pouvaient restreindre cette circulation. L'article 4 du règlement prévoit en effet que « *les exigences de localisation des données sont interdites, sauf si elles sont justifiées par des motifs de sécurité publique dans le respect du principe de proportionnalité* ». Par conséquent, il est désormais interdit pour un État membre d'imposer le stockage des données sur son sol. La seule exception retenue par le texte est le motif de sécurité publique. Toutes formes de barrières doivent donc être supprimées qu'elles soient géographiques ou bien qu'elles aient simplement pour effet la localisation des données[1259]. L'objectif étant de limiter à son strict nécessaire le *Data nationalisme*[1260]. C'est le cas, notamment, lorsque des « *règles ou pratiques administratives ont un effet équivalent en imposant des exigences spécifiques qui rendent plus difficile le traitement de données en dehors d'une zone géographique ou d'un territoire précis dans l'Union* »[1261]. De telles exigences peuvent « *représenter un coût important pour un opérateur et donc pénaliser spécialement les jeunes, petites ou moyennes entreprises* »[1262]. Cependant, il est à noter que cette interdiction ne concerne pas les exigences de localisation que l'on retrouverait dans un contrat[1263]. Seuls les textes législatifs, réglementaires et les pratiques administratives sont concernés.

[1257] *Ibid*.
[1258] Constituent de telles données « *les ensembles de données agrégées et anonymisées utilisées pour l'analyse des mégadonnées, les données sur l'agriculture de précision qui peuvent aider à contrôler et à optimiser l'utilisation des pesticides et de l'eau, ou encore les données sur les besoins d'entretien des machines industrielles* », Règl. n°2018/1807, préc., cons. 9.
[1259] MOUCHETTE, J., « Haro sur les obligations de localisation des données non personnelles », *Dalloz IP/IT*, 2020, p. 401.
[1260] CARRE, S., « Libre circulation des données, propriété et droit à l'information (1) : à propos du règlement (UE) 2018/1807 du 14 novembre 2018 », *Dalloz IP/IT*, 2020, p. 228.
[1261] Règl. n°2018/1807, préc., cons. 4.
[1262] CARRE, S., *op. cit*.
[1263] *Ibid*.

2. Le manque d'effectivité du règlement

454- **Conséquences du manque d'effectivité.** Si le règlement interdit effectivement les obligations de localisation des données dans un État membre, ses conditions d'application restent toutefois restreintes. Il faut s'interroger sur la pertinence de telles règles au regard de la pratique. La question se pose de savoir si l'obligation de localisation des *Data center* dans un État membre peut vraiment avoir pour objet ou pour effet de restreindre la circulation des données. Selon Mme S. Carre, le *« règlement met en lumière l'importance de cette catégorie juridique des données non personnelles et s'attache surtout à interdire les entraves aux exigences de localisation des données et non aux enjeux qui auraient véritablement permis leur circulation* »[1264]. En effet, le règlement n°2018/1807 ne contraint pas les acteurs du secteur de l'agriculture numérique à faire circuler les données et à s'ouvrir à la concurrence. Par conséquent, beaucoup d'entre eux adoptent des solutions prioritaires afin de conserver la confidentialité des données qu'ils détiennent. De cette manière, les acteurs qui ont les moyens techniques et financiers peuvent conserver des comportements prédateurs et accaparer de grands silos de données. Les nouveaux entrants se retrouvent donc confrontés à des barrières à l'entrée, ce qui diminue le choix de fournisseurs de services pour les utilisateurs.

455- **Champ d'application restreint**. Le CNNum[1265], le Sénat,[1266] mais aussi la doctrine,[1267] considèrent que les restrictions actuelles dans le domaine du numérique ne concernent en réalité qu'un nombre très restreint de données. En réalité, par nature, les données ont déjà vocation à circuler en nuage. Le fait qu'elles soient stockées dans un *Data center* ne représente pas une restriction à la circulation des données. Très peu de textes dans l'Union européenne ont vocation à imposer la localisation des données sur un territoire qui n'est pas justifiée par la sécurité publique. Par conséquent, il n'est pas pertinent d'interdire l'obligation de localisation. De plus, le règlement n°2018/1807 ne prend pas en compte toutes les hypothèses de restrictions de circulation.

456- **Hypothèses restreintes**. Le CNNum a eu l'occasion de soulever que d'autres obstacles que la localisation géographique des *Data centers* pouvaient avoir pour effet de limiter la circulation des données non personnelles dont le règlement ne prend pas en compte. C'est le cas, par

---

[1264] *Ibid.*
[1265] CNNum, *La levée des obligations de localisation des données*, fiche, juill. 2017, p. 1
[1266] Prop. de résolution n°80 (2017-2018) de SUTOUR, S. déposée au Sénat le 9 nov. 2017, p. 6.
[1267] ZOLYNSKI, C., « Quelle circulation des données non personnelles pour l'Union européenne ? », Rev. *Aff. Eur.*, 2018/1, pp. 73 à 78 ; MOUCHETTE, J., « Haro sur les obligations de localisation des données non personnelles », *op. cit.*

exemple, des « *silos de services en ligne* »[1268]. Dans un avis de juillet 2017, le CNNum retenait que « *la fragmentation géographique du marché de la donnée n'est que marginalement causée par les obligations légales de localisation* »[1269]. En réalité, ce sont plutôt les « *stratégies de lock in et de rétention de données entre acteurs économiques* » qui freinent la circulation.

457. **Absence de cadre juridique pour les entraves privées à la circulation**. Le règlement n'offre pas de véritable cadre juridique pour les entraves privées à la circulation des données. Ainsi, dès lors que la restriction de la circulation des données est due à « *une dépendance à l'égard des fournisseurs de services de traitement des données non personnelles* »,[1270] le règlement propose seulement d'instaurer un portage des données. Il faut alors, constater la « *portée relativement limitée du règlement sur le libre flux des données non personnelles* »[1271], qui « *n'a pas permis de donner toute sa mesure à cette idée pourtant porteuse d'une dynamique intéressante* »[1272].

B. Les restrictions d'accès aux données d'exploitation privées pour les tiers : l'exemple de la recherche scientifique

458. Dans la mesure où la norme est la réservation des données, les tiers n'ont pas accès directement aux données privées détenues par les entreprises. Par exemple, aucune obligation de mise à disposition des données d'exploitation n'existe à l'égard des institutions de recherche scientifique ou des chercheurs (**1**). Par conséquent les scientifiques doivent employer leurs propres méthodes de collecte afin de se procurer les données d'exploitation agricole (**2**).

1. L'absence de mise à disposition des données pour la recherche scientifique

459. **Relativité de l'accès aux données pour la recherche scientifique.** Les données des exploitations agricoles sont essentielles pour la recherche scientifique afin d'apporter une amélioration des conditions de travail des agriculteurs, pour développer des méthodes agronomiques plus écologiques ou encore pour soigner des maladies végétales. Néanmoins, il n'existe pas d'arsenal juridique facilitant l'accès des chercheurs aux données agricoles dont ils

[1268] MOUCHETTE, J., *ibid*.
[1269] CNNum, *La levée des obligations de localisation des données*, fiche, juill. 2017, p. 4.
[1270] CARRE, S., « Libre circulation des données, propriété et droit à l'information (1) : à propos du règlement (UE) 2018/1807 du 14 novembre 2018 », *op. cit.*
[1271] *Ibid.*
[1272] *Ibid.*

ont besoin pour mener à bien leurs projets de recherche, hormis celles incluses dans les bases de données au moyen de l'exception de fouille de textes et de données[1273]. Aucune obligation légale ou réglementaire n'oblige donc les agriculteurs ou les entreprises à communiquer à des fins de recherche scientifique les données qu'ils produisent ou collectent. Un exemple éloquent est le choix du législateur dans le RGPD de ne pas retenir la recherche scientifique, à l'article 6, comme une finalité justifiant un contournement de l'obligation d'obtenir le consentement de la personne concernée lors du traitement de ses données personnelles. Dès lors que les chercheurs souhaitent exploiter des données personnelles à des fins de recherche scientifique, ils doivent faire reposer le traitement sur l'une des cinq finalités prévues par la loi[1274] parmi lesquelles la finalité de recherche scientifique n'est donc pas prévue. Le plus souvent, les chercheurs s'appuieront sur l'intérêt légitime. Néanmoins, il existe une présomption de compatibilité avec la finalité initiale pour les traitements ultérieurs à des fins de recherche[1275]. Ainsi, chaque projet de recherche reposant sur un réseau d'observation nécessite une implication volontaire des agriculteurs au projet. C'est le cas notamment du programme de recherche et développement « Miellées » piloté par l'Itsap — Institut de l'Abeille — associé à plusieurs constructeurs de balances connectées dont l'objectif est de « *valoriser et d'analyser les données issues des balances connectées et mieux comprendre les dynamiques des colonies dans différents contextes* »[1276]. À cette fin, les chercheurs souhaitent étudier les utilisations possibles par les apiculteurs des différents capteurs afin de créer un outil d'aide à la décision à la fois sur leur exploitation et sur la gestion des cheptels. La valorisation des données (organisation, tri) dans une base de données permet de fournir de précieuses informations aux chercheurs afin de mieux comprendre et prédire les miellées. Pour cela, les apiculteurs participent volontairement à ce projet en acceptant de partager leurs données.

460- **Freins à la circulation des données.** Cet obstacle au partage des données des exploitations agricoles peut être justifié de différentes manières. De façon générale, avec la mutualisation de leurs données, les agriculteurs craignent la transparence de leur activité. Par exemple, le fait que les coopératives aient connaissance des données de rendement des agriculteurs pourrait entraîner une baisse des prix des récoltes. Il est ressorti du projet « Miellées » que les craintes des apiculteurs étaient de dévoiler l'emplacement exact de leur ruché et ainsi de favoriser un phénomène — déjà existant — de vol des ruches par leurs concurrents ou par des citoyens. Par

[1273] Voir *supra*, n°264 et s.
[1274] Voir *infra*, n°717 et s.
[1275] Art. 5, b) RGPD.
[1276] https://itsap.asso.fr/pages_thematiques/numerique/projet_miellees/

ailleurs, les constructeurs des balances connectées participant au projet « Miellées » craignaient une diminution des opportunités économiques lors de la mutualisation des données par un pillage de leur savoir-faire, par exemple. Si l'ouverture des données est conditionnée à l'autorisation des apiculteurs, les chercheurs doivent trouver des solutions afin d'encourager le partage de leurs données. Dans le cadre du projet « Miellées », les chercheurs garantissent l'anonymat en ramenant le point de localisation GPS de la ruche suivie au centre de la commune dans laquelle elle est déclarée et fournissent un accès limité aux données des balances connectées au seul apiculteur et propriétaire de la balance dans l'application du constructeur. De plus, d'autres freins au partage des données peuvent être relevés tels que les freins techniques. Dans le projet « Miellées », les constructeurs doivent pouvoir partager les données sur une interface qui nécessite d'utiliser les mêmes API[1277]. Par conséquent, les chercheurs doivent faire face à de nombreux obstacles avant de parvenir à la collecte des données d'observation dont ils auraient besoin pour mener à bien leur projet de recherche.

2. Les méthodes limitées de collecte des données à des fins de recherche

461- **Production de données.** Pour mener à bien leurs projets de recherche, les chercheurs produisent ou collectent de nombreuses données. Il peut s'agir de chiffres, des relevés de température, de textes, d'images de télédétection, des sons, des questionnaires, d'enquêtes, etc. Afin d'obtenir ces données, les chercheurs peuvent procéder à une expérimentation afin d'obtenir des données expérimentales. Mais ces données ne sont pas toujours suffisamment représentatives des exploitations agricoles. Elles s'avèrent donc limitées à des fins de recherche scientifique.

462- **Réseaux d'observation.** La solution la plus efficace est de monter un réseau d'observation qui, bien que coûteux, permet d'obtenir des données d'observation offrant une grande diversité et une meilleure représentativité afin de tester plus de leviers agroécologiques. Le réseau d'observation sert ainsi à varier les observations pour prendre en compte divers types de cultures ou méthodes culturales, les variations de température, la pluviométrie ou bien encore différents sols. Ces données sont obtenues au moyen d'enquêtes, d'appels, de monographies, mais aussi par le partage des données des exploitants agricoles. Aussi, le partage des données d'une exploitation implique donc une participation volontaire des agriculteurs et des entreprises qui détiennent ces données. À cette fin, les chercheurs doivent mettre en avant les avantages

[1277] Sur l'interopérabilité, voir *infra,* n°664 et s.

d'un tel partage. La recherche sert avant tout la cause de l'agriculture, elle permet de créer de nouveaux services, de nouveaux outils d'aide à la décision, mais aussi de créer des référentiels pour l'ensemble des agriculteurs.

463- **Exception de TDM.** L'exception de fouille de textes et de données ou *Text and Data Mining* (TDM)[1278] est défini à l'article L. 122-5-3 du CPI[1279] comme la « *mise en œuvre d'une technique d'analyse automatisée de textes et de données sous forme numérique afin d'en dégager des informations, notamment des constantes, des tendances et des corrélations* ». Il s'agit d'une exception au droit d'auteur[1280] et au droit *sui generis*[1281] qui organisent un monopole sur les droits de copie et de reproduction des bases de données. L'exception de fouille de textes et de données comporte deux composantes.

La première composante de l'exception bénéficie aux organismes de recherche, aux institutions du patrimoine culturel et, depuis le décret n°2022-928 du 23 juin 2022[1282], à d'autres personnes y compris dans le cadre d'un partenariat sans but lucratif avec des acteurs privés. Cette exception permet de copier ou de reproduire le contenu de la base de données sans demander l'autorisation de l'auteur ou du producteur de la base en vue de fouilles de textes et de données menées aux seuls fins de la recherche scientifique. Lorsque la fouille de textes et de données est effectuée « *par une autre personne, y compris dans le cadre d'un partenariat sans but lucratif avec un acteur privé* », pour le compte des bénéficiaires cités précédemment, une convention sera passée entre les deux parties afin de préciser les modalités d'accès aux œuvres, de stockage et de destruction[1283]. Les institutions doivent être en mesure de fournir « *aux titulaires de droits d'auteur, à la demande de ceux-ci, tous documents et justificatifs* » sur le stockage des œuvres. En contrepartie, les titulaires de droits d'auteur fournissent aux institutions, à la demande de celles-ci, les modalités de réalisation des reproductions numériques d'œuvres dans le cadre de la fouille de textes et de données. De plus, ces acteurs doivent préalablement avoir obtenu un accès licite à la base de données, ce qui implique qu'ils doivent avoir eu accès soit à des données publiques dans le cadre du dispositif des données ouvertes, soit avoir obtenu l'accès après accord contractuel au moyen d'un abonnement entre

[1278] Voir *supra*, n°265.
[1279] Issu de l'ordonnance n°2021-1518 du 24 nov. 2021, qui transpose la directive 2019 après avis du CSPLA, Transposition des exceptions de fouille de textes et de données : enjeux et propositions, du 18 déc. 2020.
[1280] CPI, art. L. 122-5, 10°.
[1281] CPI, art. L. 342-3, 6°.
[1282] Décret n°2022-928 du 23 juin 2022 portant modification du code de la propriété intellectuelle et complétant la transposition de la directive 2019/790 du 17 avr. 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique.
[1283] CPI, art. R. 122-23.

les titulaires de droits et les organismes de recherche[1284]. Ainsi, cette première condition limite les possibilités pour les chercheurs d'utiliser les données contenues dans les bases de données à des fins de recherche puisqu'ils doivent au préalable avoir obtenu l'accès à la base par l'auteur ou le producteur. Il semble alors qu'il s'agisse d'un consentement détourné. En effet, si l'auteur ou le producteur consent à laisser l'accès à sa base, il consent par extension à ce que les utilisateurs puissent fouiller les données à des fins de recherche, en vertu de ce principe. De plus, l'article L. 122-5-3 du CPI prévoit également comme condition que « *les copies et reproductions numériques effectuées lors d'une fouille de textes et de données sont stockées avec un niveau de sécurité approprié et peuvent être conservées à des fins exclusives de recherche scientifique* ». Ainsi, ceux qui ont accès à la base de manière licite doivent assurer un niveau de sécurité de sorte qu'elles seules puissent y accéder par la validation de leur adresse IP par exemple ou par l'authentification de l'utilisateur[1285]. Mais au sens de la directive[1286], cette exigence doit rester proportionnée aux risques inhérents et ne pas compromettre l'application effective de l'exception, ce qui se traduit à l'article L. 122-5-3 du CPI comme un niveau de sécurité approprié. Néanmoins, il demeure que cette obligation est contraignante pour les organismes de recherche et les autres personnes qui accèdent aux contenus des bases de données de manière licite.

La deuxième composante de l'exception de fouilles de textes et de données concerne toute personne, quelle que soit la finalité de la fouille qui a obtenu un accès licite dans cet objectif. Cette personne peut alors copier et reproduire le contenu de la base de données. Néanmoins, si la personne qui souhaite bénéficier de cette exception aux bases de données est confrontée à la même difficulté qui consiste à accéder de manière licite à la base de données avant de pouvoir les fouiller, il doit en plus se soumettre à la volonté de l'auteur ou du producteur qui bénéficie d'un droit d'opposition, autrement nommé *Opt out*. Cette option permet à l'auteur ou au producteur de s'opposer de manière appropriée à l'exception de TDM. Il peut s'y opposer notamment au moyen de procédés lisibles par machine et par le recours à des conditions générales d'utilisation pour les contenus mis à la disposition du public en ligne[1287]. L'auteur ou le producteur de bases de données peut donc choisir de refuser la possibilité aux utilisateurs d'extraire, de copier ou de reproduire le contenu de leur base afin

[1284] ROBIN, A., *Droit des données de la recherche, op. cit*., n°197, p. 154.
[1285] *Ibid.*, n°198, p. 154.
[1286] Cons. 16.
[1287] Décret n°2022-928 du 23 juin 2022 portant modification du code de la propriété intellectuelle et complétant la transposition de la directive n°2019/790 du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique : *JORF* n°0145 du 24 juin 2022, art. 1.

d'effectuer une fouille de textes ou de données. Ainsi, il est difficile de mettre en œuvre cette exception dont les conditions en font une exception restrictive. De plus, depuis le décret du 23 juin 2022[1288], lorsque les fouilles de textes et de données sont réalisées à des fins autres que la recherche scientifique, des documents justifiant le bon stockage des reproductions d'œuvres, ainsi que la destruction de ces dernières, doivent être fournis. Par ailleurs, dans ce cas précis, les auteurs peuvent formuler une opposition à ces fouilles, sans la motiver, « par tout moyen ». Dans tous les cas, les copies et les reproductions doivent être détruites à l'issue de la fouille de textes et de données afin d'éviter une circulation incontrôlée.

II. L'organisation de l'accès ouvert aux données privées

464- S'agissant des données privées, la logique est inverse à celle des données publiques, il ne s'agit plus d'organiser la diffusion la plus large possible des données, mais bien de les réserver économiquement, et donc intellectuellement. Aussi, la licence sert à organiser l'accès et à autoriser, si nécessaire, l'utilisation des données. C'est sur le principe de la liberté contractuelle que reposent ces contrats. En contrôlant l'accès aux données, l'entreprise maîtrise l'utilisation des données que reçoivent leurs co-contractants, au moyen de clauses d'exclusivité ou de clauses de responsabilité. C'est donc l'entreprise qui a la maîtrise de l'accès aux données collectées ou issues de l'exploitation agricole, qui contrôle également par extension leur usage. Par conséquent, l'entreprise peut, au titre de la liberté contractuelle, et en l'absence de toute règle d'ordre public, fixer les conditions d'accès et d'usage qu'elle souhaite à son cocontractant. Le droit d'accès entre donc dans l'économie globale du contrat. Mais, les conditions d'accès peuvent être sources de déséquilibre entre les droits et les obligations des parties. Aussi, l'accès peut être défini contractuellement (**A**) ou passer par un tiers de confiance (**B**).

A. Le contrôle de l'accès des données privées par la licence d'utilisation

465- L'accès aux données entre dans l'économie des contrats de l'agriculture numérique (**1**), en contrepartie du paiement d'un abonnement (**2**).

[1288] *Ibid.*

1. L'accès aux données dans l'économie des contrats de l'agriculture numérique

466- L'agriculteur obtient par la souscription d'une licence d'utilisation un droit d'accès aux données qu'il génère par son activité auprès de l'entreprise qui les collecte. Il s'agit donc d'un contrat de prestation de services autrement désigné de contrat de louage d'ouvrage dans le Code civil. Ce contrat peut être défini comme la convention par laquelle une personne s'oblige contre rémunération à exécuter un travail de façon indépendante et sans représenter son cocontractant. Elle se distingue du contrat portant sur les biens (vente, location, etc.). Par conséquent, la souscription à la licence d'utilisation du logiciel permet à l'agriculteur d'obtenir l'accès aux données prélevées sur son exploitation une fois traitées et transformées par le prestataire de services. L'objectif étant d'obtenir des informations pertinentes pour l'exploitation agricole.

En outre, pour extraire ou réutiliser une partie de la base, même non substantielle, encore faut-il y avoir accès. Or, l'accès à la base est évidemment contrôlé par le producteur, qui autorisera uniquement ceux qui accepteront le contrat (l'abonnement) qu'il leur proposera[1289]. Les tiers au contrat n'auront donc pas accès aux données de l'utilisateur.

467- Dans la mesure où l'agriculteur en souscrivant au service accède aux données de son exploitation, il semble que « *l'accès se confond(e) avec le service* »[1290]. En effet, l'accès aux données prévu contractuellement est une prestation rendue en échange du paiement d'un abonnement par l'agriculteur-utilisateur du logiciel ou de l'application. L'accès aux données participe de l'économie globale[1291] du contrat de prestation de services : l'entreprise vend ou loue le matériel, l'agriculteur collecte les données en utilisant ce matériel, puis ces données sont agrégées dans les serveurs de l'entreprise qui les traite ensuite afin de mettre à disposition de l'agriculteur, utilisateur, les données transformées desquelles sont tirées des informations utiles à l'exploitation agricole. L'objectif étant de créer, entre autres, de l'aide à la décision. Par ailleurs, l'accès au service entre dans la définition retenue de l'utilisateur dans les contrats de l'agriculture numérique. En effet, l'utilisateur final, aussi désigné selon les contrats, client, titulaire du droit ou partenaire, est défini généralement comme celui qui accède au contenu du logiciel ou de l'application. L'accès étant entendu comme une prestation permettant de rendre le service accessible aux utilisateurs.

468- La contrepartie dans les contrats de l'agriculture numérique est le paiement d'un abonnement lié à l'achat ou à la location d'un matériel connecté. L'exploitation des données permet à

[1289] LE TOURNEAU, P., *Contrats informatiques et électroniques, op. cit.*, n°343.42.
[1290] PILLET, G., « L'efficacité du droit français des contrats face aux géants de l'internet », *op. cit.*, p. 273.
[1291] *Ibid.*

l'entreprise d'offrir en réalité de « *meilleurs produits ou services, de créer des applications pertinentes, de mieux cibler sa clientèle, de prendre de meilleures décisions stratégiques* »[1292]. Par exemple, de nombreux contrats de l'agriculture numérique prévoient des clauses permettant de faire remonter les données techniques sur l'utilisation du service par le client vers le prestataire pour améliorer le service et optimiser les paramétrages. Ainsi, la société Ekylibre prévoit dans ses conditions générales d'utilisation pour la souscription aux abonnements qu'elle propose, une clause selon laquelle le prestataire « *dispose d'un droit d'accès et d'utilisation des données (celles de l'utilisateur collectées au titre de l'utilisation du Site et de l'Application) dans l'intérêt de l'utilisateur, des services et des fonctionnalités* ». En outre, « *les données peuvent être valorisées auprès de tiers concessionnaires de leur utilisation* »[1293]. C'est le cas notamment lorsqu'un prestataire souhaite, accéder, distribuer ou vendre à ses clients un logiciel, une application et/ou des outils informatiques qui appartiennent à un autre opérateur. Les conditions générales de vente entre le développeur de la solution et le prestataire peuvent convenir que ce dernier garantit au développeur qu'il a bien les droits sur les données brutes et/ou traitées *via* les solutions informatiques afin de permettre au développeur d'avoir un droit d'utilisation et d'exploitation de ces données. Parfois, les données font l'objet d'échanges dans le cadre d'une relation commerciale ou dans le cadre collaboratif. Par exemple, « *dans le cas d'applications collaboratives, le Client accepte, par l'utilisation de l'outil, la mise à disposition des données collectées sur son outil, au profit de la collectivité ; ces données permettant d'optimiser les informations concernées* »[1294].

2. Les effets du contrôle de l'accès contractuel sur l'usage

469- Le contrat ou la licence d'utilisation confèrent au souscripteur divers droits sur les données mises à disposition dans le cadre de l'accord contractuel. Les licences d'utilisation permettent donc d'organiser l'usage qui peut être fait des données par le co-contractant au cours de la relation. Le donneur de licence peut aussi restreindre l'usage des données, comme c'est le cas pour celles qui ont été enrichies.

470- Le contrôle de l'usage des données dans les licences d'utilisation. En dehors des exceptions du droit d'auteur et du droit *sui generis*, les bases de données sont fermées et peuvent être

[1292] *Ibid.*
[1293] COLLIN, P. et COLIN, N., *Mission d'expertise sur la fiscalité de l'économie numérique*, Rapport, janv. 2013, p. 2.
[1294] Aux termes de l'article 6.3 des Conditions Générales d'Utilisation : Progiciels et matériels de la société Isagri.

exploitées à condition d'obtenir l'autorisation du titulaire de droit, au moyen d'un contrat d'exploitation. Ainsi, le titulaire d'un droit d'auteur sur la base de données pourra autoriser le licencié à utiliser cette base, pour qu'il puisse l'interroger. Néanmoins, il ne peut empêcher le licencié de procéder aux actes nécessaires à l'accès au contenu d'une base de données électronique pour les besoins et dans les limites de l'utilisation prévue par le contrat[1295]. S'agissant du droit *sui generis*, « *le producteur d'une base de données a le droit d'interdire l'extraction et/ou la réutilisation du contenu de sa base, ces droits peuvent être transmis ou cédés ou faire l'objet d'une licence* »[1296]. Par conséquent, le producteur de la base peut prévoir une licence d'utilisation qui n'autorise que l'accès à la base et interdit tout usage, transformation ou encore partage de cette base de données. La licence contient alors des clauses relatives « *à l'utilisation qui peut être faite des données ou des résultats obtenus par leur interrogation* »[1297]. À noter que lorsque le producteur de la base de données ne bénéficie pas de la protection du droit de la propriété intellectuelle, il peut prévoir les conditions qu'il souhaite dans ses licences d'utilisation au nom de la liberté contractuelle[1298].

S'agissant de l'objet des licences d'utilisation, elles ne portent que sur des œuvres de l'esprit sur lesquelles l'auteur ou le créateur détient des droits. Elles ont donc vocation, en principe, à s'appliquer aux logiciels ou aux bases de données. Le donneur de licence peut fixer à l'utilisateur les droits d'utiliser, de copier, de modifier ou de diffuser l'œuvre, mais il peut également limiter les droits cédés. Ainsi, les titulaires de droits peuvent interdire toute modification de l'œuvre, c'est le cas notamment des *Creatives commons* qui sont des licences ouvertes dont l'objectif est de mettre à disposition des œuvres. Les licences peuvent être classées de la plus fermée à la plus ouverte. En effet, lorsque des bases de données privées sont mises à disposition sur une plateforme (place de marché en ligne) par des structures privées afin de répondre à une demande, la plateforme propose alors une solution de contractualisation en ligne[1299]. Sur ce modèle, la plateforme API-AGRO a construit ses propres licences et propose trois types de contrats différents, pour le diffuseur des données, plus ou moins ouverts. Les licences *Creative commons*[1300] sont les plus ouvertes et peuvent autoriser la modification, le partage et la redistribution dans un but commercial de l'œuvre. L'ouverture des données est donc modulable selon les usages que le donneur de licence souhaite permettre aux utilisateurs.

[1295] CPI, art. L. 122-5, 5e.
[1296] CPI, art. L. 342-1, voir *supra*, n°299.
[1297] BERTRAND, A., *Droit d'auteur*, Dalloz action, 2010, n°201.39.
[1298] Voir *supra*, n°305 et s.
[1299] ROBIN, A., « Les places de marché en ligne », *JCl. Commercial*, fasc. 825, 826 et 827.
[1300] Voir *supra*, n°438.

Ainsi, il est possible de ne prévoir qu'un droit d'accès et de partage sans modifications ou d'ajouter la possibilité de modifier l'œuvre à condition qu'elle soit distribuée sous la même licence. La licence peut également prévoir une autorisation de diffusion dans un but non lucratif. Celui-ci a donc le choix entre le contrat type, un contrat *ad hoc* dans lequel il peut moduler les clauses selon ses besoins et intérêts ou un contrat sous format *Open Data* qui permet de mettre à disposition les données dans le domaine public de manière volontaire. Le contrat type définit les conditions et modalités d'échange et d'utilisation de la base de données. Il peut être modulé à partir de clauses types proposées par la plateforme selon les besoins du fournisseur de données. Le contrat *ad hoc* est plus malléable et permet au fournisseur de données de soumettre ses cocontractants aux conditions qu'il souhaite. En définitive, les licences d'utilisation, telles qu'elles sont construites, organisent la mise à disposition des données et peuvent prévoir la capacité pour le cocontractant d'utiliser les données, de les transformer et de les redistribuer.

Il existe également des licences d'utilisation « multi-utilisateurs », que l'on peut nommer « guichet unique ». Ces licences permettent de mutualiser les droits d'utilisation sur les données en définissant une liste de bénéficiaires dans le cadre de la licence qui pourra accéder à ces données *via* un guichet unique. Les utilisateurs finaux sont alors autorisés par la licence à mettre en ligne les données pour des applications précises[1301]. Par exemple, les images mises à disposition, par le Centre national d'études spatiales (CNES) et la société *Airbus Defense and Space,* permettent à la communauté scientifique, aux acteurs publics français ou aux entreprises privées prestataires d'acteurs publics de les utiliser à des fins de recherche scientifique ou d'aide à l'action publique. Notamment, il peut s'agir de la gestion de l'environnement, des territoires, des risques naturels et des populations[1302].

471- **L'efficacité relative des clauses d'exclusivité.** Les entreprises qui fournissent des outils d'aide à la décision ou des services liés rédigent souvent des clauses d'exclusivité sur les données enrichies dans les conditions générales d'utilisation à leur bénéfice. Ces CGU sont soumises au principe de liberté contractuelle. Aussi, le détenteur des données et de la base non protégeable par un droit *sui generis* qui les contient peut verrouiller l'accès au moyen du contrat d'utilisation[1303]. L'intention est d'organiser, une fois de plus, la maîtrise contractuelle des données à l'égard de celui qui apporte un savoir-faire, une technologie ou des moyens financiers et/ou humains pour le traitement des données. Cependant, en l'absence d'originalité il n'existe

[1301] ROBIN, A., *Droit des données de la recherche, op. cit*., n°210, p. 162.
[1302] Equipex Géosud.
[1303] ROBIN, A., *op. cit.*, n°173, p. 135.

pas, pour l'heure, de droit de propriété sur les données enrichies, pas plus qu'il en existe sur les données brutes, à moins de démontrer un enrichissement de la donnée qui témoignerait de la créativité de son auteur, comme c'est le cas notamment pour les données satellitaires[1304]. L'intérêt d'une telle clause est limité dans la mesure où une fois que les données sont diffusées, il serait très difficile d'en interdire l'usage par des tiers. En revanche, elle peut permettre d'engager la responsabilité du co-contractant qui les aurait diffusées en dépit de cette clause. Mais, le secret des affaires, au moyen d'une clause de confidentialité, parvient au même résultat et assure à son bénéficiaire la conservation de l'exclusivité sur les données. Par conséquent, il est plus intéressant de se tourner vers les sanctions pénales en cas de non-respect d'une clause de confidentialité que de prévoir une clause d'exclusivité dont les effets seront limités. De plus, une fois qu'elles sont diffusées, il devient impossible de contrôler l'usage des données puisque la détention et l'usage par l'un n'épuisent pas les usages des autres[1305]. Ainsi, le seul moyen de contrôler l'utilisation des données est d'en limiter l'accès.

472- **L'efficacité des clauses de confidentialité.** Le droit organise ainsi la réservation des informations avec le secret. En contrôlant l'accès aux données, les entreprises maîtrisent également l'usage qui en est fait. Tout d'abord, ce contrôle se fait au moyen des conditions d'utilisation prévues au contrat qui définissent les usages possibles des données. Ensuite, les entreprises maîtrisent la circulation des données en contrôlant l'étendue des personnes qui y ont accès. Elles contrôlent, donc, par extension, leur utilisation. Si seuls les agriculteurs ont accès aux données dans les conditions d'usage prévues au contrat, cela réduit les risques que les données circulent et soient utilisées par d'autres.

473- **Clause de responsabilité.** En cas d'utilisation des données dans des conditions non prévues dans le contrat, la clause de responsabilité permet de rompre unilatéralement la relation contractuelle et ainsi de fermer l'accès aux données. Elle peut prévoir des dommages et intérêts pour la partie lésée. En outre, la violation d'un secret des affaires peut, également, conduire au paiement d'une indemnité.

Le contrôle de l'usage des données se fait donc par la maîtrise de l'accès. Si une entreprise ne souhaite pas ouvrir l'accès à sa base de données à ses concurrents, rien ne peut l'y contraindre[1306], sauf à considérer la base de données comme une infrastructure essentielle[1307].

[1304] Voir *supra*, n°60.
[1305] AUBIN-BROUTE, R.-J., « Le contrat pour la maîtrise des données agricoles », *op. cit.*
[1306] Com., 21 juin 2017, pourvoi n°15-25.941, inédit.
[1307] Voir *supra*, n°212.

B. Le contrôle de l'accès et de l'usage des données confidentielles par un tiers de confiance

474- Afin de mener à bien des projets de recherche scientifique ou historique, les acteurs ont parfois besoin d'accéder aux données confidentielles collectées par d'autres acteurs. Il faut noter que sur le plan technique une solution existe afin d'assurer le respect des règles de sécurité. Il s'agit de recourir « *à un tiers de confiance capable d'assurer une prestation technique de sécurisation des données* »[1308]. Ce sont des infrastructures de données créées dans l'objectif de stocker des données confidentielles « *dont l'utilisation est conditionnée par le respect des procédés rigoureux de sécurisation des données souvent imposées par les textes eux-mêmes, ainsi que des règles légales et contractuelles de confidentialité* »[1309]. Ce contrôle passe par un tiers de confiance qui assure la prestation technique de sécurisation des données comme le fait le Centre d'accès sécurisé aux données (CASD)[1310]. Ces infrastructures permettent d'assurer un haut niveau de sécurité pour l'accès et l'utilisation de données individuelles dans le respect de procédés rigoureux de sécurisation des données souvent imposés par les textes eux-mêmes (**1**). L'accès aux données au moyen d'un tiers de confiance nécessite la mise en place de modalités techniques et contractuelles (**2**).

1. Le Centre d'accès sécurisé aux données

475- Le Centre d'accès sécurisé aux données (CASD) organise et met en œuvre des services d'accès sécurisé pour les données confidentielles à des fins non lucratives de recherche, d'étude, d'innovation ou d'évaluation, pour des services à la recherche principalement publique, mais aussi il valorise la technologie développée pour sécuriser l'accès dans le secteur privé[1311]. Dans le cadre de la recherche, le CASD a pour missions de mettre en œuvre des services sécurisés d'accès aux données confidentielles ; de participer aux opérations d'appariement, d'anonymisation de données et à la constitution de bases de données ; de participer à la documentation et à l'archivage des données confidentielles ; de participer aux séances du

[1308] ROBIN, A., *Droit des données de la recherche, op. cit*., n°172, p. 134.
[1309] *Ibid*.
[1310] Le CASD est un groupement d'intérêt public (GIP) créé par arrêté interministériel du 29 décembre 2018 et rassemble l'INSEE, le GENES, le CNRS, l'École polytechnique et HEC Paris. Il organise et met en œuvre des services d'accès sécurisé pour les données confidentielles à des fins non lucratives de recherche, d'étude, d'innovation ou d'évaluation, pour des services à la recherche principalement publiques. Il a également pour mission de valoriser la technologie développée pour sécuriser l'accès dans le secteur privé.
[1311] https://www.casd.eu/le-centre-dacces-securise-aux-donnees-casd/gouvernance-et-missions/

Comité du secret statistique et de collaborer avec son secrétariat ; d'animer la communauté d'utilisateurs autour des données confidentielles ; de concourir à la certification des résultats de la recherche s'appuyant sur les données confidentielles ; de participer au développement de l'accès aux données confidentielles au niveau national, au niveau européen et au niveau international en lien avec les autres dispositifs de mise à disposition de données. Dans le cadre de ses missions de valorisation, notamment auprès du secteur concurrentiel, le groupement d'intérêt public doit assurer conseil et expertise dans ses domaines de compétence auprès de l'État et d'autres entités françaises ou étrangères, fournir des moyens ou des services de sécurisation dans ses domaines de compétence et mettre à disposition la technologie de sécurisation d'accès aux données à des fins privées.

Par conséquent, pour la mise à disposition sécurisée des données et leurs appariements, le CASD sert de tiers de confiance et garantit aux déposants de données un stockage, une mise à disposition et un usage de leurs données qui sont conformes aux termes des conventions et contrats passés avec eux et aux exigences de protection de la confidentialité de ces données. Il maintient, également, une infrastructure et une qualité de service de haut niveau qui permettent un accès aux données dans de bonnes conditions pour les utilisateurs. Enfin, il fournit un accès sécurisé et équitable aux utilisateurs de données accrédités, permettant des traitements et des analyses pointus dans les meilleures conditions de travail.

2. Les modalités d'accès aux données confidentielles par le Centre d'accès sécurisé aux données

476- Le CASD est un service payant qui permet donc aux acteurs publics ou privés d'analyser, de traiter ou encore de mettre à disposition de tiers les données qu'ils produisent dans des conditions de sécurité optimale. Pour cela, dans le secteur agricole, la personne qui souhaite accéder aux données confidentielles doit en faire la demande auprès du comité du secret statistique (CSS) en ce qui concerne les données mises à disposition par le ministère de l'Agriculture et de l'Alimentation. S'agissant des données du CSS, celui-ci veille au respect des règles du secret statistique et donne son avis sur les demandes de communication de données individuelles collectées par voie d'enquête statistique ou transmises au service de la statistique publique à des fins d'établissement des statistiques. Une fois l'avis favorable donné, les membres du projet qui souhaitent effectivement accéder aux données obtiennent une carte d'accès et un contrat est établi afin de garantir la bonne utilisation du service par les demandeurs d'accès.

Le CASD propose également aux entreprises privées de mettre à disposition leurs données confidentielles avec de hauts niveaux de sécurisation, auquel cas la demande d'accès se fait directement auprès de l'entreprise privée qui a mis à disposition ses données.

Dans le secteur de l'agriculture numérique, de nombreuses données sont collectées par le CSS du ministère de l'Agriculture et de l'Alimentation afin de réaliser des enquêtes statistiques. Ces données sont diffusées de manière anonymisée sur le site Agreste. Pour pouvoir fouiller et explorer les données confidentielles contenues dans ces bases, les acteurs doivent donc demander un accès auprès du CSS et en cas d'avis favorable, le CASD met en place l'accès effectif et sécurisé à ces données. C'est le cas notamment des données collectées dans le Registre agricole, celles du réseau d'information comptable agricole ou celles des pratiques culturales en grandes cultures.

§2. *La régulation de la réutilisation des données agricoles privées*

477- Les données sont caractérisées par des « *externalités fortes* » et un « *un coût marginal très faible* », aussi « *ce ne sont pas toujours ceux qui détiennent les données qui sont en mesure d'en extraire la valeur maximale* »[1312]. C'est pourquoi la question du partage des données agricoles est fondamentale dans un marché gouverné par le jeu de la concurrence et la mise en place de barrières à l'entrée. Or, pour éviter l'effet « tas d'or », il est essentiel d'assurer la circulation de certaines données afin de favoriser leur réutilisation. Jusqu'en 2020, l'approche plébiscitée par le législateur européen était l'autorégulation et la régulation *a minima* avec le règlement sur la libre circulation des données non personnelles. Mais, les enjeux forts de la concurrence américaine et chinoise sur le marché des données non personnelles ont conduit le Parlement européen et le Conseil à faire des propositions de règlements pour organiser une forme de gouvernance sur les données. Tout d'abord, il faut constater l'échec des initiatives de partage des données privées non personnelles dans le secteur agricole (**I**). Ensuite, il faudra envisager les propositions de régulation du partage des données non personnelles (**II**).

[1312] CYTERMANN, L., « Le partage des données, un enjeu d'intérêt général à l'ère de l'intelligence artificielle », *op. cit.*

I. Le constat d'échec du partage des données privées non personnelles dans le secteur agricole

478- De nombreuses initiatives ont été menées de front par les acteurs pour le partage des données non personnelles dans le secteur agricole (**A**), mais il faut s'interroger sur les raisons de l'échec de ces initiatives (**B**).

A. Les nombreuses initiatives du partage des données non personnelles

479- Tout un écosystème s'est créé dans le secteur agricole (**1**) afin d'organiser le partage des données entre les acteurs (**2**).

1. L'écosystème du partage des données agricoles

480- Certaines plateformes n'ont pas pour objectif le partage ou la mutualisation des données. C'est le cas notamment de celles développées « *pour l'utilisation d'objets et dispositifs connectés à l'internet des objets* » avec pour objectif « *de garantir [leurs] fonctionnalités […] et d'autoriser des services à valeur ajoutée* »[1313]. Ces plateformes-là sont réservées aux utilisateurs d'objets connectés ou pour l'utilisation de logiciels et d'applications et n'ont pas pour objectif de partager les données. C'est le cas notamment des plateformes créées par les créateurs d'objets connectés, tels que SMAG, ITK, etc[1314]. À titre informatif, il peut exister également des plateformes qui sont « *à l'usage exclusif d'un seul détenteur de données pour lui permettre d'utiliser les données qu'il détient* »[1315].

En revanche, il existe des plateformes dont l'objectif est de rendre effectif le partage des données non personnelles. À ce titre, un écosystème s'est mis en place au cœur duquel se trouvent ces plateformes. Ces dernières servent de prestataires de services pour le partage de données sur des marchés bifaces et multifaces entre détenteurs et utilisateurs de données. Ce sont donc des intermédiaires dans la relation entre ces différents acteurs. S'agissant de la mise en œuvre du partage effectif des données, ces plateformes de partage peuvent avoir un caractère collaboratif, participatif ou altruiste. Elles peuvent reposer sur un modèle ouvert, dans ce cas,

[1313] Commission européenne, Proposition de règlement sur la gouvernance européenne des données (acte sur la gouvernance des données), COM (2020) 767 final, 25 nov. 2020, adoptée le 4 avr. 2022.
[1314] Voir *supra*, n°184.
[1315] Acte sur la gouvernance des données, préc., cons. 22.

les données sont mises à disposition sans limite de public à titre gratuit ou onéreux. Elles peuvent avoir une dimension nationale comme Etalab et API-AGRO, ou régionale comme Zabal pour le Pays basque, Harmony Grand Est et Wiuz ou par filières comme Domopig. Mais aussi, les plateformes peuvent avoir un modèle fermé, auquel cas, la communauté d'acteurs ayant accès aux données est restreinte. Cette communauté « *choisit de mettre en commun des données et détermine les obligations personnelles relatives à l'accès aux utilités des données compilées* »[1316]. Ce modèle de plateforme est proposé par Farmleap qui est une plateforme fermée dont l'objectif est d'échanger des données entre groupes d'agriculteurs et leur permettre de se comparer de manière anonyme.

2. L'organisation du partage des données dans le secteur agricole

481- Le secteur agricole s'organise depuis déjà plusieurs années pour le partage des données de l'amont vers l'aval. D'abord, au niveau de l'Administration publique, la plateforme Etalab est un outil permettant le partage et l'utilisation des données publiques. De nombreux jeux de données concernent le secteur agricole. Néanmoins, ces jeux de données n'ont pour la plupart qu'un intérêt relatif. En effet, très peu d'entre eux sont consultés et réutilisés, en 2021, seuls 5 % sur les 1063 fichiers correspondant à l'agriculture ont été ouverts au moins une fois. Il est possible ainsi d'affirmer qu'il existe une véritable « *inadéquation entre l'offre proposée par Etalab et la demande de données agricoles* »[1317]. Ensuite, les acteurs du secteur agricole se sont concertés autour de la création de portails ouverts de données agricoles dans le cadre d'un projet financé en CasDAR[1318] de 2013 « Recherche Finalisée et Innovation ». À la suite du rapport « #AgricultureInnovation 2025 » de 2015, M. J.-M. Bournigal, alors président de l'IRSTEA, « *avait été missionné par le gouvernement pour préparer la mise en place opérationnelle* » d'un portail de données agricoles[1319]. Ce portail, d'abord, nommé AgGate a laissé la place à API-AGRO[1320]. Qui est à l'origine un souhait des instituts techniques agricoles, avec l'appui de l'ACTA[1321], de développer une plateforme commune d'API (*Application Programming*

[1316] AUBIN-BROUTE, R.-J., « Le contrat pour la maîtrise des données agricoles », *op. cit.*
[1317] WAINSTAIN, J., « Partager les données pour réussir les transitions agricoles et alimentaires », in ABIS, S. et BRUN, M., ss. dir., *Le Démeter 2021, Produire et se nourrir : le défi quotidien d'un monde déboussolé*, IRIS éd., févr. 2021, pp. 191 à 206.
[1318] Compte d'affectation Spécial au Développement Agricole et Rural (CasDAR) est financé par les agriculteurs au moyen d'une taxe prélevée sur leur chiffre d'affaires. Il finance l'appui à l'innovation et au développement agricole et rural.
[1319] https://le-lab.agriculture.gouv.fr/post/153818957488/st%C3%A9phane-le-foll-thierry-mandon-et-axelle-lemaire
[1320] https://api-agro.eu/licence_personnalisee/
[1321] Association de coordination technique agricole

Interface). L'objet principal de cette plateforme est « *d'exposer un catalogue de données et de fondement de calcul produits par les chercheurs et ingénieurs des instituts* »[1322]. Plusieurs partenaires, à l'origine, les Instituts Techniques Agricoles (ITA) et des partenaires de la Recherche & Développement (Inra, Agro-Transfert Ressources et Territoires), se sont rassemblés autour de ce projet afin de couvrir « *les besoins de l'ensemble des filières agricoles végétales et animales* »[1323]. La société AgDatahub a donc pour ambition de valoriser les données des acteurs agricoles (Acteur de R&D, acteurs privés) à travers la plateforme API-AGRO. Cette plateforme permet d'organiser l'ouverture et le partage des données avec des API plus ou moins ouvertes selon le degré de sensibilité des données. En effet, ce portail de données à destination de l'écosystème agricole facilite le partage des données, leur croisement et la création de nouveaux services pour les agriculteurs. La plateforme expose un ensemble de données provenant de différentes sources, il peut s'agir de données météorologiques, de données phytosanitaires, d'épidémiosurveillance, de pratiques agricoles, etc. Il est possible d'accéder à ces données selon la zone géographique, selon les filières[1324], selon le type de données[1325], mais aussi selon l'organisation du fournisseur ou selon le type de licence[1326]. Ainsi chaque organisation qui choisit de partager les données qu'elle détient sur la plateforme peut le faire selon les règles d'accès et d'usage qu'elle souhaite de manière plus ou moins ouverte selon la licence choisie[1327]. Néanmoins, peu de jeux de données sont partagés sur cette plateforme[1328]. Et certaines de ces bases sont déjà partagées sur le site du gouvernement Etalab. Par conséquent, le partage des données agricoles n'est pas encore efficient. La quasi-totalité des jeux de données partagés sur la plateforme provient des instituts de recherche, des instituts techniques agricoles, des chambres d'agriculture et de l'Administration (MAA). Très peu sont mises à disposition par des groupements privés, même si quelques-unes peuvent être relevées telles que des bases de données de Bayer, Weenat, Weathermeasures, Sysfarm ou Agricolio. Finalement, les acteurs de l'agriculture numérique ne partagent que très peu les données qu'ils détiennent malgré les infrastructures mises en place. De plus, certaines bases de données mises à disposition sous *Open Data* se trouvent également diffusées sur la plateforme du gouvernement Etalab, telles que la base de données sur les doses de référence IFT, les données d'Agreste, le RPG, etc.

[1322] SINE, M., HAEZEBROUCK, T.-P. et EMONET, E., « API-AGRO, Création d'une plateforme d'échange de données agricoles fédératrices d'acteurs publics et privés », *Innovations Agronomiques* n°71, 2019, n°211 à 224.
[1323] *Ibid*.
[1324] Grandes cultures, cultures fruitières, cultures légumières, viticulture, élevage ruminant, etc.
[1325] Données techniques, de référence, géolocalisées, règlements, de produits/Services, de production, environnementales, d'Aide à la décision, statistiques, issues de la recherche, etc.
[1326] *Open Data* ou prioritaire.
[1327] Voir *supra*, n°291.
[1328] Cinquante-neuf à l'heure où sont écrites ces lignes.

B. Les raisons supposées de l'échec du partage des données privées non personnelles

482- Plusieurs raisons justifient le manque d'effectivité du partage des données dans le secteur agricole. En effet, les acteurs ne se concertent pas toujours sur le développement des services de partage, ce qui limite la coordination ou le développement de standards communs (**1**). Néanmoins, des projets sont développés afin de trouver des solutions pour améliorer le partage des données dans un écosystème qui reste encore fragmenté (**2**).

1. Le manque de concertation des acteurs du secteur agricole

483- Certains auteurs font le constat d'une ouverture et d'un partage relatifs des données en France malgré la mise en place des plateformes de partage. Une des raisons tient au fait qu'il existe des doublons (entre les plateformes Etalab et API-AGRO, par exemple). Mais aussi parce que les bases de données les plus intéressantes sont souvent, malgré tout, gardées confidentielles[1329]. C'est le cas notamment de Mesparcelles qui propose de visualiser toutes les données d'exploitation dans un logiciel à l'attention des seuls agriculteurs, mais aussi des bases de données nationales d'identification (BDNI), Dephy ou Normabev. Cependant, la plateforme API-AGRO a le mérite de rassembler dans une seule et même plateforme, en grande partie, les données agricoles mises à disposition sur internet. En Allemagne, la société DKE-Data est allée plus loin en proposant la plateforme Agrirouter créée par SAP et demandée par un consortium de constructeurs[1330]. Cette plateforme propose de permettre la circulation des données agricoles collectées par les différents objets connectés et autres dispositifs sans pour autant les stocker. De cette manière, l'agriculteur conserve la maîtrise des données collectées sur son champ puisque le partage des données est soumis à son autorisation. La plateforme offre une parfaite interopérabilité entre les objets connectés, les applications et les logiciels, peu importe leur origine.

En France, l'écosystème du partage des données agricoles est aujourd'hui fragmenté du fait non seulement d'un manque de coordination et de standards communs à toutes les filières, mais aussi d'un défaut de gouvernance. Aussi, le fer de lance du partage repose sur le consentement des acteurs à mettre à disposition les données qu'ils détiennent. Leur méfiance bloque la circulation des données.

[1329] WAINSTAIN, J., « Partager les données pour réussir les transitions agricoles et alimentaires », *op. cit.*
[1330] Agco, Amazone, Grimme, Horsch, Kuhn, Krone, Lemken, Pöttinger, Rauch, et Same Deutz-Fahr.

2. Les initiatives pour l'amélioration du partage des données agricoles

484- De nombreux projets ont vu le jour dans l'objectif toujours de partager les données agricoles. Numagri par exemple regroupe des acteurs clés du secteur agricole[1331]. L'objectif de cette plateforme est de construire un langage commun de l'agriculture numérique[1332], pour une standardisation des données numériques du secteur agricole. De même, la plateforme Numalim permet « *la transparence et la valorisation des démarches de qualité dans l'ensemble de la filière pour les produits alimentaires* »[1333]. D'autres plateformes ont vu le jour, à destination cette fois de certaines communautés. Elles peuvent intéresser un secteur géographique ou une filière particulière. Par exemple, Farmleap permet à de petits groupes d'agriculteurs proches géographiquement de partager leurs données. C'est un outil de comparaison qui peut être anonyme ou non et qui permet aux agriculteurs de recevoir des bilans et des analyses de leurs performances. Dans la filière porcine, la plateforme Domopig permet aux élevages de porcs de partager et de valoriser leurs données selon les autorisations accordées par l'éleveur. Mais encore, la plateforme Harmony Grand Est est une plateforme collaborative qui permet aux acteurs de la région grand Est de partager leurs données. Également, Wiuz est une plateforme qui permet de remonter les données techniques vers les coopératives et les négoces agricoles. Ainsi, un grand nombre d'acteurs se sont positionnés sur le partage des données agricoles dans le but de favoriser l'innovation et le partage d'informations. Mais le constat reste qu'aujourd'hui les données sont partagées dans un sens comme dans un autre à leur strict minimum[1334].

Par conséquent, il faut pallier les différents obstacles au partage et trouver des arguments qui encourageraient les acteurs des filières agricoles en aval et en amont à partager effectivement « leurs » données. Des propositions ont aussi été faites de développer « *des actions d'information et de labellisation auprès des utilisateurs de ces services* » et de procéder « *à une harmonisation maximale des standards de sécurité quant à la conservation et au traitement des données, sur le modèle du mécanisme pensé par le RGPD* »[1335]. Il est également urgent d'améliorer la gouvernance du partage des données agricoles.

[1331] Fondation Avril, Chambre d'agriculture de France, FNSEA, les Jeunes Agriculteurs, Coopérative de France, Terres Univia et API-AGRO.
[1332] https://numagri.org
[1333] https://www.plateforme-numalim.fr portée par l'ANIA, le FFAS, la fondation Avril et GS1 France.
[1334] WAINSTAIN, J., « Partager les données pour réussir les transitions agricoles et alimentaires », *op. cit.*
[1335] ZOLYNSKI C., « Quelle circulation des données non personnelles pour l'Union européenne ? », *op. cit.*

II. La régulation du partage des données privées non personnelles

485- Le partage des données privées dans le secteur agricole est loin d'avoir atteint son apogée. Les acteurs sont encore trop frileux pour partager les jeux de données les plus intéressants. Jusqu'à l'adoption du règlement sur la gouvernance des données le 30 mai 2022, l'encadrement juridique du partage n'était pas suffisant pour rassurer pleinement les détenteurs de données qui souhaitaient partager celles qu'ils avaient en leur possession. Mais, le législateur européen s'est intéressé à la question brûlante du partage des données et a fait plusieurs propositions de règlement afin de réguler ces activités de partage. En effet, le législateur a proposé dès 2020 de réguler les données et les services numériques à travers divers règlements et directives. Ainsi, le législateur prône dorénavant une régulation proactive dont les enjeux reposent en priorité sur un savant équilibre entre maîtrise et partage des données dans sa stratégie européenne pour l'Europe[1336]. En effet, comme le soutient Mme A. Robin, « *le développement de l'économie de la donnée est […] conditionné non seulement par la disponibilité des données et l'accessibilité à celles-ci, mais également par l'assurance d'une utilisation responsable* »[1337]. Deux pans de l'écosystème du partage des données agricoles ont fait l'objet de réflexion autour de leur régulation : d'abord, sur les données elles-mêmes, ensuite, sur les plateformes. Par conséquent, il convient d'envisager, dans un premier temps, le règlement sur la gouvernance des données qui crée un nouveau cadre pour le partage des données (**A**). Dans un second temps, il convient d'étudier la proposition de régulation des plateformes développées en parallèle sur leurs comportements déloyaux (**B**).

A. Le règlement sur la gouvernance des données

486- L'étude du règlement sur la gouvernance des données suppose d'étudier, en premier lieu, ses objectifs (**1**), pour, en second lieu, envisager son contenu (**2**).

1. Les objectifs du règlement sur la gouvernance des données

487- Le Parlement européen et le Conseil ont fait une proposition pour un cadre général de gouvernance afin, d'une part, de permettre aux données de « *circuler facilement au sein de*

[1336] Communication de la Commission Européenne, *Une stratégie européenne pour les données*, COM (2020) 66 final, 19 févr. 2020.
[1337] ROBIN, A., « Exploitation de l'innovation », *CDST*, 12/2021.

chaînes de valeur transsectorielles européennes »[1338] et, d'autre part, de créer des espaces européens communs des données spécifiques, tels que l'agriculture[1339]. Cette proposition devait faire l'objet de projets législatifs en 2021. Ces espaces viendront ensuite compléter la législation sur les données ouvertes et la réutilisation des informations du secteur public[1340]. L'objectif de cette proposition de règlement « *consiste à établir les règles d'une nouvelle gouvernance européenne des données appelée à remplacer le modèle de plateforme actuellement dirigé par les grandes entreprises technologiques* »[1341]. Il a vocation à s'appliquer à certaines catégories de données protégées du secteur public dont le mécanisme de réutilisation est subordonné au respect des droits d'autrui (données personnelles, propriété intellectuelle, confidentialité). Le règlement sur la gouvernance des données devait harmoniser les conditions autorisant la réutilisation des données et interdire les accords d'exclusivité pour le secteur public[1342], sauf lorsque ces accords ont un objectif d'intérêt général. Ensuite, il devait organiser « *le partage des données entre entreprises, contre rémunération sous quelque forme que ce soit* »[1343] ; « *permettre l'utilisation de données à caractère personnel avec l'aide d'un "intermédiaire de partage de données à caractère personnel" conçu pour aider les personnes physiques à exercer leurs droits au titre du RGPD* »[1344]. Enfin, permettre « *l'utilisation de données pour des motifs altruistes* »[1345]. Le règlement sur la gouvernance des données a finalement été adopté le 30 mai 2022[1346].

Aussi, le règlement sur la gouvernance des données établit désormais les conditions de réutilisation de certaines catégories de données détenues par des organismes du secteur public au sein de l'Union européenne ; il fournit un cadre de notification et de surveillance pour la fourniture de services d'intermédiation de données, ainsi qu'un cadre pour l'enregistrement volontaire des entités qui collectent et traitent les données mises à disposition à des fins altruistes et enfin, un cadre pour l'établissement d'un comité européen de l'innovation dans le domaine des données.

[1338] Acte sur la gouvernance des données, préc.
[1339] Un atelier d'information sur un espace européen communs des données agricoles s'est tenu le 2 décembre 2021, organisé par la Commission européenne, et a rassemblé plusieurs acteurs du secteur agricole européen tels que Copa cogeca, CEMA, Agdatahub ou encore FNSEA.
[1340] Dir. n°2019/1024, 20 juin 2019, préc.
[1341] ROBIN, A., « Exploitation de l'innovation », *op. cit.*
[1342] BERTRAND B., « La volonté de réguler les activités numériques », *RTD Eur.* 2021, p. 160.
[1343] Acte sur la gouvernance des données, préc.
[1344] *Ibid.*
[1345] *Ibid.*
[1346] Règl. n°2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement n°1018/1724 (règlement sur la gouvernance des données) : *JOUE* L 152/1 du 3 juin 2022.

2. Le contenu du règlement sur la gouvernance des données

488- **Définition du partage des données.** Le règlement sur la gouvernance des données définit le partage des données comme « *la fourniture de données à un utilisateur de données par une personne concernée ou un détenteur de données, en vue de l'utilisation conjointe ou individuelle desdites données, sur la base d'accords volontaires ou du droit de l'Union ou du droit national, directement ou via un intermédiaire, par exemple dans le cadre de licences ouvertes ou commerciales, moyennant le paiement d'une redevance ou gratuitement* »[1347].

489- **Organisation du partage des données.** Le règlement distingue selon l'origine des données pour organiser leur partage. Tout d'abord, s'agissant des données du secteur public, le règlement prévoit un principe d'interdiction des accords d'exclusivité[1348] afin d'autoriser leur réutilisation, sauf exception. Ensuite, s'agissant des données privées partagées entre particuliers et entreprises (CtoB) et entre entreprises (BtoB), le règlement encadre deux activités de prestations de services l'une à des fins commerciales, l'autre à des fins altruistes. En effet, le règlement encadre l'activité des prestataires de service d'intermédiation de données[1349]. Cependant, sont exclus de cette catégorie : 1°, les services qui n'établissent pas de relations commerciales directes entre les détenteurs de données et les utilisateurs de données, 2°, les services axés sur l'intermédiation de contenus protégés par le droit d'auteur ; 3°, les services qui sont utilisés exclusivement par un seul détenteur de données pour lui permettre d'utiliser les données qu'il détient ou qui sont utilisés par des personnes morales multiples au sein d'un groupe fermé, y compris dans le cadre de relation de fournisseurs ou de clients ou de collaborations établies par contrat en particulier ceux qui ont pour principal objectif de garantir les fonctionnalités d'objets et de dispositifs connectés à l'« internet des objets » ; 4°, les services pour le partage de données proposés par des organismes publics qui ne cherchent pas à établir de relations commerciales.

Sont incluses dans cette catégorie toutes les plateformes qui proposent un écosystème de partage de données agricoles avec d'un côté les détenteurs de données, c'est-à-dire les personnes morales ou physiques qui ont le droit d'octroyer l'accès à certaines catégories de données à caractère personnel ou non personnel[1350] et, d'autre part, les utilisateurs de données,

---

[1347] Règlement sur la gouvernance des données, préc., art. 2, 10°.
[1348] *Ibid.*, art. 4
[1349] « *Un service qui vise à établir des relations commerciales à des fins de partage de données entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et d'utilisateurs de données, d'autre part, par des moyens techniques, juridiques ou autres, y compris aux fins de l'exercice des droits des personnes concernées en ce qui concerne les données à caractère personnel* ».
[1350] Règlement sur la gouvernance des données, préc., art. 2, 8).

c'est-à-dire, les personnes physiques ou morales qui disposent d'un accès licite à certaines données à caractère personnel ou non personnel et qui ont le droit d'utiliser ces données à des fins commerciales ou non commerciales. En revanche, les plateformes qui mettent à disposition des données afin de garantir les fonctionnalités d'objets connectés et de dispositifs connectés à l'IOT, tel que le proposent les sociétés ITK ou encore SMAG, ne sont pas soumises à cette réglementation. Aussi, certains prestataires d'intermédiation de données sont soumis à cette réglementation en raison du fait qu'ils servent d'intermédiation entre les détenteurs de données et les utilisateurs. À cette fin, ils mettent à disposition des moyens techniques ou autres qui sont nécessaires pour la fourniture de ces services[1351]. Mais aussi, sont soumis à cette réglementation les services d'intermédiation entre les personnes qui cherchent à mettre à disposition leurs données à caractère personnel ou des données à caractère non personnel et les utilisateurs de données potentiels.

490- **Encadrement de l'activité des prestataires d'intermédiation de données.** Tous ces services d'intermédiation sont soumis à une procédure de notification et doivent répondre à de nombreuses conditions. En effet, ces prestataires de services sont soumis à des règles de neutralité et de loyauté afin de renforcer la confiance des acteurs du secteur. Ils doivent utiliser les données seulement à des fins de mise à disposition des utilisateurs, répondre à des conditions en matière de sécurité, d'interopérabilité, de modalités commerciales, etc.[1352] Ils doivent également notifier leur activité à l'autorité compétente qui délivre une déclaration standardisée confirmant que le prestataire a soumis la notification et qu'elle est dûment complétée. Grâce à cette déclaration, l'autorité donne le droit au prestataire de fournir le service qui peut également obtenir le label de prestataire de service d'intermédiation de données reconnu dans l'Union européenne. Ces règles ne s'appliquent néanmoins pas aux organisations altruistes en matière de données reconnues ni aux entités sans but lucratif puisque leurs activités consistent à collecter, pour des objectifs d'intérêt général, des données mises à disposition, par des personnes physiques ou morales, sur le fondement de l'altruisme. En revanche, ces règles s'appliquent à ces organisations lorsque leur objectif est d'établir des relations commerciales entre un nombre indéterminé de personnes concernées et de détenteurs de données avec des utilisateurs de données.

[1351] Ces services peuvent comprendre des échanges bilatéraux ou multilatéraux de données ou la création de plateformes ou de bases de données permettant l'échange ou l'utilisation conjointe de données, ainsi que la mise en place d'une autre infrastructure spécifique pour l'interconnexion des détenteurs de données avec les utilisateurs de données.

[1352] Règlement sur la gouvernance des données, préc., art. 12.

491- **L'altruisme en matière de données.** Le règlement favorise également le partage de données[1353] pour des raisons purement altruistes. Il s'agit de données mises à disposition volontairement par des particuliers ou des entreprises pour le bien commun[1354]. Cette activité a pour objectif l'intérêt général. Le règlement donne plusieurs exemples de cas de partage altruiste, il peut s'agir des données concernant les soins de santé, la lutte contre le changement climatique, l'amélioration de la mobilité, la facilitation du développement, de la production et de la diffusion de statistiques officielles, l'amélioration de la prestation de services publics, l'élaboration des politiques publiques ou la recherche scientifique. Aussi, afin de favoriser ces comportements altruistes, le règlement permet aux organisations qui jouent le jeu du partage à des fins d'intérêt général de s'enregistrer volontairement en tant qu'organisation altruiste en matière de données reconnues dans l'Union européenne, aux termes de l'article 19 du règlement. L'objectif est de mettre en place un référentiel commun de données. Le fait d'obtenir la qualification d'organisation altruiste, pour les entités qui respectent volontairement un ensemble d'exigences, renforce la confiance des personnes physiques et des entreprises dans le partage des données à caractère personnel et non personnel à des fins d'intérêt général. Par ailleurs, un formulaire européen de consentement à l'altruisme doit être élaboré afin de faciliter le recueil et le retrait du consentement et doit pouvoir s'adapter à des secteurs particuliers à des fins différentes[1355]. Enfin, le comité de contrôle de la gouvernance des données doit contrôler la mise en œuvre du règlement. Pour cela, il est question de désigner un groupe d'experts, qui aura pour mission de faciliter l'émergence de bonnes pratiques par les autorités des États membres et de conseiller la Commission sur la gouvernance de la normalisation intersectorielle ainsi que sur l'élaboration de demandes stratégiques.

B. La régulation des comportements déloyaux des plateformes

492- Le législateur européen a proposé de réguler le marché numérique en offrant la possibilité de contrôler en amont les plateformes avec le plus de parts de marché dont le comportement pourrait avoir des effets sur le libre jeu de la concurrence. En effet, en présence de

[1353] *Ibid.*, art. 2. 16), définit le partage des données comme « *le partage volontaire de données fondé sur le consentement donné par les personnes concernées au traitement de données à caractère personnel les concernant, ou l'autorisation accordée par des détenteurs de données pour l'utilisation de leurs données à caractère non personnel sans demander ni recevoir de contrepartie qui aille au-delà de la compensation des coûts qu'ils supportent lorsqu'ils mettent à disposition leurs données, pour des objectifs d'intérêt général prévus par le droit national* ».
[1354] *Ibid.*
[1355] *Ibid.*, art. 25.

comportements anticoncurrentiels lors du partage des données (**1**), le législateur propose de réguler les comportements déloyaux (**2**). Néanmoins, des solutions sont envisageables afin d'organiser le partage des données dans le secteur agricole (**3**).

1. Les comportements anticoncurrentiels des entreprises lors du partage des données

493- **Définition de l'entente anticoncurrentielle.** Tout d'abord, la question se pose de savoir si le partage de données agricoles peut constituer une entente anticoncurrentielle au titre des articles 101 § 1 du TFUE et L. 420-1 du Code de commerce. En effet, la pratique concertée se définit comme « *une forme de coordination entre entreprises qui, sans avoir été poussée jusqu'à la réalisation d'une convention proprement dite, substitue sciemment une coopération pratique entre elles aux risques de la concurrence* »[1356].

494- **Caractérisation de l'entente anticoncurrentielle**. À ce sujet, l'Autorité de la concurrence a déjà eu l'occasion de reconnaître que des échanges d'informations dans le secteur agricole pouvaient constituer un objet anticoncurrentiel[1357]. En revanche, les organisations interprofessionnelles peuvent « *diffuser des données statistiques portant sur les données passées, anonymisées et suffisamment agrégées* »[1358] sans que cela porte atteinte au libre jeu de la concurrence. Aussi, selon Mme la professeure A.-S. Choné-Grimaldi, il existe un faisceau d'indices pour identifier une atteinte à la concurrence. D'abord, il faut distinguer selon l'objet des données, ainsi, il est présumé que l'échange de données dans le cadre de la recherche scientifique « *ne semble pas susceptible de créer une restriction de concurrence, contrairement à l'échange d'informations commerciales* »[1359]. Ensuite, il existe moins de risque collusoire à partager des données portant sur le passé que celles portant sur l'avenir[1360]. Enfin, les données personnelles ont « *un caractère stratégique plus fort qui peut rendre [leur] diffusion anticoncurrentielle* »[1361].

495- **Caractérisation d'une entente anticoncurrentielle dans le secteur agricole.** En outre, le partage de données agricoles sur une plateforme telle qu'API-AGRO, intéressant des

---

[1356] CJCE, 14 juill. 1972, aff. C-48/ 69, *Imperial Chemical Industries.*

[1357] Aut. conc., Rapport annuel 2012, 20 mars 2013, p. 134 : « *Tout échange d'informations stratégiques, confidentielles, récentes et insuffisamment désagrégées, qui n'ont pas un caractère public et ne peuvent pas être obtenues par les entreprises autrement que par l'échange, est susceptible d'avoir un effet restrictif sur la concurrence* ».

[1358] Aut. conc., avis n°18-A-04, 3 mai 2018, relatif au secteur agricole, pt 191 et s.

[1359] CHONE-GRIMALDI, S., « Données agricoles et droit de la concurrence », *op. cit.* ; Aut. conc., note n°7, p. 135.

[1360] Aut. conc., Rapport annuel 2012, *op. cit.*, note n°1, p. 135.

[1361] CHONE-GRIMALDI, S., « Données agricoles et droit de la concurrence », *op. cit.* ; Aut. conc., *ibid.*, n°1, p. 135.

informations commerciales portant sur l'avenir peut constituer une entente anticoncurrentielle. D'autant plus, lorsque ces informations ont un caractère personnel. Ce constat est renforcé par le fait que la plateforme API-AGRO réunit l'ensemble des opérateurs économiques de toutes les filières agricoles. Ce conglomérat caractérise l'entente et empêche l'obtention d'une dérogation par le règlement portant Organisation commune des marchés (OCM)[1362]. Néanmoins, une pratique peut être exemptée au titre de l'article 101 § 3 du TFUE si la pratique concertée « *contribue à améliorer la production ou la distribution des produits ou à promouvoir le progrès technique ou économique, tout en réservant aux utilisateurs une partie équitable des profits qui en résulte* ». Mais, pour cela, la pratique ne doit pas imposer de restrictions aux entreprises qui ne sont pas indispensables pour atteindre ces objectifs et il ne doit pas en résulter une élimination totale de la concurrence sur le marché. Or, dans la mesure où l'échange des données agricoles a pour objectif de favoriser la compétitivité et d'assurer une meilleure utilisation des ressources et un meilleur rendement, l'obtention d'une exemption paraît possible[1363]. Néanmoins, le contrôle de licéité a lieu *a posteriori*, ce système n'offre donc pas une sécurité juridique optimale. Ainsi, Mme la professeure A.-S. Choné-Grimaldi préconise de modifier le règlement OCM afin d'intégrer une nouvelle exemption à l'applicabilité de l'article 101 du TFUE. Enfin, il faut noter que le portail de données pourrait être qualifié de ressources essentielles[1364] auquel cas, il devra être accessible à tous, ce qui est néanmoins déjà prévu par API-AGRO, parfois avec des conditions financières.

Il semble alors que certaines plateformes peuvent avoir un fort pouvoir de marché et créer une distorsion de la concurrence. Par exemple, des entreprises privées signent des accords pour rendre interopérables leurs outils numériques, à l'image des sociétés Bayer et Horsch[1365]. L'accord qu'elles ont conclu permet désormais de connecter la plateforme de Bayer aux semoirs et planteurs de la société Horsch. Cet accord pourrait constituer une concentration limitant de fait la concurrence.

[1362] *Ibid.*
[1363] *Ibid.*
[1364] Voir *supra*, n°207 et s.
[1365]https://www.tradingsat.com/actualites/informations-societes/bayer-accord-avec-horsch-sur-l-agriculture-numerique-952131.html

2. Le Digital Markets Act

496. La Commission européenne a proposé l'adoption de deux règlements afin de réguler les plateformes dans l'espace économique européen au travers le *Digital Markets Act*[1366] (DMA) et le *Digital Service Act*[1367] (DSA) le 15 décembre 2020 afin de remplacer la directive Commerce électronique du 8 juin 2000[1368] et compléter le Règlement P2B[1369]. Ces deux règlements ont vocation à passer de modèles de régulation sectorielle et d'un régime de sanctions *ex post* à une régulation globale *ex ante*[1370]. Le DSA établit les obligations des fournisseurs de services intermédiaires et leur responsabilité[1371]. Il porte sur le contrôle des contenus illégaux diffusés sur les plateformes ainsi que sur la désinformation. Les plateformes agricoles n'ont pas pour objet de diffuser des contenus illicites, c'est-à-dire, des contenus haineux par exemple ou de la désinformation. Par conséquent, ce règlement est hors propos s'agissant des plateformes diffusant des données au bénéfice du secteur agricole.

497. La législation sur les marchés numériques[1372] instaurant le DMA a été adoptée le 5 juillet 2022 par le Parlement européen et approuvé par le Conseil de l'Union européenne le 18 juillet 2022. Il doit entrer en application en 2023. Ce nouveau règlement a pour objectif de prévenir les pratiques particulièrement déloyales ou préjudiciables sur la concurrence des contrôleurs d'accès ou « *gatekeepers* », c'est-à-dire des plateformes qui ont un pouvoir de marché tel que leur position leur permet de contrôler un écosystème entier dans l'économie numérique, en raison de l'APIsation des entreprises[1373]. Cette APIsation consiste en un large développement d'interfaces d'échanges de données (API) qui permettent l'accès aux données et aux services d'un tiers ainsi que d'échanger des données entre des applications externes. Ainsi, ces plateformes sont des « *services de plateforme de base* », elles ont le pouvoir de bloquer la concurrence à l'accès au marché, c'est pourquoi elles sont nommées contrôleuses d'accès. Les « *services de plateformes de base* » comprennent les services d'intermédiation en ligne (comme

---

[1366] Proposition de règlement du parlement européen et du conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques), COM (2020) 842 final du 15 déc. 2020.
[1367] Proposition de règlement relatif à un marché intérieur des services numériques et modifiant la directive 2000/31/CE, COM (2020) 825 final.
[1368] Dir. n°2000/31/CE 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 : *JOUE* L 178 du 17 juill. 2000.
[1369] Règl. n°2019/1150 du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne : *JOUE* L 186/57 du 11 juill. 2019.
[1370] FAVRO, K. et ZOLYNSKI, C., « DSA, DMA : l'Europe encore au milieu du gué », *Dalloz IP/IT*, 2021, p. 217.
[1371] *Ibid.*
[1372] Résolution législative du Parlement européen du 5 juillet 2022 sur la proposition de règlement du Parlement européen et du Conseil relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques) (COM [2020] 0842 – C9-0419/2020 – 2020/0374 [COD]).
[1373] BERTRAND B., « Le modèle européen de partage des données », *Europe* n°2, févr. 2021, ét. 1.

les marchés, les magasins d'applications et les services d'intermédiation en ligne dans d'autres secteurs, comme la mobilité, les transports ou l'énergie), les moteurs de recherche en ligne, les réseaux sociaux et les services en nuage, etc. Cette nouvelle réglementation vise donc « *à agir a priori sur le comportement des gatekeepers tant sur les sources de leur pouvoir de marché, essentiellement tiré des données, que pour lutter contre les effets de réseau […]* »[1374].

Pour être qualifié de contrôleur d'accès, il existe plusieurs critères qualitatifs ou quantitatifs. Trois critères cumulatifs permettent d'établir cette qualité. Premièrement, la société doit être d'une taille telle qu'elle a une incidence sur le marché intérieur. Cette taille est présumée atteinte si la société a réalisé un chiffre d'affaires annuel dans l'espace économique européen d'au moins 7,5 milliards d'euros au cours des trois derniers exercices ou si sa capitalisation boursière moyenne ou sa juste valeur marchande équivalente s'est élevée au moins à 75 milliards d'euros au cours du dernier exercice et qu'elle fournit un service de plateforme essentiel dans au moins trois États membres. Deuxièmement, la société doit exploiter un service de plateforme essentiel qui constitue un point d'accès important des entreprises utilisatrices pour atteindre les consommateurs finaux. Cette condition est présumée remplie si la société exploite un service de plateforme essentielle comptant plus de 45 milliards d'utilisateurs finaux actifs chaque mois établis ou situés dans l'Union européenne et une moyenne de plus de 10 000 entreprises utilisatrices actives également établies dans l'Union européenne au cours du dernier exercice. Enfin, la société doit occuper une position dont on s'attend à ce qu'elle soit bien ancrée et durable, ce qui est présumé si la société a rempli les deux autres critères au cours de chacun des trois derniers exercices. Le Règlement prévoit ainsi que ces sociétés devront, par exemple[1375], permettre à des tiers d'interagir avec leurs propres services, dans des situations spécifiques, mais aussi, permettre aux entreprises utilisatrices d'accéder aux données générées par leurs activités sur leur plateforme, enfin, autoriser les entreprises utilisatrices à promouvoir leur offre et à conclure des contrats avec leurs clients en dehors de la plateforme. En revanche, elles ne pourront plus[1376], empêcher les consommateurs d'accéder aux services d'entreprises en dehors de leur plateforme, empêcher les utilisateurs de désinstaller des logiciels ou des applications préinstallés s'ils le souhaitent, croiser les données personnelles des utilisateurs avec celles d'autres de leurs services sans leur consentement, etc.

[1374] FAVRO, K. et ZOLYNSKI, C., « DSA, DMA : l'Europe encore au milieu du gué », *op. cit.*
[1375]https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets.fr
[1376] *Ibid.*

Ainsi, les contrôleurs d'accès sont des entreprises qui peuvent contrôler l'accès aux marchés numériques, en profitant de leur position de force sur chaque marché afin d'empêcher toute concurrence d'émerger. Ils peuvent également imposer leurs conditions aux entreprises et aux utilisateurs finaux de leurs services. La question se pose de savoir si des sociétés interfilières telles qu'API-AGRO qui ont vocation à regrouper l'ensemble des données d'un secteur, en l'occurrence du secteur agricole pourraient être qualifiées de contrôleuses d'accès. Néanmoins, en réalité, seulement les géants d'internet, c'est-à-dire, les GAFAM[1377] et les BATX[1378], répondent, pour l'heure, aux conditions de qualification de contrôleurs d'accès. La société API-AGRO a déclaré un chiffre d'affaires de 41 700 euros pour l'année 2020, ce qui est très loin des 7,5 milliards d'euros exigés, et ne compte pour le moment que 1200 utilisateurs inscrits en avril 2022[1379], ce qui est une fois encore très éloigné des 45 millions d'utilisateurs finaux actifs exigés par le règlement. Aucune société de l'agriculture numérique ne correspond donc pour l'heure à ces critères.

3. Solutions envisageables pour l'organisation du partage des données agricoles

498- **Solutions opérationnelles envisageables.** Le droit doit organiser la maîtrise et le partage des données afin de permettre leur réutilisation. L'objectif étant de remplacer le puzzle de droits par un véritable encadrement juridique des données non personnelles dont le but est de faciliter leur partage et leur réutilisation. À ce titre, plusieurs propositions ont été faites. D'abord, M. J. Wainstain propose de mettre en place sur le modèle des *Smart territories* des « *plateforme(s) digitale(s) locales mettant en réseau les acteurs économiques des filières alimentaires, quel que soient leur taille et leur position dans la chaîne de valeur* »[1380]. Il s'agit donc d'organiser une gouvernance technologique en déterminant une « *entité qui serait garante du partage des données* »[1381]. Dans un tel cas, les collectivités territoriales serviraient de « *tiers de confiance, [de] cofinanceurs et [d']acteurs de régulation* »[1382]. Ensuite, la Commission européenne, dans sa Stratégie européenne pour les données, a émis le souhait de créer des espaces communs de données à travers une plateforme neutre[1383] pour améliorer la qualité des

[1377] Google, Apple, Facebook, Amazon, Microsoft
[1378] Baidu, Alibaba, Tencent, Xiaomi
[1379] BIARD, V., « partage de données agricoles, les applications montent en puissance en France », avr. 2022, https://www.larevuedudigital.com/partage-de-donnees-agricoles-les-premieres-applications-en-france/
[1380] WAINSTAIN, J., « Partager les données pour réussir les transitions agricoles et alimentaires », *op. cit*.
[1381] *Ibid*.
[1382] *Ibid*.
[1383] Une stratégie européenne pour les données, préc.

services dans l'agriculture[1384]. C'est pour cela que la Commission encourage des projets comme celui de Gaia-X qui pourrait, en outre, répondre à la problématique de la gouvernance numérique[1385]. Ce projet porté par les gouvernements allemand et français depuis mai 2020 consiste en « *un écosystème numérique ouvert dans lequel les données peuvent être mises à disposition, rassemblées et partagées en toute sécurité et en toute confiance, selon un certain nombre de standards techniques et de règles d'interopérabilité* »[1386]. Il permet de créer « *une identité numérique* » pour « *toutes les exploitations agricoles* » afin d'assurer « *la sécurité des échanges dématérialisés* »[1387]. Le projet Gaia-X permet également de créer « *une plateforme d'échange, c'est-à-dire des espaces de stockage sécurisés dédiés aux données sensibles* »[1388], ainsi que d'assurer l'interopérabilité technique des données.

Dans le cadre du partage des données dans un objectif purement altruiste, peut-être serait-il envisageable de créer une plateforme mixte sur les modèles d'Agrirouter et d'API-AGRO. Cette plateforme proposerait à la fois le stockage de données et la circulation de certains jeux de données, sans stockage. Ainsi, les détenteurs de données auraient la possibilité d'exposer les catégories de données qu'ils détiennent sans pour autant les transférer sur la plateforme. De fait, un catalogue se constituerait et le partage de chaque jeu de données pourrait être revêtu de conditions de finalité, d'usage et de partage choisies au préalable par le détenteur des données. Les utilisateurs tiers qui souhaiteraient obtenir les données pourraient alors en faire la demande et devraient se soumettre aux modalités d'échanges prévues par le détenteur des données. Ainsi, ce dernier conserverait la pleine maîtrise des données qu'il détient et ce partage pourrait alors reposer sur des licences d'échange de données personnalisées, comme le propose déjà API-AGRO. Chaque personne dans la chaîne de valeur devrait ainsi pouvoir exploiter les données selon ses besoins sans pouvoir outrepasser ses droits[1389].

499. **Conclusion de la section.** Les données agricoles privées ne font pas l'objet, pour l'heure, d'un régime particulier s'agissant de la maîtrise de leurs usages. Aussi, seule la réservation de l'accès permet de contrôler l'usage qui peut en être fait par ceux qui sont autorisés à y avoir accès.

[1384] https://www.euractiv.fr/section/avenir-de-l-ue/news/leak-eu-plans-common-data-spaces-to-exploit-agriculture-and-health-potential/

[1385] Voir *supra*, n°283.

[1386] PICARDAT, S., « GAIA-X : L'agriculture au cœur de la souveraineté numérique européenne », in ABIS, S. et BRUN, M., ss. dir., *Le Démeter 2021, Produire et se nourrir : le défi quotidien d'un monde déboussolé*, IRIS éd., févr. 2021, p. 205.

[1387] *Ibid.*

[1388] *Ibid.*

[1389] ROBIN, A., « Agriculture numérique, données et droit : topographie juridique de l'"écosystème informationnel vert" », *op. cit.*

Pourtant, la régulation de la réutilisation et du partage des données est une problématique majeure dans le secteur agricole puisque la valorisation des données passe par leur circulation. Or, le constat est qu'aujourd'hui, les données agricoles sont très peu partagées et donc très peu réutilisées, en raison d'un défaut de cadre juridique et d'un manque de standards communs. Des propositions ont été faites en ce sens et devraient, aujourd'hui, être menées à bien.

500- **Conclusion du chapitre.** Si les données agricoles publiques sont libres de réutilisation, ce n'est pas le cas de la grande majorité des données privées. Aussi, ce sont les détenteurs des données privées, c'est-à-dire, en général, les entreprises de l'*AgTech*, qui en contrôlent l'accès et en définissent les usages au moyen de la technique et du contrat. C'est également eux qui empêchent leur partage et leur réutilisation. Le générateur de la donnée, c'est-à-dire, l'agriculteur, quant à lui, ne dispose, pour l'heure, d'aucun droit de contrôle sur l'usage des données issues de son exploitation. Pourtant, cette question est fondamentale afin d'assurer leur protection.

Chapitre 2. Le développement du contrôle de l'usage des données non personnelles d'exploitation par l'agriculteur

501- Le silence de la loi sur le contrôle de l'usage des données elles-mêmes est tout à fait remarquable (**Section 1**). Aussi, afin de combler ce vide légal, les acteurs du secteur de l'agriculture numérique ont proposé des solutions, qui s'avèrent toutefois limitées, pour protéger l'exploitant agricole et lui offrir les outils de contrôle de l'usage des données non personnelles de son exploitation (**Section 2**).

Section 1. Le silence de la loi sur le contrôle de l'usage des données d'exploitation

502- Pour l'heure, il n'existe aucun dispositif légal permettant de contrôler l'usage des données d'exploitation (**§1**). Le portage des données développé par le législateur européen dans le règlement sur la circulation des données non personnelles s'avère inefficient et ne permet pas de contrôler l'usage des données (**§2**).

§1. *L'absence de dispositif légal de contrôle de l'usage des données d'exploitation*

503- Le statut des données d'exploitation est complexe à déterminer. L'étude du droit de propriété, qui est un droit attaché au corpus, conduit à conclure à son inadaptation à une chose incorporelle par nature telle que les données (**I**). Pour autant, la propriété intellectuelle qui a vocation à protéger l'incorporel ne parvient pas, non plus, à les appréhender tout à fait (**II**).

I. L'inadaptation du droit de propriété aux données d'exploitation

504- Seuls les biens peuvent faire l'objet d'un droit de propriété. Cette catégorie, malléable et extensible, intègre un très grand nombre de choses (**A**). Néanmoins, les données ont des caractéristiques dont l'étude doit mener à la conclusion qu'elles doivent être définitivement exclues de cette catégorie (**B**).

A. Le principe de l'appropriation des biens

505.- Afin d'étudier l'appropriabilité des données, il convient, dans un premier temps, d'envisager les caractéristiques du droit de propriété (**1**) pour, dans un second temps, s'intéresser à la catégorie extensible et malléable des biens (**2**).

1. Les caractéristiques du droit de propriété

506.- Droit absolu et exclusif. La propriété a été érigée en droit absolu dès la Révolution française. Demolombe affirmait que « *la propriété est évidemment le premier et le plus complet des droits réels ; c'est le droit réel par excellence* »[1390]. Nul autre droit ne surpasse le droit de propriété qui est lié à la notion de liberté comme se sont évertués à le démontrer de grands philosophes tels que Hobbes, Rousseau ou encore Kant. C'est d'ailleurs, l'un des trois piliers de notre système juridique[1391]. La preuve du caractère primordial de ce droit repose dans son absolutisme et son exclusivisme pour les personnes qui en sont titulaires. Le droit de propriété est régi par l'article 544 du Code civil qui le définit comme le « *droit de jouir et de disposer des choses de la manière la plus absolue, pourvu qu'on n'en fasse pas un usage prohibé par les lois ou les règlements* ». Il est donc question d'un droit réel — la *traditio* de la Rome antique — qui permet aux personnes d'exercer un pouvoir direct et exclusif sur une chose.

507.- Éléments constitutifs. Le droit de propriété se décompose en trois éléments constitutifs que sont l'*usus* ou le droit d'usage, le *fructus* ou le droit de percevoir les revenus sur le bien et l'*abusus* ou le droit de disposer de la chose comme le propriétaire l'entend. Pour qu'une chose soit appropriable, elle doit être, en principe, tangible, c'est-à-dire, avoir « *une existence matérielle propre et susceptible d'être objet de droit* »[1392], autrement dit, être un bien. Le caractère tangible d'un bien permet au possesseur d'avoir « *les pouvoirs d'en disposer et d'en exclure les autres* »[1393]. Selon M. le Professeur J. Carbonnier « *toutes choses ne sont pas des biens. C'est qu'il faut une possibilité d'appropriation pour faire un bien d'une chose* »[1394].

[1390] DEMOLOMBE C., *Traité de la distinction des personnes et des biens*, in DEMOLOMBE, C., Cours de Code Napoléon, t. IX, Paris, Durand, 1870, n°471, p. 352.
[1391] CHARDEAUX, M.-A., *Les choses communes*, *op. cit*., p. 4.
[1392] CABRILLAC, R. et Alii., *Dictionnaire du vocabulaire juridique*, J.-Cl., 2002.
[1393] BENABOU, V.-L. et ROCHFELD, J., *À qui profite le clic ?, op. cit.,* p. 47.
[1394] CARBONNIER, J., *Droit civil, Les biens, les obligations*, PUF, 2017, p. 1595.

2. La catégorie extensible et malléable des biens

508- Absence de définition. Les biens ne sont pas définis par le Code civil « *partant implicitement de ce que toute chose est bien, [le Code civil] se contente de définir les critères de répartition des biens entre meubles et immeubles* »[1395]. La liste des choses qui entrent dans la catégorie des biens n'est donc pas figée, elle évolue selon les besoins et les attentes de la société.

509- Doctrine. Une partie de la doctrine[1396] retient une conception utilitariste des biens, il s'agirait de toutes choses utiles à l'Homme. Portalis écrivait à ce sujet que « *les choses ne seraient rien pour le législateur sans l'utilité qu'en tirent les Hommes* ». De manière alternative, certains auteurs ont préféré retenir la notion d'utilité économique[1397], les biens seraient avant tout monnayables, ils auraient une valeur vénale, appréciable et quantifiable en argent. Deux autres critères sont également pris en compte pour savoir si une chose peut entrer dans la catégorie des biens, il s'agit de son appropriation et de sa saisissabilité. En effet, pour qu'une chose soit considérée comme un bien, elle doit être objet de désir, évaluable selon son utilité ou sa rareté et surtout appropriable[1398]. Un rapport d'exclusivité doit exister entre le propriétaire et la chose vis-à-vis des tiers. D'ailleurs, certains auteurs, comme Mme M.-A. Chardeaux, retiennent comme unique critère de distinction entre la chose et le bien, l'*appropriabilité*[1399]. La chose doit en outre participer au commerce[1400]. Pour certains, elle doit pouvoir circuler, être transmissible et aliénable, et tout cela de manière licite[1401].

510- Catégorie extensible et malléable. Il apparaît que la catégorie des biens est une catégorie qui n'est pas tout à fait fixée par la doctrine et qu'une quantité de conditions peuvent intervenir pour faire entrer, de force, une chose dans la catégorie des biens. De plus, il faut noter que

---

[1395] PERINET-MARQUET, H., « Regard sur les nouveaux biens », *JCP G*, n°44, 2010, p. 2071.

[1396] ZENATI-CASTAING, F. et REVET T., *Les biens*, 3e éd., PUF, 2008, n°2, p. 18 « *dont l'utilité justifie l'appropriation* » ; ATIAS, C., *Droit civil, Les biens*, 11e éd., Litec, 2011, n°1, p. 1 reprenant la définition de BAUDRY LACANTANERIE, *Traité théorique et pratique de droit civil, Les biens*, Paris, 1e éd., 1896, n°10, p. 10 « *toutes choses qui pouvant procurer à l'homme une certaine utilité sont susceptibles d'appropriation* », *in* REBOUL-MAUPIN, N., *Droit des biens*, 5e éd., Dalloz, 2014, p. 9 ; TERRE F. et SIMLER P., *Droit civil, Les biens*, 9e éd., Dalloz, 2014, n°26, p. 34.

[1397] REBOUL-MAUPIN, N., *Droit des biens*, *op. cit.*, p. 20 ; BERLIOZ, P., *La notion de bien*, LGDJ, 2007, t. 489, n°1708 ; PIEDELIEVRE, A., *Le matériel et l'immatériel, essai d'approche de la notion de bien*, Mélanges M. de JUGLART, LGDJ, 1986, p. 57, « *la notion de valeur est essentielle, toute valeur doit être considérée comme un bien* » ; MIGNOT, V., *La notion de bien - contribution à l'étude du rapport entre droit et économie*, *RRJ*, 2006-4 (I), p. 1805.

[1398] ZENATI-CASTAING, F. et REVET, T, *Les biens*, 3e éd., PUF, 2008, n°2.

[1399] CHARDEAUX, M.-A., *Les choses communes*, Quadrige, LGDJ, 2006, n°68, p. 74 : « *Tandis que la chose est un terme générique qui permet de désigner toutes formes d'entités existantes appréhendées par le droit, le terme bien accomplit la même fonction au regard des entités appropriables, qu'elles soient corporelles ou incorporelles* ».

[1400] ZENATI-CASTAING, F. et REVET, T., *Les biens*, 3e éd., 2008, PUF, n°2, p. 18.

[1401] MATTATIA, F. et YAICHE, M., « Être propriétaire de ses données personnelles (1ère partie) : peut-on recourir aux régimes traditionnels de propriété ? », *RLDI*, 2015/114 ; pp. 60 à 63.

l'autorité publique dispose d'un pouvoir d'inclusion ou d'exclusion de la liste des biens[1402]. Par exemple, les quotas de gaz à effet de serre[1403] ont été inclus dans cette catégorie[1404] alors qu'il ne s'agit que d'une simple autorisation d'émettre des gaz à effet de serre ne répondant pas aux conditions d'appropriabilité au sens du Code civil. Au contraire, les stupéfiants, qui répondent eux aux conditions, puisqu'il s'agit d'une chose matérielle appropriable, en ont été exclus[1405].

511- **Appropriation des informations.** Comme exposé plus haut[1406], une chose a fait l'objet de grands débats doctrinaux, il s'agit des *informations*. Si pour une partie de la doctrine dont M. le Professeur P. Catala est l'instigateur, l'information avait une valeur et peut de fait faire l'objet d'un droit de propriété[1407], la doctrine majoritaire considère, tout au contraire, qu'il ne peut pas y avoir de droit de propriété sur l'information et qu'elle doit être de surcroît exclue de la catégorie des biens[1408]. Certaines exceptions sont néanmoins relevées. M. le Professeur H. Périnet-Marquet précise, en effet, « *[qu'] une information construite, tel le classement de Shanghai, ou la note mise aux États par les agences de notation, qui découle du travail de l'Homme, est un bien parce qu'elle est un produit, pour reprendre la distinction particulièrement pertinente faite par certains auteurs* »[1409]. Ce qui ne serait pas le cas, notamment, pour les informations brutes. C'est d'ailleurs ce qu'avance Mme la Professeure M. Clément-Fontaine, en spécifiant qu'un « *consensus a été trouvé pour considérer que l'information dans sa forme brute devait demeurer libre de réservation* »[1410].

[1402] PERINET-MARQUET, H., « Regard sur les nouveaux biens », *op. cit.,* p. 2073.

[1403] Le quota étant défini comme ce qui permet d'autoriser « *à émettre une tonne d'équivalent-dioxyde de carbone en cours d'une période spécifiée, valable uniquement pour respecter les exigences de la présente directive, et transférable conformément aux dispositions de la présente directive* » ; Dir. n°2003/87/CE du 13 oct. 2003 établissant un système d'échange de quotas d'émission de gaz à effet de serre dans la communauté et modifiant la directive 96/61/CE du conseil : *JOUE* L 275/32 du 25 oct. 2003, art. 3, a).

[1404] C. env., art. L. 229-1, al. 1. : « *Les quotas d'émission de gaz à effet de serre sont des biens meubles exclusivement matérialisés par une inscription au compte de leur détenteur dans le registre mentionné à l'article L. 229-12. Ils sont négociables, transmissibles par virement de compte à compte et confèrent des droits identiques à leurs détenteurs. Ils peuvent être cédés dès leur délivrance sous réserve des dispositions des articles L. 229-8 et L. 229-10 et des dispositions des actes délégués pris en application de l'article 19 de la directive 2003/87/CE du 13 octobre 2003* ».

[1405] Les stupéfiants sont des substances dangereuses dont l'usage est contraire à l'ordre public au sens de l'article L. 3421-1 du Code de la santé publique.

[1406] Voir *supra*, n°18 et s.

[1407] CATALA, P., *La propriété de l'information, op. cit.,* p. 97.

[1408] DARAGON, E., « Étude sur le statut juridique de l'information », *op. cit* : « *… l'information ne se confond pas avec le message, l'idée, la donnée, ou la connaissance, même si elle intervient d'une manière ou d'une autre dans leur définition* ».

[1409] PERINET-MARQUET, H., *Regard sur les nouveaux biens*, JCP G, n°44, 2010, p. 2073 ; voir égal., ZENATI-CASTAING, F. et REVET, T., *Les biens,* 3e éd., PUF, 2009, note (1), n°8.

[1410] CLEMENT-FONTAINE, M., « communs numériques (approche juridique) », in CORNU, M., ORSI, J. et ROCHFELD, J., ss. dir., *Dictionnaire des biens communs, op. cit.*, pp. 311 à 314, spéc. p. 312 : « *Lorsque la question de l'appropriation de l'information a été posée notamment par le professeur Catala, un large consensus s'est dégagé pour considérer que seule l'information dans sa forme brute devait demeurer libre de réservation. De plus le législateur en accordant un droit sui generis aux producteurs de bases de données, qui interdit aux tiers de procéder à l'extraction quantitative ou qualitative du contenu, a permis la réservation de l'information brute, des*

B. L'exclusion des données de la catégorie des biens

512- Plusieurs raisons justifient une exclusion des données de la catégorie des biens. D'abord, les données sont non rivales et reproductibles empêchant toute forme d'appropriation (**1**). Ensuite, elles n'ont pas de valeur intrinsèque (**2**).

1. Les caractères non rival et reproductible des données

513- Exclusion de la catégorie des biens. Les données n'entrent pas dans la catégorie des biens compte tenu de leur nature non rivale et reproductible. Les économistes distinguent les différentes catégories de biens (biens privés, biens clubs, biens publics ou communs de ressources) selon leur caractère rival et excluable[1411]. Les biens rivaux sont des « *ressources limitées dont la possession et l'utilisation par un individu empêchent ou restreignent sa possession ou son utilisation par d'autres (toute ressource naturelle non régénérable par exemple). À l'inverse, les biens non rivaux sont des biens qui peuvent être possédés et utilisés par tout un chacun sans que cela influe sur leur possession et/ou leur utilisation par d'autres (exemple des connaissances scientifiques)* »[1412]. Les économistes distinguent également selon que le bien est exclusif ou non exclusif : « *les biens exclusifs sont des biens qui peuvent être accaparés par une personne et dont l'accès peut être alors restreint ou interdit aux autres. À l'inverse, les biens non exclusifs sont les biens dont l'accès ne peut être interdit ou restreint facilement par un individu ou un groupe (exemple de la lumière d'un phare, qu'on ne peut limiter par exemple à ceux qui auraient payé pour)* »[1413]. Ainsi, les économistes considèrent les données comme un bien non-rival, ce qui signifie qu'elles peuvent être utilisées par plusieurs personnes en même temps sans que cela affecte l'usage des autres puisqu'elles peuvent être reproduites à l'infini et leurs caractéristiques limitent les possibilités de réservation. Par conséquent, le fait de détenir une donnée n'empêche pas une autre personne de la détenir et de l'exploiter également, de la même manière que l'information. De plus, la confidentialité ne peut être à l'origine d'un droit de propriété[1414]. Il serait également très difficile d'admettre un droit

---

œuvres tombées dans le domaine public (Mallet-Poujol, 1996) et plus récemment des données publiques » ; CAA de Bordeaux, 4e ch., 26 févr. 2015, *Notrefamille.com* c/ *Département de la Vienne*.

[1411] CORIAT, B., ss. dir., *Le retour des communs, la crise de l'idéologie propriétaire*, LLL, 2015, pp. 74 et s ; BENABOU, V.-L. et ROCHFELD, J., *À qui profite le clic ?, op. cit*., p. 49.

[1412] MOUVEMENT UTOPIA, *Propriété et communs, Idées reçues et propositions*, préf. CORIAT B., éd. Utopia, 2017, p. 101.

[1413] *Ibid*., p. 102

[1414] ROBIN, A., « Agriculture numérique, données et droit : topographie juridique de l'"écosystème informationnel vert" », *Sciences Eaux & Territoires*, 2019, p. 40.

de suite, prérogative du propriétaire lui permettant de récupérer son bien dans quelque main qu'il soit, pour le détenteur originaire des données. Ces caractéristiques permettent d'apporter un élément justificatif au fait que les données ne sont *a priori* pas appropriables. C'est, d'ailleurs, cet argument d'inappropriabilité des données qui les distingue des choses sans maître — *res nullius* — appropriables par le premier occupant. *A contrario,* la nature des données et, pour certaines, leur destination, empêchent toute forme d'appropriation et les exclut de la catégorie des *res nullius*.

En outre, le législateur européen distingue les régimes applicables aux données à caractère personnel et aux données à caractère non personnel. Dans le premier cas, les données permettent d'identifier ou rendent identifiable une personne physique, le législateur a donc créé un régime protecteur. Ainsi, les données à caractère personnel font l'objet d'un droit spécifique à la détermination personnel pour les personnes physiques concernées. Le Conseil d'État a donc rejeté l'idée de toute appropriation de ces données dans son rapport de 2014 sur le numérique et les droits fondamentaux[1415]. Le Conseil National du Numérique estime, également, dans son avis de 2014 portant sur la neutralité des plateformes, que les données personnelles ne peuvent faire l'objet d'un droit d'exclusivité par son appropriation.

Dans le second cas, les données à caractère non personnel ne permettent pas d'identifier une personne physique. La Commission européenne a pensé, un temps, créer un nouveau droit de propriété en faveur du producteur de données[1416]. Cette idée a un temps été abandonnée parce qu'elle aurait eu notamment pour effets de surprotéger les données et de créer des problèmes de concurrence. Néanmoins, le législateur européen a proposé une nouvelle exception au droit *sui generis* à l'article 35 de la Proposition de règlement sur les données du 23 février 2022[1417].

514- Malgré ces régimes différents selon le contenu des données, il est nécessaire de rappeler qu'une donnée reste une donnée, peu importe son contenu ou son usage futur. C'est donc une chose non rivale qui empêche toute relation d'exclusivité entre une personne et une donnée. Or, le droit de propriété ne s'attache pas au contenu ou à la destination de la chose, mais seulement, *a priori,* à la chose elle-même. Par conséquent, si la donnée est inappropriable au regard de ses caractéristiques intrinsèques, il serait incohérent de créer des régimes spécifiques d'appropriation pour certaines d'entre elles, comme les données personnelles[1418] ou les données

[1415] CE, *Numérique et droits fondamentaux*, rapport pour l'année 2014, pp. 264 et s.
[1416] Voir *supra*, n°247.
[1417] *Ibid.*
[1418] DESTREGUIL, M., « Plaidoyer en faveur d'une approche propriétariste des données personnelles », *RJPF*, n°3, 1er mars 2019.

industrielles. Une telle reconnaissance ferait perdre de son intérêt au droit du producteur des bases de données. En effet, le droit des bases de données porte sur le contenu de la base qu'il s'agisse d'éléments protégés ou non[1419]. Pour autant, l'information n'est pas appropriée par cette voie puisque « *la finalité du dispositif est de défendre l'investissement qu'implique l'activité de collecte et de traitement des données contre les risques de pillage de la totalité ou d'une partie substantielle du contenu de la base* »[1420]. Or, la constitution d'une base de données n'empêche pas de se procurer l'information par d'autres sources. Ainsi, « *une information ne devient pas objet d'un monopole par cela seul qu'elle a été insérée dans une base* »[1421]. La reconnaissance d'un droit de propriété sur les données aurait donc de trop lourdes conséquences sur le droit du producteur de bases de données, le rendant inopérant. En outre, une telle proposition pourrait créer de l'insécurité juridique et des difficultés d'application. Ces difficultés résideraient notamment dans les limites de la distinction faite par le législateur entre les données personnelles et les données non personnelles[1422].

2. L'absence de valeur intrinsèque de la donnée

515- **Appropriation des données en raison de leur valeur ?** Certains auteurs ont une vision dite « réaliste »[1423] en ce qu'ils partent du postulat que l'évaluation en argent des données en font un objet de propriété[1424] ou du moins qu'il est possible pour une personne de se les approprier[1425]. En revanche, cette appropriation n'aurait pas pour conséquence pour autant d'intégrer les données dans le commerce juridique. Ce n'est pas parce qu'une chose est appropriable qu'elle doit forcément être autorisée dans le commerce. Aussi, pour des considérations d'ordre social, il serait possible d'envisager que même si les données sont des biens appropriables, personne ne pourrait en disposer[1426], comme c'est déjà le cas pour les stupéfiants.

D'autres auteurs ont évoqué l'idée de s'appuyer sur l'aspect comptable pour affirmer que des données non structurées sont des actifs incorporels de l'entreprise ayant une valeur

[1419] PASSA, J., « La propriété de l'information : un malentendu ? », *Droit et patrimoine*, n°91, 1er mars 2001.
[1420] *Ibid*.
[1421] *Ibid*.
[1422] Voir *infra*, n°683 et s.
[1423] BENABOU, V.-L. et ROCHFELD, J., *À qui profite le clic ?, op. cit*., p. 59.
[1424] BABINET, G., *L'ère numérique, Un nouvel âge de l'humanité*, Le passeur, 2014.
[1425] BENABOU, V.-L. et ROCHFELD, J., *op. cit.*
[1426] BASDEVANT, A. et MIGNARD, J.-P., *L'empire des données, Essai sur la société, les algorithmes et la loi,* Don Quichotte, 03/2018, p. 127.

économique[1427]. Ces données feraient donc l'objet d'un droit de propriété en faveur de l'entreprise qui les détient.

516- **Étude de la valeur des données.** Les propositions de la reconnaissance de l'appropriation des données incitent à s'interroger sur la question fondamentale de leur valeur. Les données sont utiles pour les entreprises qui créent grâce à elles de nouveaux services. Dans ce sens, un papier de l'Université de Cambridge relève que le *Big Data* permet la création de nouveaux modèles d'affaires en ce que les acteurs utilisent ces ressources pour créer de nouveaux services à valeur ajoutée[1428]. La production, la collecte et le traitement des données obligent les entreprises à employer du personnel, utiliser des matériels et des applications onéreux. Le travail sur les données représente alors un coût considérable pour ces entreprises. Une chaîne de valeur se crée autour de celles-ci et un marché de la donnée se met en place. Ce coût doit donc, en principe, être retranscrit sur la valeur de la donnée. Selon l'Organisation de Coopération et de Développement Économiques (OCDE), la donnée obtient une valeur qui dépend de son contexte, selon l'information qu'elle contient et de ce que l'on peut en faire[1429].

En France, les économistes L.-D. Benyayer et S. Chignard se sont intéressés à la valeur de la donnée[1430]. Pour ces auteurs, plus « *la donnée est raffinée et […] présente un certain niveau d'exclusivité* », plus elle est chère. Pour déterminer un prix, ils évoquent trois approches possibles : prendre le coût de production de la donnée, le gain des données ou utiliser le prix de marché[1431]. Plusieurs éléments permettent donc de déterminer la valeur d'une donnée : tout dépendra de son *coût de production* (créer, collecter, transporter, stocker, sécuriser, préparer, qualifier, analyser, visualiser et détruire), de son *utilité* (en la raffinant et en agglomérant un grand nombre de données), mais aussi de sa *rareté*. Ici, à la différence de nombreux biens, la donnée n'est pas rare, elle est au contraire très abondante (phénomène du *Big Data*). Ainsi, la valorisation des données se trouve dans leur agglomération. La rareté réside quant à elle dans l'accès à la source de ces données. Leur valeur est également « *coconstruite et future* », c'est dans l'usage immédiat ou futur de cette donnée que se dégagera une valeur. En principe, donc, la valeur des données est coconstruite[1432], c'est la comparaison entre elles, leur agrégation, qui leur confère une valeur. Et souvent, les entreprises conservent les données dans l'attente d'une

[1427] CYTERMANN, L., *Rapport relatif aux données d'intérêt général, op. cit.,* p. 43.
[1428] HARTMANN, P. et alii, « Big Data for big business? A taxonomy of Data-driven Business Models erseo by Start-up Firms », *Working paper, University of Cambridge*, mars 2014.
[1429] OECD, « A measurement roadmap for the future » ; in *Measuring The Digital Transformation : A Roadmap for the Future*, OECD Publishing, Paris, 2019, www.oecd.org/going-digital/measurement-roadmap.pdf, p. 8.
[1430] CHIGNARD, S. et BENYAYER, L.-D., *Datanomics, Les nouveaux business models des données*, FYP éd., 2015.
[1431] *Ibid*, p. 58.
[1432] *Ibid.*, p. 49.

utilité future, ce que l'on appelle la *valeur d'option*. Il semblerait alors qu'une donnée isolée n'ait qu'une valeur infime. C'est la circulation de la donnée qui lui confère une valeur et non pas son stockage[1433]. Mais aussi, c'est par l'analyse d'une donnée, ou plutôt d'un ensemble de données, que l'on peut dégager une information qualifiée à valeur ajoutée, « *la donnée est la cellule de base du renseignement qu'elle est susceptible de fournir après transformation* »[1434].

En économie, le caractère non rival des données aura des conséquences lors de la recherche du régime juridique qui leur est applicable. En effet, la donnée isolée ne semble pas avoir une utilité particulière, c'est bien l'agglomération d'un grand nombre de données et la possibilité de les comparer entre elles, qui la rend utile. De fait, il y a un véritable déplacement de la valeur, ce n'est pas dans la donnée elle-même que la valeur se crée, mais dans la possibilité de créer de nouveaux biens et services en partant de ces données isolées. C'est pourquoi la Commission européenne a choisi d'offrir une protection aux producteurs de bases de données. C'est, donc, le travail effectué pour agglomérer, trier et classer les données qui est récompensé et c'est seulement ce travail qui doit être protégé. Les bases de données représentent des valeurs économiques considérables[1435], mais pas les données en elles-mêmes. Néanmoins, la Commission européenne envisage dans sa proposition de règlement sur les données en date du 22 février 2022 que les données produites par des dispositifs et des objets connectés à l'internet des objets ne peuvent plus être protégées par le droit *sui generis*[1436]. En effet, ces données représentent une grande valeur, c'est pourquoi il faut favoriser leur accès et leur partage afin de limiter leur concentration dans les mains de grandes compagnies.

517. **Valeur des données de l'agriculture numérique.** Les données collectées par les machines agricoles et autres objets connectés sont des données brutes qui ne sont pas encore traitées, raffinées ou analysées. Ce sont des cellules qui contiennent une information non encore exploitée. Une fois traitées, elles portent des informations sur la pluviométrie, la composition du lait, les rendements, le suivi des animaux, etc. Ces données que l'on peut qualifier « *[d']*

1433 *Ibid.*, p. 41 : La donnée « *est disponible en quantité toujours croissante, difficile à protéger et facile à reproduire, ne s'épuise pas quand on la consomme et sa valeur réside davantage dans la circulation que dans la thésaurisation* ».

1434 MAISON ROUGE (de), O., « La donnée : Enjeu cardinal de la cybersécurité, Définition, nature, classification et extraction », *Dalloz IP/IT*, 2018, p. 170.

1435 CATALA, P., « La transformation du patrimoine dans le droit civil moderne », *RTD civ.*, n°185, 1966 ; *Id.*, « Ébauche d'une théorie juridique de l'information », *op. cit.* ; « La propriété de l'information », *op. cit.* ; BINCTIN, N., « Le statut juridique des informations non appropriées », *Légicom*, n°49, 2013/1, n°29, p. 82 ; STORRER, O., « Pour un droit commercial de l'exploitation des données à caractère personnel », *D.*, 2013, p. 1844.

1436 Commission européenne, proposition de règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données - Data Act), COM(2022)68 final, 23 févr. 2022, art. 35.

industrielles »[1437], constituent l'intrant même de l'agriculture numérique. C'est la matière première qui permet l'innovation. La valeur des données vient donc *a priori* du rassemblement et du traitement des informations afin de créer de nouveaux services[1438], l'agrégation et le croisement des informations constituent la valeur économique des données[1439]. L'agglomération d'un grand nombre de données d'exploitation permet de créer de l'aide à la décision et de prévenir les évènements, à l'image des données météorologiques. De ce fait, elles obtiennent une valeur d'actif issue du travail qui est fait sur ces données, de l'utilité qui en ressort et par la rareté des sources d'accès[1440]. Cependant, pour les économistes, le fait que les données soient coconstruites, c'est le croisement de différents jeux de données qui crée une valeur d'usage. Elles sont également futures, ce qui signifie qu'elles ne sont pas toujours exploitables à un instant « T », c'est la valeur potentielle future de ce qu'il sera possible d'en retirer qui va être prise en compte[1441]. Elles constituent donc un levier de développement important des activités agricoles. C'est par leur usage et par leur circulation que ces données vont prendre de la valeur. Par conséquent, au vu de ces éléments, les données étant non rivales, il est difficile d'établir un véritable lien de propriété entre une donnée et une personne. L'argument de la valeur des données ne semble pas pouvoir être retenu pour démontrer un éventuel droit de propriété sur elles. La valeur ne réside donc pas dans la donnée elle-même, mais dans l'accès à ses sources[1442]. Il s'agit simplement d'admettre un état de fait à un instant « T » dans le patrimoine de l'entreprise. Cette dernière détient un actif incorporel composé de données, mais en cas de diffusion, elle ne disposera pas de prérogatives sur celles-ci. Il n'existe donc pas de droit de propriété sur les données agricoles[1443].

[1437] ZOLYNSKI, C., « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », *op. cit.*
[1438] BENABOU,V.-L. et ROCHFELD, J., *À qui profite le clic ?, op. cit.*, p. 40.
[1439] BENABOU, V.-L., « L'extension du domaine de la donnée », *Légicom*, n°59, 2017/2, pp. 3 à 17.
[1440] CHIGNARD, S., BENYAYER, L.-D., *Datanomics*, *op. cit.*
[1441] *Ibid*.
[1442] ZENATI, F., *Essai sur la nature juridique de la propriété : contribution à la théorie du droit subjectif*, thèse, ss. dir. Rubellin-Devichi J., Lyon III, 1981.
[1443] ROBIN A., « Agriculture numérique, données et droit : topographie juridique de l'"écosystème informationnel vert" », *op. cit.*, p. 41.

II. La difficile appréhension des données par le droit de la propriété intellectuelle

518- La question de l'application de la propriété intellectuelle aux données suppose de s'intéresser aux données elles-mêmes et non pas aux bases de données qui ont déjà fait l'objet d'un développement plus haut[1444]. L'article L. 111-1 du CPI dispose que « *l'auteur d'une œuvre de l'esprit jouit sur cette œuvre du seul fait de sa création, d'un droit de propriété incorporelle exclusif et opposable à tous. Ce droit comporte des attributs d'ordre intellectuel et moral ainsi que des attributs d'ordre patrimonial* ». Aussi, afin d'analyser l'application du droit de la propriété intellectuelle sur les données, il faut nécessairement envisager, tout d'abord, la création de forme, c'est-à-dire les données (**A**), puis la création originale, c'est-à-dire les données traitées et analysées (**B**).

A. La création de forme : les données

519- Il convient d'envisager, dans un premier temps, les choses immatérielles susceptibles d'appropriation (**1**), pour, dans un second temps, s'interroger sur la qualification des données (**2**).

1. Les choses immatérielles

520- **Enclosure des biens immatériels.** Garrett Hardin évoquait la tragédie des communs[1445] au sujet des ressources naturelles, on assiste aujourd'hui à une tragédie des « anti-communs ». Si la « première enclosure » a porté sur le foncier[1446], la propriété intellectuelle a permis la « seconde enclosure »[1447] pour, cette fois-ci, accorder des monopoles d'exploitation sur des biens immatériels. M. B. Coriat affirme sur ce point que « *l'enclosure propre aux biens informationnels est constituée par les droits de propriété intellectuelle* »[1448]. Aussi, ce mouvement a commencé par les œuvres de l'esprit avec le droit d'auteur puis s'est étendu aux inventions grâce aux brevets. Michael Heller et Rebecca Eisenberg nomment cette enclosure « *la tragédie des anticommuns* », qui fait référence à « *une connaissance […] sous-utilisée en*

[1444] Voir *supra*, n°218 et s.
[1445] HARDIN G., « The tragedy of commons », *Science*, 13 déc. 1968.
[1446] BOYLE, J., « The Second Enclosure Movement and the Construction of the Public Domain », in *Law and Contemporary Problems*, vol. 66, n°1 et 2, 2003.
[1447] *Ibid.*, pp. 33 à 74.
[1448] CORIAT, B., « *Communs informationnels* », *in* CORNU, M., ORSI, F. et ROCHFELD, J., ss. dir., *Dictionnaire des biens communs*, PUF, 08/2017, pp. 308 à 311, spéc. p. 309.

raison des règles limitant sa circulation »[1449]. Ce phénomène a eu selon M. H. Le Crosnier des « *effets secondaires néfastes comme la diminution de la communication sur les idées ou les travaux en cours, l'arrêt des échanges de matériaux, notamment les virus et au final le ralentissement des découvertes* »[1450]. Mais, si le droit d'auteur et le brevet permettent de fermer l'accès économique pour les tiers à ces informations, l'accès intellectuel reste malgré tout ouvert[1451].

521- L'exigence de tangibilité s'est quelque peu assouplie avec l'évolution des sociétés de l'information qui ont vu apparaître de nouvelles catégories de *choses*. Le droit a reconnu leur existence et la notion de choses immatérielles est toujours en pleine expansion[1452]. Il est notable que cette catégorie soit toutefois ignorée par le Code civil. Ces choses sans *corpus,* dénuées de substance matérielle[1453], sont le fruit d'une construction de l'esprit. Elles doivent répondre à certains critères pour être considérées comme objets de droit de propriété. Elles doivent avoir une valeur[1454], faire l'objet de relations économiques[1455], mais aussi être objet de désir, évaluable selon leur utilité ou leur rareté, être appropriable, autrement dit, faire bénéficier d'un rapport d'exclusivité à leur propriétaire vis-à-vis des tiers et participer au commerce. Il faut noter que les choses immatérielles comme les choses matérielles peuvent même faire l'objet d'une copropriété. En effet, dès lors qu'une œuvre de l'esprit est créée par le concours de plusieurs personnes alors elle fait bénéficier d'une propriété commune aux co-auteurs qui répond aux principes de l'indivision, selon l'article L. 113-3 du CPI[1456]. Une invention peut également faire « *l'objet d'un dépôt commun par plusieurs personnes* », au titre de l'article L. 613-19 du CPI[1457]. Ainsi, « *la copropriété ou l'indivision sont en réalité surtout des modalités*

[1449] LE CROSNIER, H., « Communs de la connaissance », in *idem*, pp. 302 à 305, spéc. p. 303.
[1450] *Ibid*.
[1451] CHARDEAUX, M.-A., *Les choses communes*, *op. cit.*, n°129, p. 154. En ce sens, VIVANT, M., « Touche pas à mon filtre ! Droit de marque et liberté de création : de l'absolu et du relatif dans les droits de propriété intellectuelle », *JCP E*., 1993, I, 251, n°5 ; MOUSSERON, J.-M. et VIVANT, M., « Les mécanismes de réservation et leur dialectique : le terrain occupé par le droit », *op. cit.*, p. 2 : « *La formule du brevet est la reconnaissance d'un droit privatif sur une création en contrepartie de la mise à disposition de tous de l'invention faite, de l'idée industrielle* ».
[1452] LAMBERTYE-AUTRAND (de), M.-C, *Nature des biens*, eEssentiel, 2017.
[1453] LIBCHABER, R., « Répertoire de droit civil », *RTD civ*., 2016.
[1454] ROCHFELD, J., *Les grandes notions du droit privé*, PUF, 2011, pp. 229 et s. ; PIEDELIEVRE, A., *Le matériel et l'immatériel, essai d'approche de la notion de bien*, Mélanges M. Juglart, LGDJ, 1999, p° 55.
[1455] CATALA P., « La propriété de l'information », *op. cit.*, p. 97 ; voir GALLOUX, J.-C., « Ébauche d'une définition juridique de l'information », *D.,*1994. *Chron.* ; MALLET-POUJOL, N., « Appropriation de l'information : l'éternelle chimère », *op. cit.* ; DARAGON, E., « Étude sur le statut juridique de l'information », *D.*, 1998. Chron.
[1456] ROBIN, A., *La copropriété intellectuelle*, Préface de Thierry Revêt. Presses Universitaires d'Auvergne, 2005 ; ROBIN, A. et CHATRY S., *Introduction à la propriété intellectuelle*, 2e éd., Bruylant, 2020, n°270-1, p. 166-7.
[1457] ROBIN, A. et CHATRY S., *ibid*., n°326, p. 202.

d'exercice de la propriété »[1458]. La chose doit enfin pouvoir circuler, donc être admissible et aliénable de manière licite[1459], voire saisissable[1460].

2. Les données, des choses immatérielles ?

522- Le droit d'auteur oblige à distinguer selon « *les données qui constituent une création de celles qui n'en sont pas et qui, de ce fait, sont dans le domaine public* »[1461]. Or, la donnée brute n'est qu'une description élémentaire de la réalité[1462]. Elle se contente de relever l'existant. En effet, les objets connectés collectent les données sur les champs et dans les fermes, elles ne sont pas issues d'un travail de création. Il est donc possible d'ores et déjà de conclure que ces données ne peuvent pas entrer dans la catégorie des choses immatérielles susceptibles d'appropriation par le droit d'auteur. En revanche, s'agissant des données traitées ou analysées, il faut se demander si elles sont des créations intellectuelles appropriables ou bien s'il ne s'agit pas seulement d'un savoir-faire qui ne peut faire l'objet d'un droit de propriété intellectuelle.

B. La création originale, les données traitées ou analysées ?

523- Alors que « *les personnes saisissent concrètement les choses corporelles, leur corpus et les placent sous leur emprise matérielle* »[1463], la question de l'appropriation des choses intangibles, sans corpus, pose quelques difficultés. La jurisprudence a dû délimiter les contours de la propriété des choses intangibles. Ainsi, il convient, tout d'abord, d'envisager l'originalité des choses immatérielles (**1**) pour, ensuite, envisager l'originalité des données traitées et analysées (**2**).

1. L'originalité des choses immatérielles

524- Diminution de la force du droit de propriété intellectuelle par le développement des nouvelles technologies. Aujourd'hui, avec les nouvelles technologies, il est difficile de

---

[1458] *Ibid.*
[1459] MATTATIA, F. et YAICHE, M., « Être propriétaire de ses données personnelles (1ère partie) : peut-on recourir aux régimes traditionnels de propriété ? », *RLDI*, 2015/114, pp. 60 à 63.
[1460] BERLIOZ P., *La notion de bien*, LGDJ, préf. AYNES L., 2007.
[1461] BERTRAND, A., *Droit d'auteur*, *op. cit.*, 2010.
[1462] ABITEBOUL, S., « Sciences des données. De la logique du premier ordre à la Toile », Leçon inaugurale à la chaire informatique et sciences numériques du Collège de France, prononcée le 8 mars 2012 ; ABITEBOUL, S. et PEUGEOT, V., *Terra Data. Qu'allons-nous faire des données numériques ?*, Le pommier, 2017, p. 30.
[1463] ROCHFELD, J., ss. dir., *La propriété dans la jurisprudence de la Cour de cassation, op. cit.*

maintenir un véritable droit de propriété sur les choses immatérielles. En effet, les œuvres sont facilement reproductibles et non rivales. Le droit d'auteur se concilie mal avec ces caractéristiques, il est donc difficile d'affirmer que les auteurs à l'origine des œuvres ont toujours « *un droit de propriété véritable et effectif* »[1464]. La doctrine a également développé la notion de « *bien-information* »[1465], le concept de biens informationnels englobe « *à la fois, l'information et tous types de créations caractérisées par la compilation et/ou le traitement de l'information, voire les services d'information eux-mêmes* »[1466]. Mais cette notion ne concerne en réalité que les logiciels et les bases de données. Il est question des informations qui font l'objet d'une réservation par la mise en œuvre de techniques[1467]. Cette notion a été délaissée avec le temps et lui a été préféré, « *le concept de Creative Commons porteur, au plan juridique, d'enjeux nouveaux pour la propriété intellectuelle* »[1468]. Existe-t-il pour autant un droit de propriété intellectuelle sur les données ?

525. **Fichier numérique.** Pour analyser l'application du droit de propriété intellectuelle sur les données, il semble opportun de s'intéresser, au préalable, au fichier numérique qui a déjà fait l'objet d'un consensus doctrinal, mais aussi pour sa proximité avec la donnée. En effet, le fichier numérique peut être envisagé comme synonyme de la donnée elle-même, comme la mise en forme d'un contenu informationnel ou bien encore comme le support numérique[1469].

L'arrêté du 22 décembre 1981 relatif à l'enrichissement du vocabulaire ne définit pas la notion de fichier. Néanmoins, il peut être retenu que « *le fichier est, dans le langage informatique, considéré comme un ensemble de données, constitué d'informations hétérogènes ou homogènes, susceptibles de faire l'objet d'un traitement informatique* »[1470]. C'est dans le même sens que l'article 2 de la LIL dispose que « *constitue un fichier de données à caractère personnel tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés* ». Également, l'article 4 § 6 du RGPD définit le fichier comme « *tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou*

[1464] BENABOU, V.-L. et ROCHFELD, J., *À qui profite le clic ?, op. cit,* p. 48.
[1465] CATALA, P. « La propriété de l'information », *op. cit.* ; MAISON ROUGE (de) O. « La donnée : enjeu cardinal de la cybersécurité. Définition, nature, classification et extraction », *op. cit.* ; BIGOT-BESTREGUIL, M., *Le bien information,* ss. dir. LOISEAU G., Paris 1, 2017.
[1466] MALLET-POUJOL, N., « Biens informationnels (approche juridique) », in CORNU M., ORSI, F. et ROCHFELD, J., ss. dir., *Dictionnaire des biens communs, op. cit.,* pp. 142 à 143, spéc. 142.
[1467] CHARDEAUX, M.-A., *Les choses communes, op. cit*., n°129, p. 154.
[1468] MALLET-POUJOL, N., « Biens informationnels (approche juridique) », *op. cit.*, pp. 142 à 143, spéc. p. 143 ; voir AIGRAIN, P., *Cause commune, l'information entre bien commun et propriété*, Fayard, 2005.
[1469] ROBIN, A., « Le statut juridique ambivalent du fichier : de l'appropriation de la compilation à la réservation de l'information », *op. cit. ;* BENABOU, V.-L. et ROCHFLELD, J., *À qui profite le clic ?, op. cit.,* p. 65.
[1470] ROBIN, A., *ibid.*

géographique ». Enfin, Mme A. Robin retient que « *le fichier représente […] un ensemble de données et constitue finalement le moyen ordonné de stockage de celles-ci. On ajoutera simplement que le fichier est un instrument dynamique destiné à évoluer grâce au traitement dont il peut être l'objet, sachant que ce traitement est entendu largement (art. 2, L. 1978, mod. L. 2004)* »[1471]. Par conséquent le fichier est une « *information numérique constituée d'une séquence d'octets (de nombres) [qui] constitue une mise en forme d'un contenu informationnel dans le cadre d'une convention d'écriture qui permettra qu'il soit stocké, lu et transmis* »[1472]. Il contient en plus les métadonnées sur son propre fonctionnement. Le fichier peut avoir une valeur intrinsèque dès lors qu'il a des utilités propres (fiabilité, intelligibilité, mobilité, interopérabilité, capacité à épouser les évolutions de formats ou à verrouiller l'accès[1473]). Cette valeur se distingue de celle des informations contenues dans le fichier. C'est le cas, par exemple, dans l'agriculture numérique, lorsqu'il faut échanger les données des cultures. Aussi, s'agissant de l'appropriation des fichiers, quelle que soit leur utilité ou leur fonction, « *il y a lieu de considérer que [ceux-ci peuvent] être objet de droit d'auteur, dès lors qu'il est possible d'y déceler une création de forme* »[1474]. Le contenant du fichier c'est-à-dire son architecture peut alors faire l'objet d'un droit de propriété intellectuelle. C'est le droit des bases de données qui s'applique aux fichiers[1475]. En dehors de toute originalité ou de tout investissement justifiant une protection, c'est le contrat qui règle le sort de la maîtrise du fichier numérique lorsqu'il est partagé sur des plateformes, par des conditions générales d'utilisation et par le pouvoir économique de la plateforme[1476]. Aussi, les fichiers devront être interopérables, intelligibles, mobiles et pouvoir être lus par tous. Néanmoins, l'étude de l'appropriation des fichiers revient à s'intéresser à une architecture de données et non pas aux données elles-mêmes. Aussi, il faut étudier l'originalité de ces données sans formalisation.

526- **L'originalité des données.** Le critère de protection d'une œuvre de l'esprit réside dans son originalité. Cette condition s'entend comme le reflet de la personnalité de l'auteur[1477]. Toutes les œuvres de l'esprit « *quel qu'en soit le genre, la forme d'expression, le mérite ou la*

[1471] *Ibid.*
[1472] BENABOU, V.-L. et ROCHFELD, J., *À qui profite le clic ?, op. cit.*, p. 65.
[1473] *Ibid.*
[1474] ROBIN, A., « Le statut juridique ambivalent du fichier : de l'appropriation de la compilation à la réservation de l'information », *op. cit.*
[1475] *Ibid.*
[1476] BENABOU, V.-L. et ROCHFELD, J., *op. cit.*, p. 65.
[1477] BERNAULT, C., LUCAS, A. et LUCAS-SCHLOETTER, A., *Traité de la propriété littéraire et artistique, op. cit,* n°108, p. 127.

destination »[1478] peuvent bénéficier de cette protection. *A contrario*, les idées sont exclues de la protection et restent de libre parcours.

La question se pose de savoir si un travail effectué sur les données par leur traitement ou leur analyse peut faire bénéficier d'un droit d'auteur sur ces « *nouvelles* » données ou si cela ne relève que du savoir-faire de l'entreprise. Deux difficultés apparaissent. La première consiste à connaître l'éventuel titulaire du droit puisque de nombreuses personnes peuvent intervenir pour traiter les données. La seconde question soulevée consiste à identifier la valeur ajoutée à protéger. En effet, « *il conviendrait préalablement d'identifier la valeur ajoutée à protéger, ce qui reste aujourd'hui pour le moins délicat, au risque de limiter, sans justification suffisante, les libertés d'information et d'entreprendre* »[1479]. Le travail d'analyse des données ne revêt pas un caractère original puisqu'il s'agit d'un travail automatisé. Aussi, il s'agit simplement de corriger les données et d'en tirer des informations.

527- **Photographies.** La question de l'originalité des données a déjà été posée s'agissant des photographies. La jurisprudence a en effet eu l'occasion de juger qu'une photographie prise méthodiquement et systématiquement était dépourvue d'originalité, ainsi que les photographies techniques et scientifiques. Toutefois, la loi du 11 mars 1957 a fait entrer les photographies dans la catégorie des œuvres de l'esprit. Cette loi exigeait un caractère artistique ou documentaire pour bénéficier de cette protection. Elle a, ensuite, été abrogée par la loi du 3 juillet 1985 transposée à l'article L. 112-2 du CPI qui protège les œuvres photographiques et celles réalisées à l'aide de techniques analogues à la photographie. Aujourd'hui, seule la condition d'originalité compte. La question se pose donc de savoir où se trouve l'originalité dans une photographie. Selon la jurisprudence, l'originalité peut se retrouver dans le choix ou l'intérêt du sujet[1480], dans le décor et/ou la mise en scène[1481] ou encore dans le choix de l'angle de vue, du cadrage, de l'éclairage, des effets d'ombres et de lumière, la combinaison de ces choix, au-delà d'un simple savoir technique, démontre une approche propre à son auteur, exprime sa sensibilité et porte l'empreinte de sa personnalité[1482]. En revanche, le caractère original n'a pas été reconnu pour des photographies d'objets courants destinés à des catalogues[1483] ou à des vues techniques de caractère documentaire[1484].

[1478] CPI, art. L. 112-1.
[1479] CSPLA, *Droit de la propriété littéraire et artistique, données et contenus numériques*, Rapport, sept. 2018, p. 60.
[1480] CA, Montpellier, 2e ch., 2 mars 2007, *Robert* c/*Amed,* Juris-Data n°342090.
[1481] CA Paris, 4e ch., B, 28 avr. 2000, *Midi minuit* c/ *Hesser,* Juris-Data n°117960.
[1482] CA, Versailles, 26 janv. 2018, RG, n°16-02894.
[1483] CA, Bordeaux, 1e ch., 29 avr. 1997, *Pradier c/Artphoto*.
[1484] TGI Nanterre, 18 mai 1994, Gaz. Oal. 1997, 2, somm.

Ainsi, les photographies scientifiques ou techniques dont l'objectif principal est de reproduire le plus fidèlement possible le réel, que l'on cherche à atteindre une « *représentation objective de phénomènes biologiques* »[1485] ou que l'on reproduise « *sans aucune recherche esthétique* » des espèces animales[1486] et, certainement, végétales, ne devraient pas avoir de caractère original. Elles peuvent être qualifiées de photographies-instruments, c'est-à-dire, « *celles qui ne reposent pas sur une création, mais qui se contentent de reproduire de manière neutre le réel* »[1487]. Par conséquent, les photographies prises de manière automatique ne sont pas des œuvres de l'esprit protégées par le droit d'auteur. Lorsque les choix sont imposés par la technique, les photos ne sont pas originales. En revanche, lorsque l'auteur-photographe conserve sa liberté créative, les photographies documentaires peuvent bénéficier du droit d'auteur[1488].

En ce qui concerne les photographies aériennes prises par des drones, il faut démontrer que l'auteur a effectué une recherche graphique avec un cadrage particulier pour bénéficier du droit d'auteur. Mais s'il ne s'agit que d'une simple vue, ou d'un sujet d'une grande banalité, la photographie dans ce cas ne sera pas originale[1489], à tel point qu'il devient indifférent que les photos soient aériennes[1490]. Il en va de même lorsque la photographie a été prise de manière méthodique et systématique sans rechercher un effet particulier, c'est le cas notamment lorsque le déclenchement est automatique[1491]. S'agissant des photographies satellitaires, si dans un premier temps, certains auteurs ont considéré que les clichés transmis par des satellites n'étaient pas des œuvres protégées en raison du fait que l'homme ne participe pas directement à l'élaboration du cliché[1492], la jurisprudence considère aujourd'hui que chaque photo satellitaire est originale puisqu'elles ont toujours un angle de vue différent[1493]. Aussi, il apparaît que « *le processus qui permet d'obtenir ces photographies, […] est le fruit d'une succession d'opérations techniques, qui implique notamment la fabrication et le lancement du satellite, […] a néanmoins été initié par une personne physique ou une personne morale. Les photos prises par satellites constituent donc des œuvres collectives au sens de l'article L. 113-2 du*

1485 CAA Nancy, 3e ch., 19 mars 2009, n°07NC01327 : Juris-Data n°2009-005087.
1486 Cass. 1ère civ., 20 oct. 2011, n°10-21.251.
1487 VIVANT, M. et BRUGUIERE, J.-M., *Droit d'auteur et droits voisins, op. cit.,* n°200 ; LATREILLE, A., « L'appropriation des photographies d'œuvres d'art », *D.*, 2002, p. 299.
1488 CA, Paris, pôle 5-2, 19 juin 2020, n°19/02523 : JurisData n°2020-009513 ; CEIPI sept 2020 p. 2, obs. LE CAM, S., *Dalloz IP/IT*, 2021, p. 96, obs. DALEAU, J.
1489 CA, Metz, 8 janv. 2009, RG 06/03499.
1490 CA Paris, Pôle 5, 2e ch., 21 juin 2013, n°12/10106, Cass. 1ère civ., 18 févr. 2015, n°13-26.036.
1491 TGI paris, 3e ch., 1re section, 6 oct. 2009, *Casalis c/Ville de Paris* : Juris-Data n°2009-020440, CARON, C., *CCE* n°5, mai 2010, comm. 45.
1492 LELOUP, J.-M., *Le journal, les journalistes et le droit d'auteur*, thèse, 1960, p. 164.
1493 TGI, Paris, 19 déc. 1968, *D.*, 1969, somm. 118.

CPI »[1494]. Néanmoins, « *les photographies aériennes n'ont aucun caractère original et ne portent pas l'empreinte de la personnalité de leur auteur qui a réalisé la vue qu'aurait effectuée un autre technicien placé dans les mêmes conditions* »[1495].

528- **Savoir-faire.** L'analogie des photographies avec le traitement de données traitées et analysées impose de s'interroger sur leur caractère original ou bien de savoir s'il ne s'agit pas simplement d'un savoir-faire de l'entreprise. Néanmoins, il semble que le traitement des données, au moyen d'algorithmes, ne relève en réalité que du savoir-faire de l'entreprise, une autre personne aurait pu obtenir le même résultat dans les mêmes conditions. En effet, les algorithmes permettent de transformer des données brutes en informations exploitables et de les valoriser[1496]. La condition d'originalité est une fois encore difficile à démontrer[1497]. Effectivement, l'algorithme est un principe mathématique relevant du champ des idées qui ne sont pas protégeables. En revanche, le droit d'auteur offre une protection, depuis 1985, pour les logiciels[1498], à condition, toutefois, de démontrer l'empreinte de la personnalité de l'auteur. L'originalité du logiciel est très difficile à démontrer en pratique s'agissant d'une « *création essentiellement utilitaire et fonctionnelle* »[1499]. La jurisprudence a néanmoins reconnu la protection d'un logiciel par le droit d'auteur dans le cas où son code source porterait « *la marque de l'apport intellectuel* » de son auteur[1500]. Selon cet arrêt, l'originalité d'un logiciel s'entend donc d'un « *effort de personnalité allant au-delà de la simple mise en œuvre d'une logique automatique et contraignante* » et « *la matérialisation de cet effort réside dans une structure individualisée* ». Par ailleurs, les logiciels et les algorithmes peuvent être brevetés à condition d'être « *intégré(s) à une invention et qu'il(s) apporte(nt) à [l'invention] une contribution technique, notamment "un effet technique*

[1494] BERTRAND, A., *Droit d'auteur*, *op. cit.*, n°204.26 ; voir CA Riom, ch. Com., 14 mai 2003, *Rubie's France c/Msat*, *CCE*, déc. 2003, n°12, p. 27 § 117 note CARON, C.

[1495] TGI Paris, 3e ch., préc.

[1496] BOIZARD, M., « La valorisation des données numériques par la protection juridique des algorithmes », *op. cit.*

[1497] Civ. 1ère, 14 nov. 2013, n°12-20.687, *D.* 2014. 2078, obs. SIRINELLI, P. ; CJUE, 2 mai 2012, aff. C-406/10, *SAS Institute c/World Programming*, *D.* 2012. 1186 ; En ce sens, SCHULER, M. et ZNATY, B., « Quelle protection juridique pour l'algorithme ? », p. 44 et s., *in* INPI, *La propriété intellectuelle et la transformation numérique de l'économie*, 2015.

[1498] CPI, art. L. 112-2, al. 14, issu de la loi n°85-660 du 3 juill. 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle mod. par la loi n°94-361 du 10 mai 1994 prise en application de la directive communautaire 91/250/CEE du 14 mai 1991.

[1499] PIGNATARI, O. et COUSIN, A., « L'originalité des logiciels », *Dalloz IP/IT*, n°248, 2016.

[1500] Cass. ass. plén., 7 mars 1986, n°84-93.509, *D.* 1986. 406, note EDELMAN, B. ; *RTD com.* 1986. 399, obs. FRANÇON, A. ; *JCP* 1986. II. 20 631, note MOUSSERON, J.-M., TEYSSIE, B. et VIVANT, M.

supplémentaire"[1501] »[1502]. En l'absence de ces conditions, l'algorithme n'est pas brevetable[1503]. En réalité, la seule protection véritablement efficace pour les logiciels et les algorithmes est le secret, au moyen de la technique contractuelle et par la protection du secret des affaires[1504]. Mme M. Boizard relève toutefois « *[qu'] il y a lieu de penser qu'en matière d'algorithme et plus généralement pour toutes les données numériques, la condition "d'obtention illicite" risque de limiter très sérieusement la répression de la violation du secret des affaires. En effet, la victime devra apporter la preuve de cette obtention illicite et non pas seulement celle de l'utilisation des informations par le tiers. Or, la démonstration de l'origine de la fuite n'est généralement pas chose aisée. Pareille condition probatoire marque une différence significative avec les droits de propriété intellectuelle. Elle risque de réduire l'effectivité de la protection des algorithmes et d'affaiblir l'utilisation pratique de la violation du secret des affaires* »[1505].

Le droit de la propriété intellectuelle n'est donc pas applicable, dans la grande majorité des cas, aux données qui restent de libre parcours.

§2. *L'inefficience du portage des données sur la maîtrise de l'usage*

529. Le législateur européen a prévu dans le Règlement n° 2018/1807 du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, le portage des données afin de faciliter la circulation des données à caractère non personnel dans l'Union européenne. Il a également décidé d'offrir la possibilité aux acteurs privés de s'autoréguler sur cette question. Néanmoins, il faut s'interroger sur l'efficience du portage sur les données et sur son apport quant à la maîtrise de leur usage. Il est donc nécessaire, tout d'abord, d'envisager le portage comme outil réglementaire de la circulation des données (**I**) pour ensuite, s'intéresser au manque d'efficacité de cet outil (**II**).

[1501] OEB, ch. rec. tech. 3.5.1, déc. 1er juill. 1998, T-1173/97, *Produit « programme d'ordinateur » c/IBM I, JOOEB* 1999, p. 609. Voir égal. OEB, ch. rec. tech. 3.5.1, déc. 15 juill. 1986, T-208/84, *Invention concernant un calculateur c/ Vicom, JOOEB* 1987, p. 14, et OEB, ch. rec. tech. 3.5.1, déc. 21 avr. 2004, T-258/03, *Méthode d'enchères c/ Hitachi, JOOEB* 2004, p. 575 ; *RTD com*. 2006. 341, obs. GALLOUX, J.-C. ; *PI*, 2005, n°16, p. 352, obs. WARUSFEL, B.

[1502] BOIZARD, M., « La valorisation des données numériques par la protection juridique des algorithmes », *op. cit.*

[1503] OEB, ch. Rec. Tech., 16 nov. 2015 T-22/12, *Spam classification c/Microsoft*.

[1504] Voir *supra*, n°346 et s.

[1505] BOIZARD, M., « La valorisation des données numériques par la protection juridique des algorithmes », *op. cit.*

I. Le portage, outil réglementaire de la circulation des données

530- Dans un premier temps, il est nécessaire d'envisager le principe du portage des données (**A**) pour, dans un second temps, étudier sa mise en œuvre (**B**).

A. Le principe du portage

531- S'il faut, tout d'abord, analyser le contenu du portage comme il l'est décrit dans le règlement n°2018/1807 (**1**), il sera, ensuite, nécessaire d'aborder la question des titulaires du droit de portage (**2**).

1. Le contenu du portage

532- **Outil pour la circulation des données.** Le portage des données doit faciliter la libre circulation des données non personnelles sur le marché qui les concerne. Laisser le choix aux utilisateurs professionnels du fournisseur de services auquel il souhaite transmettre les données qu'il collecte ou émet permet, en effet, de stimuler la concurrence[1506]. Cette liberté de circulation doit pour cela se faire non seulement à travers les frontières de l'Union européenne, mais également entre les opérateurs[1507]. Toutefois, le portage n'est pas défini par le règlement, il est précisé néanmoins au considérant 29 qu'il s'agit de « *la capacité de transférer des données [non personnel] sans entrave* », tant trans-frontières que transopérateurs. Ainsi, les entreprises de l'*AgTech* sont contraintes d'innover afin de fournir les services les plus compétitifs possibles aux exploitants agricoles. Le règlement n°2018/1807 préconise à cette fin que le portage des données repose sur la transparence et l'interopérabilité.

533- **Limites.** Le portage des données est un outil facilitant la circulation des données mais il ne permet pas de contrôler l'usage qui en est fait. Alors que le RGPD offre un véritable droit de contrôle de l'usage des données pour les personnes concernées, le règlement n° 2018/1807 ne favorise que la circulation des données et ne prévoit aucun droit permettant de contrôler l'usage des données non personnelles. De plus, le règlement n° 2018/108 ne fait aucune distinction selon l'intérêt des données à caractère non personnel. Aussi, le règlement crée une catégorie unique de données non personnelles pour lesquelles il est présumé qu'elles doivent toutes

[1506] Règl. n°2018/1807, préc., cons. 29.
[1507] CARRE, S., « Libre circulation des données, propriété et droit à l'information (1) : à propos du règlement (UE) 2018/1807 du 14 novembre 2018 », *op. cit.*

circuler afin de favoriser la concurrence. Toutefois, certaines données non personnelles devraient faire l'objet d'un contrôle de l'usage parce qu'elles peuvent être considérées comme sensibles par les exploitants agricoles. Par conséquent, les professionnels-utilisateurs de données ne connaissent, pour l'heure, aucune limite d'utilisation ou de réutilisation des données non personnelles qu'ils détiennent.

2. Les titulaires du droit de portage

534- Seules les personnes exerçant une activité commerciale ou professionnelle[1508] sont visées par le règlement n° 2018/1807. Les consommateurs disposaient déjà d'un droit de récupération de l'ensemble de leurs données personnelles et d'utilisateurs[1509] depuis la loi pour une République numérique de 2016, mais ce droit de récupération ne s'appliquait qu'à l'encontre des fournisseurs de services de communication en ligne les plus importants dépassant un certain nombre d'utilisateurs fixé par décret[1510]. La Loi n° 2018-493 du 20 juin 2018 relative à la protection des données à caractère personnel faisant application du RGPD en droit français a néanmoins abrogé les dispositions du droit de récupération du Code de la consommation. Cette suppression a permis d'harmoniser les règles applicables aux données personnelles. Désormais, le règlement n° 2018/1807 offre la possibilité pour une personne exerçant une activité commerciale ou professionnelle de transmettre ses données à un autre fournisseur sans que le premier ne puisse opposer son refus. Il s'agit de la personne qui dispose des données, et non pas celui qui les a créées ou produites. Ce droit protège donc les fournisseurs de services et les utilisateurs professionnels et non pas les utilisateurs d'objets connectés générateurs de données. Par conséquent, le droit de portage ne concerne pas directement l'agriculteur en tant que créateur ou générateur de données.

B. La mise en œuvre du portage

535- Le portage des données est fixé à l'article 6 du Règlement n° 2018/1807. Les utilisateurs professionnels peuvent se dégager de « *toute dépendance* »[1511] à l'égard des fournisseurs de services et c'est aux acteurs du secteur eux-mêmes que revient la possibilité de fixer les règles

[1508] Règl. n°2018/1807, préc., cons. 29.
[1509] C. conso., art. L. 224-42-1.
[1510] C. conso., art. L. 224-42-4.
[1511] CARRE, S., « Libre circulation des données, propriété et droit à l'information (1) : à propos du règlement (UE) 2018/1807 du 14 novembre 2018 », *op. cit.*

applicables aux relations contractuelles entre fournisseurs et collecteurs de données sur la question du portage[1512]. Ils doivent également mettre en place des « *dispositifs de certification* »[1513]. Les seuls éléments imposés dans le règlement concernent la transparence contractuelle (**1**) et l'interopérabilité (**2**).

1. Le principe de transparence contractuelle

536. S'agissant de l'exigence de transparence, les fournisseurs de services doivent « montrer patte blanche » en fournissant les informations nécessaires aux utilisateurs professionnels. Ces informations doivent être suffisamment claires, détaillées et transparentes. Elles concernent les processus, les exigences techniques, les délais et les frais qui s'appliquent dans le cas où un utilisateur professionnel souhaiterait changer de fournisseur de services ou transférer ses données pour les rapatrier vers ses propres systèmes informatiques[1514]. Il s'agit essentiellement des conditions techniques et financières du portage, afin que l'utilisateur professionnel s'engage en connaissance de cause avec le fournisseur de services.

2. Le principe d'interopérabilité des systèmes

537. Les fournisseurs de services doivent mettre en place des standards d'interopérabilité afin de permettre une mobilité pleine et entière des données à caractère non personnel. L'interopérabilité nécessite la mise en place de formats ouverts, usuels et lisibles par machine, notamment dans des standards ouverts, lorsque le fournisseur de services le demande ou l'exige[1515]. Le règlement n°2018/1807 ne retient pas de définition à cette notion d'interopérabilité. Toutefois, il est possible d'affirmer que l'interopérabilité permet à différentes interfaces de communiquer entre elles[1516]. La Directive du 23 avril 2009 concernant la protection juridique des programmes d'ordinateur retient, quant à elle, que l'interopérabilité est « *la capacité d'échanger des informations et d'utiliser mutuellement les informations échangées* »[1517]. L'interopérabilité des systèmes doit donc permettre de réduire les coûts de

[1512] BOUGEARD, A., « Les dispositions relatives à l'accès et au portage des données : code de conduite et bonnes pratiques », *Dalloz IP/IT*, 2020, n°7 et 8.
[1513] Règl. n°2018/1807, préc., art. 6.
[1514] *Ibid.*, art. 6, 1. b).
[1515] Règl. n°2018/1807, préc., art. 6, 1. a).
[1516] VIVANT, M. et BRUGUIERE, J.-M., *Droit d'auteur et droits voisins*, *op. cit.*, n°1036, p. 1004.
[1517] Dir. n°2009/24/CE du 23 avr. 2009 concernant la protection juridique des programmes d'ordinateur (version codifiée) : *JOUE* L 111/16 du 5 mai 2009, cons. 10.

transfert et d'accroître la concurrence, mais à l'inverse, le fait de l'imposer a pour conséquence de réduire l'intérêt d'innover pour les plateformes[1518].

II. Le portage des données : entre manque de cohérence et insécurité juridique

538- Le portage des données s'avère être un outil insuffisant pour le traitement des données non personnelles, il manque de cohérence et crée de l'insécurité juridique. Le choix du législateur de proposer le portage des données au lieu de créer un véritable droit à la portabilité fait apparaître des incohérences dans les différents régimes de traitement des données (**A**) ce qui fait naître, par conséquent, de l'insécurité juridique (**B**).

A. L'incohérence des régimes de traitement des données

539- Le choix de l'adoption du portage des données pour les données à caractère non personnel a fait apparaître un manque d'harmonisation entre les règlements sur les données (**1**). En effet, alors que la portabilité des données personnelles offre un véritable outil de contrôle de l'usage des données pour les personnes concernées, le portage des données non personnelles ne facilite que leur circulation (**2**).

1. Le manque d'harmonisation entre les réglementations sur les données

540- Le portage des données ne semble pas suffisant pour répondre aux besoins et aux attentes des acteurs du secteur agricole sur la question de la maîtrise de l'usage des données. La question se pose de savoir pour quelles raisons le législateur européen a pris le parti de proposer un simple portage des données plutôt que d'imposer un véritable droit à la portabilité. Il est regrettable de constater un sérieux manque d'harmonisation entre les réglementations sur les données[1519].

[1518] GUICHARDAZ, R. et PENIN. J., « L'économie de la réutilisation des données (non personnelles) », *Dalloz IP/IT*, 2020, p. 218.
[1519] CARRE S, « Libre circulation des données, propriété et droit à l'information (1) : à propos du règlement (UE) 2018/1807 du 14 novembre 2018 », *op. cit.*

2. Des outils de portée différente

541- Si certains y voient « *une copie miroir* »[1520] du droit à la portabilité, il semble qu'à la lecture du règlement n°2018/1807 le choix des mots ne soit toutefois pas anodin[1521]. En outre, si le droit à la portabilité permet à la personne d'avoir une réelle maîtrise sur ses données, le portage n'est qu'un simple outil de transfert de données et ne favorise que leur circulation. Le G29 précise en effet dans ses lignes directrices que le droit à la portabilité permet de « *recevoir ses données* »[1522]. Cette récupération doit se faire dans un format qui le permet et ainsi les personnes concernées peuvent « *gérer et réutiliser les données à caractère personnel les concernant* »[1523]. Mais, le droit à la portabilité permet également de transmettre les données personnelles d'un responsable de traitement à un autre sans que le premier ne puisse y faire obstacle. Le portage des données n'est quant à lui pas impératif, il offre simplement la possibilité pour les acteurs de se réguler sur la question des transferts des données non personnelles sur les plans transfrontières et transopérateurs[1524]. Tandis que l'un est un véritable outil à l'autodétermination informationnelle, l'autre repose sur un principe concurrentiel qu'est la liberté d'entreprendre[1525]. Par conséquent, le portage des données est bien limité en comparaison du droit à la portabilité. En ce sens, le Conseil National du Numérique propose de reconnaître un véritable droit à la portabilité sur les données non personnelles pour tout individu et toute entreprise sur les données générées par leur utilisation d'un service[1526].

B. L'insécurité juridique

542- Le manque d'harmonisation entre les règlements sur les données peut être source d'insécurité juridique. Des personnes exerçant une activité commerciale ou professionnelle peuvent tout à fait produire ou collecter des données qui permettent de les identifier. Ainsi, les entreprises devront distinguer les données qui auront un caractère personnel de celles qui n'en ont pas. Les premières seront soumises au RGPD et pourront bénéficier du droit à la portabilité alors que les secondes seront soumises au Règlement n° 2018/1807 et ne seront pas automatiquement

[1520] BOUGEARD, A., « Les dispositions relatives à l'accès et au portage des données : code de conduite et bonnes pratiques », *op. cit.*
[1521] CARRE, S., *op. cit*.
[1522] CEPD (ex. G29), *Lignes directrices relatives au droit à la portabilité des données*, WP242, Rev. 01, adoptées le 13 déc. 2016, révisées et adoptées le 5 avril 2017, p. 5.
[1523] *Ibid*.
[1524] CARRE S., *op. cit.*
[1525] *Ibid*.
[1526] CNNum, *La libre circulation des données dans l'Union européenne*, avis, avr. 2017, p. 4.

soumises à une obligation de portage. Ce manque de cohérence entre les régimes peut être source d'inquiétudes pour les exploitants agricoles qui apportent autant d'importance aux données qui émanent de leur exploitation qu'à celles qui les concernent[1527]. Par conséquent, une telle distorsion de régime occasionne un sentiment d'insécurité juridique et produit un effet contraire à l'objectif poursuivi qui est de créer de la confiance dans le secteur du numérique.

543- **Conclusion de la section.** Le droit n'organise pas l'appropriation des données que ce soit au titre du droit civil ou du droit de la propriété intellectuelle. Aussi, le législateur n'a pris en compte, pour l'heure, que les enjeux concurrentiels en permettant le portage des données à caractère non personnel dans l'Union européenne. Cette possibilité, à la différence du droit à la portabilité contenu dans le RGPD, ne permet pas de contrôler l'usage des données issues des exploitations agricoles et détenues par les entreprises de l'*AgTech*. Par conséquent, la loi reste encore silencieuse à ce sujet, seul le contrat permet de combler ce besoin pour les agriculteurs.

Section 2. *La contractualisation du contrôle de l'usage des données brutes d'exploitation non personnelles*

544- En l'absence d'un véritable cadre juridique sur la question du contrôle de l'usage des données brutes d'exploitation non personnelles, c'est le contrat qui permet de régir les droits et obligations des parties lors de l'utilisation et du partage des données. C'est pourquoi il convient d'envisager, dans un premier temps, le principe de la contractualisation du droit de contrôle de l'usage **(§1)** pour, dans un second temps, étudier ses limites **(§2)**.

§1. *Le principe de la contractualisation du droit de contrôle de l'usage*

545- Tout d'abord, il faut s'intéresser à la source contractuelle du droit de contrôle de l'usage (**I**). Ensuite, il conviendra d'envisager la création du cadre contractuel par le droit souple pour le contrôle de l'usage des données non personnelles (**II**).

[1527] Voir *supra*, n°329.

I. La source contractuelle du droit de contrôle de l'usage

546- Aujourd'hui, l'autorégulation et la co-régulation en lieu et place d'une régulation législative tendent à se développer (**A**), ce qui a permis l'émergence du droit souple dans le secteur agricole (**B**).

A. Le développement des modèles alternatifs de régulation

547- Après avoir étudié les notions d'autorégulation et de co-régulation (**1**), il sera nécessaire d'envisager l'intérêt de ces systèmes de régulation (**2**).

1. Les notions d'autorégulation et de co-régulation

548- En plus de la régulation législative, il existe deux modes alternatifs de régulation que sont la co-régulation et l'autorégulation. Ces deux modes de régulations ont été intégrés dans l'accord institutionnel « *Mieux légiférer* » de 2003, puis supprimés dans celui de 2016, le législateur considérant que ce nouvel accord ne contient plus de cadre légal pour l'utilisation des modes de régulation alternatifs[1528].

L'autorégulation était définie en 2003 comme « *la possibilité pour les opérateurs économiques, les partenaires sociaux, les organisations non gouvernementales ou les associations, d'adopter entre eux et pour eux-mêmes des lignes directrices communes au niveau européen (notamment codes de conduite ou accords sectoriels)* »[1529]. Avec un tel mécanisme, la législation s'adapte aux problèmes et aux secteurs concernés. Il permet également d'alléger le travail législatif en se concentrant sur les aspects essentiels et de profiter de l'expérience des parties concernées[1530].

La co-régulation était définie quant à elle comme « *le mécanisme par lequel un acte législatif communautaire confère la réalisation des objectifs définis par l'autorité législative*

[1528] Résolution du Parlement européen, 30 mai 2018, sur l'interprétation et la mise en œuvre de l'accord interinstitutionnel « Mieux légiférer » (2016/2018[INI]), pt D.
[1529] Parlement Européen, Conseil de l'Union européenne et Commission des communautés européennes, *Accord interinstitutionnel — « Mieux légiférer »* : *JOUE* C 321 du 31 déc. 2003 pp. 1 à 5, pt 22, (ancien), remplacé par Accord interinstitutionnel entre le Parlement européen, le Conseil de l'Union européenne et la Commission européenne « *Mieux légiférer* » : *JOUE* L 123/1 du 12 mai 2016.
[1530] *Ibid.*

aux parties concernées reconnues dans le domaine (notamment les opérateurs économiques, les partenaires sociaux, les organisations non gouvernementales ou les associations) »[1531].

2. L'intérêt des modèles alternatifs de régulation

549 **Efficacité de modèles alternatifs de régulation**. L'autorégulation et la co-régulation sont des instruments de régulation marqués « *par le pragmatisme et la flexibilité* »[1532]. Les acteurs du secteur, considérés comme plus compétents pour répondre aux besoins et aux attentes des participants à leur activité, ont des intérêts à défendre, c'est pourquoi ils peuvent au moyen de cette forme de régulation confronter et arbitrer les intérêts sociaux[1533] de leurs activités. Cet « *autre droit* »[1534] complète ou accompagne la législation contraignante (*Hard Law*)[1535] en s'adaptant au concret, en se rapprochant des individus et en étant en adéquation avec le contexte des sociétés qu'il prétend régir[1536]. Il répond mieux aux attentes et aux contraintes d'un secteur donné. En effet, les destinataires de la régulation sont associés au processus d'élaboration des normes[1537]. En intervenant dans le processus de décision, les acteurs font entendre leurs intérêts et « *le droit devient un droit négocié, qui est le fruit d'une délibération collective* »[1538]. Ils orientent eux-mêmes leurs comportements. Le droit mou est ainsi élaboré sous forme d'objectifs, de directives, de recommandations et mise sur la dissuasion plutôt que sur la répression[1539]. Il s'inscrit dans un mouvement de déréglementation dont l'objectif est de réajuster les modalités de la régulation juridique[1540]. Ce n'est, en revanche, pas « *un repli de la régulation juridique au profit d'autres modes de régulation sociale* »[1541]. La *Soft Law* a aussi un « *rôle de diffusion du droit dur* »[1542], elle permet de mieux atteindre les acteurs d'un secteur et de mieux contrôler l'effectivité d'un règlement.

[1531] *Ibid.*, pt 18.
[1532] CHEVALLIER, J., « La régulation juridique en question », *Droit et société*, 2001/3, n°49, pp. 827 à 846, spéc. 834.
[1533] *Ibid.*
[1534] TIMSIT, G., « Les deux corps du droit : essai sur la notion de régulation », *RFAP*, 78, 1993, pp. 375, et s. FRISON-ROCHE, M.-A., « Le droit de la régulation », *D.*, 2001, chron., pp. 610 et s. ; CHEVALLIER, J., « La régulation juridique en question », *op. cit.*, p. 833.
[1535] CAPPELLO M. (Ed.), « Autorégulation et corégulation dans la nouvelle directive SMAV », IRIS *Spécial*, Observatoire européen de l'audiovisuel, Strasbourg, 2019, (dir. n°2018/1808 du 14 nov. 2018, Services de médias audiovisuels : *JOUE* L 303/69 du 28 nov. 2018).
[1536] TIMSIT G., « Les deux corps du droit : essai sur la notion de régulation », *op. cit.*
[1537] CHEVALLIER J., « La régulation juridique en question », *op. cit.*, p. 834.
[1538] *Ibid.*
[1539] *Ibid.*
[1540] *Ibid.*, p. 833.
[1541] *Ibid.*
[1542] AILINCAI, M., « *La soft law est-elle l'avenir des droits fondamentaux ?* », dossier : Le droit des libertés en question(s) – Colloque des 5 ans de la RDLF, *RDLF*, 2017, chron., n°20.

550. **Des modèles de régulation plébiscités par les autorités.** Les autorités françaises « *entendent porter une régulation plus souple et collaborative en s'appuyant sur le pouvoir des utilisateurs […]* »[1543]. C'est donc la multitude qui offre le pouvoir de réguler les activités numériques. L'ARCEP[1544] plébiscite même une « *régulation par la Data* »[1545] qui se sert « *du pouvoir d'action de la multitude* »[1546] *via* l'État-plateforme. Également, le règlement pour la protection des données à caractère personnel et celui sur la libre circulation des données à caractère non personnel, préconisent aux acteurs des secteurs de rédiger des codes de bonnes conduites afin de régir, notamment, la circulation des données agricoles. L'ensemble des initiatives des syndicats agricoles offre donc un cadre pour l'exploitation de ces données. Un cadre qui s'avère flexible et pragmatique. Ces réglementations viennent s'ajouter à la réglementation positive étatique et supra-étatique.

551. **Les risques des modèles de régulation alternatifs.** La prolifération de normes peut conduire à un éclatement de la régulation juridique[1547] et prendre la forme « *d'un "entrelacement d'actions multiples" dont la compatibilité reste problématique ce qui pose la question de son effectivité* »[1548]. Ainsi, « *trop de régulation tue la régulation* » et les acteurs pourraient s'affranchir des contraintes imposées par leur propre secteur en raison des failles, des incohérences et des contradictions du système existant[1549].

B. L'émergence du droit souple dans le secteur agricole

552. Le secteur de l'agriculture numérique a pris à bras le corps la question de la circulation et du partage des données agricoles dans des textes déontologiques afin de réguler leur propre secteur (**1**). De même, afin d'assurer la mise en œuvre effective de cette *Soft Law,* les acteurs ont mis en œuvre des outils techniques pour l'obtention du consentement des agriculteurs (**2).**

[1543] ZOLYNSKI, C., « La loyauté des plateformes pensée par la loi pour une République numérique », *in* CHATRY, S. et GOBERT, T., ss. dir., *Numérique : Nouveaux droits, nouveaux usages,* Mare & Martin, 2017, pp. 125 à 126.
[1544] L'autorité de régulation des communications électroniques, des postes et de la distribution de la presse.
[1545] ARCEP, *Pour un numérique soutenable*, rapport d'étape, 15 déc. 2020, pp. 86 et s.
[1546] ZOLYNSKI, C., « La loyauté des plateformes pensée par la loi pour une République numérique », *op. cit.*
[1547] CHEVALLIER, J., « La régulation juridique en question », *op. cit.,* pp. 827 à 846.
[1548] *Ibid*., p. 844.
[1549] *Ibid*., p. 845.

1. Les textes déontologiques du secteur agricole

553- **Principe.** L'objectif du règlement nº 2018/1807 est d'encourager les acteurs du secteur agricole à s'autoréguler sur les questions du portage des données par le biais de codes et de bonnes pratiques. Ces règles vont bien plus loin que le cadre proposé par ce règlement qui reste tout à fait en retrait sur la question de la maîtrise des données. L'enjeu est bien là pourtant. Le règlement ne s'attarde que sur la libre circulation et les enjeux concurrentiels, alors que de vraies problématiques existent concernant la perte de maîtrise des données non personnelles par les générateurs de données. C'est ainsi que le secteur de l'agriculture numérique a pris en considération la question de la circulation et du partage des données agricoles, ainsi que leur maîtrise et a proposé des initiatives afin de les réguler dans leur propre secteur.

554- **Étendue.** Déjà en 2015, l'ACTA[1550] et les instituts techniques agricoles préconisaient dans leurs recommandations[1551] d'établir une charte sur l'accès et la valorisation des données agricoles. Cette charte avait pour objectif de garantir la maîtrise des données, d'établir une chaîne de confiance et d'encourager l'ouverture des données des entreprises. De même, le *Think Tank* renaissance numérique, recommandait en novembre 2015 de « *libérer et tirer profit de la donnée sans exploiter l'agriculteur* »[1552]. Des initiatives européennes et françaises offrent, aujourd'hui, un droit souple autour de l'usage et de l'exploitation des données agricoles. Ces initiatives s'inscrivent dans la même veine que la charte « *Privacy and security principles of Farm Data* » établie par le *Farm Bureau* aux États-Unis le 1er avril 2016. En France, en 2018, deux syndicats français à savoir la FNSEA[1553] et les JA[1554] ont rédigé la Charte Data-Agri. Cette charte contient treize principes dont l'objectif est d'assurer pour l'agriculteur la lisibilité du contrat, la transparence de l'usage des données, la maîtrise de l'usage des données et enfin la sécurité des données. De plus, elle offre la possibilité pour les entreprises de l'*AgTech* de faire labelliser leurs contrats d'utilisation des données agricoles selon ces recommandations. De cette façon, les syndicats du secteur agricole assurent un rôle de contrôle[1555] de l'équilibre contractuel. Mais, également, cette labellisation favorise la confiance des agriculteurs « *en les rassurant sur les pratiques professionnelles des sites concernés, en conformité avec la*

[1550] Association de coordination technique agricole.
[1551] ACTA, *L'accès aux données pour la recherche et l'innovation en agriculture, Position des Instituts techniques agricoles,* oct. 2016.
[1552] THINK TANK RENAISSANCE NUMERIQUE, *Les défis de l'agriculture connectée dans une société numérique*, nov. 2015, p. 68.
[1553] Fédération nationale des syndicats d'exploitations agricoles.
[1554] Jeunes Agriculteurs
[1555] FERAL-SCHUHL, C., ss. dir., C*yberdroit, op. cit.*, chap. 221.

législation en vigueur »[1556]. La même année, en 2018, un Code de conduite[1557] sur le partage des données dans le secteur agricole a été établi par plusieurs syndicats agricoles européens[1558]. Ce code a vocation à poser des principes et des lignes directrices dont l'objectif est de soutenir le développement de l'agriculture numérique.

2. Les outils techniques pour la gestion des consentements

555 **Gestion des consentements.** Certains des points développés par la *Soft Law* font l'objet de développements techniques par d'autres acteurs, afin de garantir une mise en œuvre effective de ces recommandations par les entreprises de l'*AgTech*. Le Code de l'Union européenne et la Charte Data-Agri préconisent de renforcer le consentement des agriculteurs sur l'usage des données issues de leur exploitation. La Charte Data-Agri exige, ainsi, le consentement de l'agriculteur pour tout traitement ou tout usage par un tiers sur les données collectées. De même, le Livre blanc sur l'accès aux données pour la recherche et l'innovation souhaite voir généraliser un « *consentement préalable conscient et mesuré* »[1559]. C'est ce que propose de développer le CASDAR Multipass au moyen d'un outil de gestion des consentements. Ce projet lancé en 2018 « *vise à mettre à disposition des producteurs et valorisateurs de données agricoles, un écosystème de gestion des consentements des agriculteurs protégeant les échanges de données des exploitations. En renforçant la confiance des producteurs nécessaire au partage de leurs données, le projet vise l'émergence de nouveaux services innovants* »[1560]. L'objectif est de construire une chaîne de confiance entre les acteurs de l'agriculture numérique fondée sur le consentement. Ainsi, sur le modèle du RGPD, l'exploitant agricole devrait pouvoir donner son consentement à chaque étape de la vie de la donnée de son exploitation, pour l'accès aux données, leur partage ou tout usage non prévu initialement dans le contrat. Le consentement doit donc être libre, spécifique, éclairé et univoque. Sur la forme, ce consentement doit faire l'objet d'un écrit « *soit par une clause du contrat liant l'exploitant*

[1556] *Ibid.*
[1557] COPA COGECA, Code de conduite de l'UE relatif au partage des données agricoles par accord contractuel, 2018.
[1558] Fertilizers europe, Copa Cogeca, eettar, EFFAB, CEJA, FEFAC, European Crop Protection, CEMA, ESA, CLIMMAR, animalhealth europe.
[1559] ACTA, *L'accès aux données pour la recherche et l'innovation en agriculture, Position des Instituts techniques agricoles, op. cit.*, p. 25.
[1560] LAUGA, B., Synthèse du projet MULTIPASS – faire émerger de nouveaux services dans une chaine de confiance, mai 2021.

agricole et le collecteur de données, soit par un avenant ou tout autre moyen écrit permettant d'établir l'expression d'un consentement »[1561].

Ainsi, l'issue de ce projet devait permettre de mettre en œuvre efficacement le principe de la Charte Data-Agri et du Code de conduite de l'Union européenne consistant à demander le consentement de l'agriculteur avant tout traitement, usage et partage des données collectées sur leur exploitation. Multipass a publié douze recommandations pour renforcer la confiance dans le cadre du partage de données en agriculture. Notamment, les professionnels du secteur agricole sont exhortés à généraliser le consentement, à construire une chaîne de confiance et à respecter les bonnes pratiques.

556- **Risques de l'utilisation du consentement comme base juridique du traitement.** Si le consentement pour le renforcement des pouvoirs de l'agriculteur est fondamental afin de lui octroyer le contrôle de l'usage des données issues de son exploitation, il n'en reste pas moins qu'un simple consentement comporte des limites. Hormis le fait que les textes de droit souple sont très peu appliqués dans les faits, le risque principal d'un consentement comme permission d'utilisation des données par le co-contractant est qu'il soit dévoyé ou encore que l'agriculteur accepte toutes les demandes de consentement sans se renseigner ou au contraire qu'il les refuse toutes d'un bloc[1562]. Alors le consentement n'apporterait pas les garde-fous nécessaires à la protection des données et pourrait avoir pour conséquence de limiter l'innovation. De plus, l'obtention d'un consentement libre dans une relation contractuelle déséquilibrée, telle que le sont, bien souvent, les contrats de l'agriculture numérique, s'avère difficile, voire impossible[1563].

II. La création d'un cadre contractuel par le droit souple pour le contrôle de l'usage des données brutes non personnelles

557- Les acteurs du secteur agricole ont offert un cadre contractuel aux producteurs et utilisateurs de données issues des exploitations agricoles. L'étude de ces textes conduit à développer, en premier lieu, la Charte Data-Agri (**A**), puis, en second lieu, le Code de conduite de l'Union européenne relatif au partage des données agricoles par accord contractuel (**B**).

[1561] FNSEA et JA, *Valoriser et sécuriser les données des exploitations agricoles dans les contrats*, Charte Data-agri, 2018.
[1562] Voir *infra*, n°765.
[1563] Voir *infra*, n°759 et s.

A. L'apport de la Charte Data-Agri

558- Il convient d'envisager d'abord, le contenu de la Charte Data-Agri (**1**), puis sa mise en œuvre (**2**).

1. Le contenu de la Charte Data-Agri

559- **Principe.** La Charte Data-Agri propose un cadre pour les contrats de l'agriculture numérique. Elle invite les collecteurs de données[1564] à prévoir dans leurs contrats la maîtrise exclusive de l'usage des données agricoles au bénéfice de l'exploitant agricole. L'objectif principal est de replacer l'agriculteur au centre de l'économie des données agricoles, en lui donnant plus de poids dans les relations contractuelles avec ses cocontractants. À cette fin, l'exploitant agricole doit pouvoir contrôler l'accès et l'usage aux données collectées sur son exploitation. Le champ d'application de la Charte entoure les données brutes et les données primaires non anonymisées, c'est-à-dire, les données qui n'ont pas fait l'objet d'un traitement ou de manipulation ou bien les données issues de l'expertise ou de l'analyse de données agricoles brutes qui n'ont pas été anonymisées. Par conséquent, seules les données primaires qui ont fait l'objet d'une anonymisation sont exclues de la Charte. Ainsi, l'exploitant agricole peut contrôler l'accès et l'usage des données primaires non anonymisées et le contrôle de la collecte de l'accès et de l'usage des données brutes d'exploitation. La Charte Data-Agri est lapidaire sur la question de l'accès, mais elle reconnaît un droit d'accès exclusif à l'agriculteur, excluant de fait les tiers. Elle exige le consentement de l'agriculteur pour tout traitement ou tout usage par un tiers sur les données collectées. L'exploitant agricole peut également choisir les données collectées, ce qui peut en être fait (droit de contrôle de l'usage), à qui elles peuvent être transmises (droit de regard), il peut aussi les récupérer (droit à la portabilité) et les supprimer (droit à l'oubli). L'exploitant agricole peut s'il le souhaite, octroyer certains de ses droits à son co-contractant.

560- **Objectifs.** La *Soft Law* permet aux acteurs du secteur de contrôler eux-mêmes l'application de ces règles par les acteurs de l'écosystème de l'agriculture numérique. En effet, elle offre la possibilité de labelliser les contrats du secteur agricole au regard de la Charte Data-Agri éditée par les syndicats. De cette manière, les entreprises qui s'y soumettent s'engagent à respecter la

[1564] Une personne physique ou morale qui est responsable de la collecte des Données agricoles brutes dans le but de constituer une base de données afin de les traiter et/ou de les céder à un tiers. Il s'agit notamment de fournisseurs de matériels ou de logiciels/applications et des prestataires de services.

Charte lors de l'utilisation des données. Au-delà de la labellisation, les acteurs du secteur contrôlent ainsi le respect de leurs propres règles par l'ensemble des acteurs.

2. La mise en œuvre du droit de contrôle de l'usage

561- La Charte Data-Agri prévoit des outils afin d'assurer l'effectivité des droits de contrôle de l'usage par les exploitants agricoles. D'abord, le collecteur de données a un devoir d'information à l'égard de l'exploitant agricole. Il doit rendre l'information accessible et lisible au moyen d'un contrat ainsi que de notices explicatives sur l'usage et le stockage des données. À cette fin, le collecteur doit tenir informer tout au long de la relation contractuelle l'exploitant agricole des modalités et du lieu de stockage des données. En outre, le collecteur de données doit être expressément identifié dans le contrat afin de faciliter le retrait des données par l'exploitant agricole. En plus du lieu et des modalités de stockage, le collecteur de données doit informer l'exploitant agricole des données qui seront collectées, traitées, rendues accessibles à des tiers, ainsi que la finalité du recueil ou du traitement. Ensuite, le collecteur de données doit assurer la portabilité des données pour que l'exploitant agricole puisse les récupérer et les transférer à d'autres collecteurs de données. L'objectif ici est de permettre la circulation des données entre plusieurs objets connectés et éviter la rétention technique des données par un opérateur. Mais encore, en cas de changement du côté du collecteur de données, par la cession de la base de données, un changement de contrôle du collecteur de données ou des termes du contrat, l'exploitant agricole doit toujours pouvoir retirer et récupérer ses données. De plus, le collecteur de données doit obtenir le consentement exprès, explicite et éclairé de l'exploitant agricole, en cas de collecte, d'accès et d'usage des données brutes et des données primaires non anonymisées. En outre, le collecteur de données doit obtenir le consentement préalable à toute cession, utilisation ou diffusion des données brutes et primaires non anonymisées à un tiers. Les contrats conclus avec les tiers doivent contenir les mêmes garanties et conditions de confidentialité que dans le contrat initial (chaîne de contrat). Il est fait ici une analogie avec le consentement du RGPD qui permet de faire reposer le traitement des données à caractère personnel sur le consentement de la personne physique concernée[1565]. Ainsi, l'exploitant agricole répartit les droits qu'il détient sur les données entre les co-contractants selon leurs besoins. En outre, le collecteur de données qui détient ses droits d'un agriculteur ne peut pas les outrepasser et en céder plus qu'il n'en possède aux tiers. De plus, le partage des données avec un tiers ne peut aller à l'encontre des engagements pris dans le contrat initial avec

[1565] CASDAR, Multipass pour une extension du consentement à toutes les données agricoles.

l'exploitant agricole. Le collecteur de données doit aussi informer l'exploitant agricole des conséquences de ses choix selon qu'il accepte ou non la collecte, le traitement et l'usage des données agricoles sur l'accessibilité ou non des services offerts. À l'issue du contrat, le collecteur de données doit assurer à l'exploitant agricole, le retrait, la destruction sécurisée ou la récupération par l'exploitant agricole des données générées par son exploitation selon des modalités fixées par contrat. Enfin, la sécurité et la confidentialité des données sont à la charge du collecteur de données. En effet, lorsque les données sont agrégées dans des bases de données, l'entreprise doit assurer la confidentialité des données en empêchant toute possibilité de réidentification afin de garantir l'anonymat des exploitants agricoles. En outre, il ne peut utiliser les données à l'encontre des intérêts de l'exploitant agricole.

B. L'apport du Code de conduite de l'Union européenne relatif au partage des données agricoles par accord contractuel

562- Sur le même principe que la Charte Data-Agri, il sera nécessaire d'analyser, en premier lieu, le contenu du Code de conduite de l'Union européenne relatif au partage des données agricoles par accord contractuel (**1**), puis sa mise en œuvre (**2**).

1. Le contenu du Code de conduite

563- **Principe.** Le Code de conduite de l'Union européenne sur le partage des données agricoles par accord contractuel propose également un cadre applicable aux relations contractuelles entre les exploitants agricoles et leurs co-contractants. L'objectif est d'assurer plus de transparence dans les contrats et de responsabiliser les acteurs de l'agriculture numérique afin de gagner la confiance des créateurs de données. L'objectif final étant le partage des données entre les différents opérateurs. Le champ d'application du Code de conduite entoure les données agricoles non personnelles, il exclut donc les données à caractère personnel et les données de machines[1566]. Le Code de conduite est plus large également que la Charte puisqu'elle s'intéresse aux contrats tripartites : le créateur, le fournisseur et l'utilisateur de données. Également, la notion de créateur de données est élargie par rapport à celle *« [d'] exploitant agricole* » retenue par la Charte Data-Agri, elle comprend tous ceux qui produisent des données ou qui les

[1566] COPA COGECA, *Code de conduite de l'UE relatif au partage des données agricoles par accord contractuel*, p. 10.

commande. Le créateur de données est donc défini comme « *la personne ou l'entité qui peut prétendre disposer d'un droit exclusif d'accorder l'accès aux données et de contrôler leurs utilisation ou réutilisation plus en aval* »[1567]. C'est donc celui qui crée ou collecte les données en utilisant lui-même des moyens techniques ou qui confie cette tâche à des fournisseurs de données[1568]. Le plus souvent, le créateur de données sera l'agriculteur[1569], mais il peut aussi s'agir de l'utilisateur des données qui traite et fournit des informations d'aide à la décision et crée de nouvelles données. Ensuite, les données sont collectées par le fournisseur de données, le plus souvent le prestataire de services qui fournit le matériel, le logiciel et/ou l'application. L'utilisateur de données est, quant à lui, défini comme celui qui reçoit les données de la part du créateur ou du fournisseur de données en vertu d'un contrat. Enfin, le tiers est entendu comme la personne physique ou morale autre que le créateur de données qui reçoit des données de la part d'un utilisateur de données ou du fournisseur en vertu d'un contrat. Le tiers n'a donc pas de lien direct avec l'exploitant agricole, à la différence du fournisseur et de l'utilisateur de données.

564- **Objectifs.** Le Code de conduite qualifie le créateur de données de « *propriétaire* »[1570], dans le même sens que le *Farm Bureau* aux États-Unis. Il est considéré comme celui qui peut prétendre disposer d'un droit exclusif d'accorder l'accès aux données et de contrôler leur utilisation par le fournisseur ou l'utilisateur de données en vertu d'un contrat. À cette fin, un large panel de droits est reconnu à l'exploitant agricole. Il dispose ainsi du droit d'accès, du droit de contrôle, du droit à la portabilité et du droit d'effacement ou droit à l'oubli. Il a la maîtrise exclusive des données, il contrôle la collecte, l'accès, le traitement et l'usage des données. Il doit également pouvoir choisir les services dont il a besoin en connaissance de cause et il doit pouvoir rompre le contrat s'il le souhaite. L'issue de ce contrat doit alors être corrélée avec la suspension ou l'arrêt de la collecte et de l'utilisation des données de son exploitation.

2. La mise en œuvre du contrôle de l'usage

565- Afin d'assurer la maîtrise des données par les exploitants agricoles, les entreprises de l'*AgTech* voient leurs obligations renforcées. Le Code de conduite prévoit une obligation d'information

[1567] *Ibid*. p. 6.
[1568] *Ibid.*, p. 9
[1569] *Ibid.*, p. 9 : Les données étant « *produites par un opérateur de la chaine agricole en raison de son activité ou sont commandées par ce dernier, l'opérateur en question est considéré comme étant le créateur des données* ».
[1570] *Ibid.*, p. 6 : « *Déf. Créateur de données (parfois désigné propriétaire) : dans ce code, le créateur (propriétaire) est généralement défini comme étant "la personne ou l'entité qui peut prétendre disposer d'un droit exclusif d'accorder l'accès aux données et de contrôler leur utilisation ou réutilisation plus en aval"* ».

claire et accessible de la part du fournisseur de données à l'égard du créateur dans les contrats. Ainsi, les co-contractants du créateur de données, mais aussi les tiers, doivent fixer des finalités de traitement. Le contrat doit être rédigé dans un langage simple et compréhensible. Il doit définir clairement les conditions de collecte et de partage des données selon les besoins de chaque partie. De cette manière, les co-contractants peuvent bénéficier des droits d'accès et d'usage que le créateur de données accepte de répartir. Ils peuvent, alors, accéder puis utiliser les données de l'exploitant agricole au moyen du contrat. Le Code de conduite prévoit également que l'accès aux données collectées ne peut avoir lieu que dans le cadre d'une « *autorisation explicite, expresse et informée sous forme d'un document contractuel* »[1571] du créateur de la donnée. Par conséquent, le Code conclut que « *le droit de déterminer qui peut accéder aux données et les utiliser* »[1572] doit revenir, généralement, à l'agriculteur. Toutes les parties au contrat peuvent protéger les informations sensibles « *en limitant leur future utilisation ou futur traitement* ». Le Code ajoute dans le même paragraphe une obligation d'obtenir le consentement du créateur de données avant toute utilisation, traitement ou partage des données.

Ensuite, le Code de conduite innove en proposant en échange de la création et du partage des données par le créateur une contrepartie qui peut être financière ou non. Il peut s'agir de l'obtention de services, de meilleurs produits ou autres. Cette proposition, comme il l'a été vu plus haut[1573], semble bien difficile à appliquer au vu de la difficulté d'évaluer la valeur des données et en raison de l'absence d'appropriation sur les données.

Le Code prévoit également une obligation d'obtenir l'autorisation (consentement) expresse, explicite et informée sous la forme d'un document contractuel pour tout(e) collecte, accès, stockage et utilisation des données agricoles. Le fournisseur de données doit assurer l'anonymat du créateur de données lors de leur traitement et de leur usage. Il faut noter que le Code de conduite exige la pseudonymisation des données lorsqu'elles sont utilisées. Dans ce cas, le fournisseur de données ne peut spécifier les conditions selon lesquelles l'identification du créateur de données peut être rendue possible et lorsqu'elles sont transmises aux tiers. Or, les données pseudonymisées sont des données personnelles régies par le RGPD. Par conséquent, ces données doivent reposer sur une base légale. Ainsi, seule l'anonymisation des données permet de les utiliser sans le consentement de leur créateur ou dans le cadre de l'une des finalités prévues par le RGPD.

[1571] *Ibid.*, p. 9
[1572] *Ibid.*
[1573] Voir *supra*, n°517.

Mais aussi, le créateur de données doit autoriser le partage de ses données avec des tiers. Si le partage des données avec les tiers doit intervenir en cours de réalisation du contrat, le créateur de données doit également donner son consentement et ne peut être sanctionné en cas de refus. Le partage des données doit se faire dans les mêmes conditions et garanties que dans le contrat initial.

De plus, les co-contractants doivent respecter des obligations techniques sur les données, ils ne peuvent les conserver au-delà du temps strictement nécessaire à la réalisation des analyses prévues. Ils doivent assurer le traçage des données afin de reporter les transferts et les modifications des données au créateur de données. Les co-contractants doivent également assurer l'accessibilité des données, sauf impossibilité technique qui devra être précisée dans le contrat.

De même, ils doivent assurer la portabilité et l'interopérabilité des données pour le créateur des données qui doit pouvoir transférer ses données à d'autres utilisateurs, mais aussi utiliser ses données dans d'autres plateformes, systèmes ou installations de stockage, selon des modalités précisées dans les contrats. Le Code de conduite rappelle ensuite que les contrats ne peuvent pas être modifiés unilatéralement sans l'accord du créateur de données. Ce dernier peut se retirer du contrat et mettre fin ou suspendre la collecte et l'utilisation de ses données, à condition toutefois d'avoir respecté ses obligations contractuelles. Il doit pouvoir choisir entre les services qui lui sont proposés en toute connaissance de cause.

Enfin, les co-contractants des créateurs de données ne peuvent utiliser les données à d'autres fins que celles prévues au contrat et à des fins contraires aux intérêts du créateur de données. Ils ne doivent jamais détourner les données à quelques fins autres que celles prévues au contrat. Par exemple, il est interdit de faire un usage frauduleux des données tel que de la spéculation sur les marchés ou encore « *[d'] évaluer la capacité à payer de l'exploitant agricole pour disposer du service ou de la machine* ». Les utilisateurs de données doivent, par ailleurs, assurer la protection des données. Ainsi, les entreprises cocontractantes engagent leur responsabilité et doivent mettre en œuvre les mesures techniques nécessaires afin d'assurer la sécurité des données, d'autant plus lorsqu'elles sont considérées comme sensibles. Elles doivent donc protéger les données contre les tentatives de vol, de piratage, de saisie, de confiscation, etc. Enfin, le Code de conduite rappelle que le RGPD s'applique aux données à caractère personnel.

§2. *Les limites de la contractualisation du droit de contrôle de l'usage*

566. Le développement du droit souple pour encadrer l'usage des données agricoles n'est toutefois pas sans limites. Aussi, il convient d'envisager, dans un premier temps, la portée limitée du droit souple (**I**) pour, dans un second temps, s'intéresser au manque d'effectivité du droit souple sur le contrôle de l'usage des données agricoles (**II**).

I. La portée limitée du droit souple

567. Tout d'abord, il faut soulever l'absence de contrainte du droit souple qui n'encourage pas les acteurs du secteur agricole à se plier aux règles (**A**). Il sera également nécessaire d'envisager les risques de confusion dus à la multiplicité des textes de *Soft Law* et des acteurs (**B**).

A. L'absence de contrainte

568. Le droit souple n'est pas assorti de sanctions juridiques imposables aux personnes qui ne respecteraient pas les règles (**1**), ce qui conduit, malheureusement, au constat d'une faible participation volontaire des acteurs du secteur agricole (**2**).

1. Des sanctions non juridiques

569. Si la régulation par les textes de *Soft Law* offre plus de souplesse pour répondre aux attentes des acteurs, son principal inconvénient reste son aspect non contraignant. En effet, il n'existe aucune contrainte juridique pour l'application des textes de droit souple. Leur application repose sur le principe d'une participation volontaire des acteurs. Le non-respect de ces règles par les acteurs peut seulement entraîner des sanctions d'ordre économique ou social, comme par l'atteinte à la réputation par exemple, ou l'exclusion d'une communauté, ou encore, des sanctions de natures commerciales. La *Soft Law* permet donc de faire une mauvaise presse aux entreprises qui ne la respecteraient pas. Ainsi, dans la balance bénéfices-risques, certaines entreprises en situation de monopole ou de position dominante sur un secteur peuvent préférer conserver leur avantage concurrentiel plutôt que de partager les données qu'ils détiennent ou de fournir le contrôle de l'usage de ces données à leurs clients. En effet, la rétention des données par les entreprises participe à l'obtention d'un monopole, alors que le droit souple prône la

maîtrise des données par l'exploitant agricole afin de favoriser leur circulation. Il en va de même pour les nouveaux arrivants sur le marché, comme un constructeur d'objets connectés innovants qui choisirait de restreindre l'accès aux données qu'il collecte dans le but d'obtenir un avantage concurrentiel. En outre, les grands groupes internationaux auront moins de scrupules à limiter l'accès au marché dans leur propre intérêt.

2. Une faible participation volontaire des acteurs

570- En l'absence de contraintes juridiques, il faut faire le constat que les acteurs sont très peu nombreux à s'être volontairement soumis aux textes de *Soft Law*. Le nombre d'entreprises labellisées par la Charte Data-Agri en est un exemple concret. Très peu d'entreprises ont été labellisées à l'heure actuelle[1574]. Ceci peut s'expliquer par différentes raisons. D'abord, le désintérêt des acteurs peut résulter d'un manque de publicité des textes. Ensuite, il peut s'agir simplement du refus de s'y soumettre. La maîtrise des données par l'exploitant agricole n'est pas toujours une priorité pour les entreprises. Un élément de réponse tient au fait, également, que la labellisation porte sur les contrats eux-mêmes, ce qui implique que chaque contrat doit être labellisé. La procédure s'avère ainsi fastidieuse.

B. Les risques de confusion

571- La *Soft Law* peut faire naître des risques de confusion dans l'esprit des acteurs du secteur agricole et, par conséquent, engranger une perte de confiance dans ce mode de régulation. D'abord, parce qu'il existe plusieurs règles venant de différents acteurs. Ensuite, parce qu'il existe des distinctions fondamentales dans les notions et les régimes de ces différents textes. Aussi, il faut faire le constat d'un manque d'homogénéité des textes (**1**), aboutissant à un manque de clarté pour les acteurs du secteur agricole (**2**).

1. L'hétérogénéité des textes

572- **Hétérogénéité du vocabulaire.** Parmi les risques d'une « *inflation non maîtrisée des chartes, codes et autres textes de Soft Law* »[1575], il faut relever, notamment, des distinctions fondamentales dans les notions et les régimes. En effet, un trop grand nombre de

[1574] https://www.data-agri.fr
[1575] JUILLET-REGIS, H., « Quelle régulation pour les données agricoles ? », *op. cit.*

recommandations et de principes venant de différents acteurs peut créer un effet de boulimie et rendre ces initiatives contreproductives. En l'occurrence, de trop nombreuses initiatives pourraient créer un climat anxiogène et confus et laisser les acteurs du secteur perplexes face à des recommandations qui diffèrent, notamment sur les définitions retenues. Par exemple dans la Charte Data-Agri, le « collecteur de données » est défini comme « *une personne physique ou morale qui est responsable de la collecte des Données agricoles brutes dans le but de constituer une base de données afin de les traiter et/ou de les céder à un Tiers. Il s'agit notamment des fournisseurs de matériels ou de logiciels/applications et des prestataires de services* ». Ainsi, selon cette définition, le collecteur de données est le fournisseur de matériels et/ou de services, celui qui traite les données en vue d'en retirer une information. Le collecteur des données n'est donc pas l'exploitant agricole qui est considéré comme « *la personne physique ou morale qui a le contrôle de l'acte de production agricole* ». L'exploitant agricole est donc maintenu en dehors du cycle de création et de collecte des données. Or, dans le Code de conduite européen, la « personne qui collecte ou crée les données » est nommée « créateur de données » et est définie comme « *celui qui a créé/collecté ces données soit en utilisant lui-même des moyens techniques (machines agricoles, programmes électroniques de traitement des données, etc.) soit en confiant cette tâche à des fournisseurs de données* », il peut donc s'agir de l'agriculteur qui utilise les objets connectés sur son champ.

573- **Hétérogénéité des régimes.** Ces différences sont fondamentales puisque la qualification des co-contractants entraîne le régime qui leur est applicable selon qu'ils détiennent ou non les droits sur les données de l'exploitation. Ainsi, dans la Charte Data-Agri l'exploitant agricole a bien la maîtrise des données, mais cette qualité de créateur de données n'est pas justifiée, alors qu'elle l'est dans le Code de conduite. De plus, les termes utilisés par les deux documents sont différents et induisent des régimes distincts quant à la maîtrise juridique des données. Le Code de conduite désigne le « *créateur de données* » comme étant le « *propriétaire* » des données qu'il génère. Alors que de manière plus nuancée, la Charte Data-Agri ne retient qu'une « *maîtrise exclusive qui fait naître des droits pour l'exploitant agricole sur les données générées sur son exploitation* ». La maîtrise exclusive des données n'a pas les mêmes effets qu'un droit de propriété. En effet, la maîtrise exclusive est relative, opposable aux seules parties au contrat, alors que le droit de propriété est un droit réel opposable *erga omnes*. Ces deux notions juridiques n'ont pas les mêmes effets sur la chose. Par conséquent, ces différences peuvent avoir des conséquences sur le régime applicable aux données.

574- **Risques de perte de confiance**. L'hétérogénéité des textes peut être préjudiciable pour les acteurs du secteur agricole qui peuvent se perdre et refuser de les prendre en compte. Le risque bien évidemment est de retenir les acteurs de partager les données qu'ils détiennent et de conserver, au contraire, des comportements prédateurs.

2. Le manque de clarté des textes

575- **Effets de l'absence de texte impératif.** L'absence de réglementation impérative entraîne des comportements de réservation chez les acteurs du secteur agricole qui ont pour conséquence la rétention des données. Ces comportements freinent l'innovation et le développement des activités agricoles. Mais aussi, les agriculteurs perdent totalement confiance dans l'agriculture numérique et refusent de participer à la mise en commun des données et des savoirs en ne partageant pas les données de leur exploitation[1576]. De plus, le manque de limpidité de la *Soft Law*, pointé du doigt par le *Think tank* Renaissance numérique dans sa note sur « *La valeur des données agricoles* » du 26 février 2018[1577], peut empêcher de rééquilibrer les « *forces au sein de la chaîne de valeur* »[1578].

576- **Importance d'un texte impératif.** Le *Think tank* propose que la circulation des données soit fondée réellement « *sur des bases juridiques partagées par tous* » dans « *un effort pédagogique* » en se fondant sur la loi, le contrat et le contentieux pour régir la collecte, le traitement et le partage des données. Il ajoute que « *les relations contractuelles ont un rôle clé à jouer, à condition de ne pas servir de base au maintien de relations asymétriques* ». Une des options possibles envisageables pourrait être la blockchain qui « *peut offrir un cadre alternatif se passant d'intermédiaires pour sécuriser juridiquement (à travers des smart-contracts) et économiquement les transactions* ». Il apparaît indéniable que « *la Soft Law ne suffit pas, il faut adopter une régulation plus impérative* »[1579] dont l'objectif est la recherche d'un équilibre entre circulation et maîtrise. Une contrainte juridique est donc justifiée afin d'éviter ce type de verrouillage, mais aussi afin de permettre une réutilisation des données et de démultiplier leur valeur[1580]. Ainsi « *ces multiples verrous justifient l'intervention publique et l'organisation*

[1576] Reportage, « Agriculture et numérique : la technologie au service des agriculteurs ? », *Un monde en docs*, présenté par CHAPUIS J., émission diffusée sur Public Sénat, le 27 févr. 2021.
[1577] THINK TANK RENAISSANCE NUMERIQUE, *La valeur des données agricoles*, févr. 2018.
[1578] *Ibid.*
[1579] JUILLET-REGIS, H., « Quelle régulation pour les données agricoles ? », *op. cit.*
[1580] BERTRAND, B., « Le modèle européen de partage des données », *op. cit.*, n°19.

d'une gouvernance des données »[1581]. Par conséquent, il y a, à ce jour, un véritable enjeu de clarification qui tient en l'avènement d'un véritable droit des données non personnelles.

II. L'inefficience du droit des contrats sur le contrôle de l'usage des données d'exploitation

577- Si le droit des contrats permet de contrôler l'accès aux données brutes par le biais de la confidentialité, il n'en va pas de même pour l'usage. Ceci s'explique par le fait que lorsque les données sont détenues par une personne, cette dernière peut mettre en place, en plus d'une clause de secret, des moyens techniques pour en conserver l'accès. Or, l'usage des données brutes non personnelles ne peut être contrôlé puisqu'aucun droit n'existe sur ces données et la technique ne permet pas d'appuyer ce contrôle. C'est pourquoi les clauses de propriété qui peuvent laisser croire en l'existence d'un contrôle de l'usage des données par le contrat sont des mirages (**A**). En outre, le contrôle de l'équilibre contractuel dans les contrats ne permet pas non plus de contrôler l'usage des données (**B**).

A. Le mirage de la clause de propriété

578- La clause de propriété dans les contrats de l'agriculture numérique a été inventée par la pratique (**1**), mais, sans fondement, cette clause s'avère inefficiente (**2**).

1. Une clause inventée par la pratique

579- Au sens de l'article 1103 du Code civil, le contrat tient lieu de loi à ceux qui l'ont fait. Aussi, pour rappel, chacun est libre de déterminer le contenu de leurs engagements et de contracter ou de ne pas contracter. La pratique est libre de créer les contrats qu'elle souhaite, il s'agit alors de contrats innomés. Par conséquent, pléthore de contrats voient le jour afin de régir les relations entre les agriculteurs et leurs cocontractants. Ces contrats ne sont donc pas réglementés, mais restent soumis au contrôle du déséquilibre significatif et doivent respecter les principes de bonne foi, de loyauté et de transparence[1582]. L'absence de régime spécifique applicable aux contrats portant sur les données conduit la pratique à établir les clauses qu'elle

[1581] *Ibid.*
[1582] Voir *supra*, n°316 et s.

souhaite selon les intérêts et les besoins des parties. Des clauses ont alors été créées par la pratique supposées organiser la maîtrise juridique des données brutes non personnelles. Si rien ne permet de contester leur validité formelle, la question de leur efficience se pose néanmoins. En effet, la pratique a largement intégré dans ses contrats la clause de propriété des données brutes d'exploitation. Bien que le plus souvent rédigée au bénéfice du client, agriculteur, cette clause peut aussi bénéficier à l'équipementier, au fournisseur de services ou à l'éditeur de logiciel. D'autres contrats prévoient un partage de la propriété entre les co-contractants dans une clause nommée clause de copropriété et offrent à chaque partie la liberté d'utiliser les données brutes comme elles l'entendent. Ces clauses ont donc pour objet de prévoir contractuellement la propriété des données.

2. Une clause inefficiente

580- Les clauses de propriété dans les contrats de l'agriculture numérique ne reposent sur aucun fondement. En outre, elles ne produisent aucun effet en cas de non-respect par l'autre partie, mis à part celui de rassurer l'agriculteur au cours de la relation contractuelle. En effet, cette clause ne saurait octroyer véritablement les droits d'un propriétaire à l'agriculteur au sens juridique du terme. Le droit de propriété est un droit réel sur une chose[1583]. Or, les données n'étant pas objet de propriété[1584], dans le cas d'un conflit sur l'utilisation des données sans l'accord de l'agriculteur par exemple, le juge serait impuissant pour faire reconnaître une telle atteinte. Le simple fait de rédiger une clause de propriété dans un contrat n'engendre pas la reconnaissance d'un droit de propriété sur les données. Mme A. Robin soutient à ce sujet « *[qu'] il y a […] ici une contrevérité qui fait figure d'incantation en ce qu'elle laisse croire à la possibilité d'une sanction contractuelle (rupture du contrat, par exemple) applicable à celui qui aurait utilisé ou diffusé ces données* »[1585]. Ainsi, aucune sanction ne pourrait être retenue à l'encontre de l'entreprise qui utilise ou diffuse des données non personnelles sans le consentement de la personne désignée comme propriétaire dans le contrat, sauf à démontrer l'existence d'une clause de secret, mais on se situe dans ce cas en dehors du champ de la propriété. De plus, les contrats ne créent que des droits personnels dont les effets sont relatifs c'est-à-dire qu'ils n'ont d'effet qu'à l'égard des parties. Il serait donc impossible de poursuivre un tiers qui recevrait les données du fournisseur de services, à la différence du droit de propriété

[1583] Voir *supra*, n°506.
[1584] Voir *supra*, n°512 et s.
[1585] ROBIN, A., « Agriculture numérique, données et droit : topographie juridique de l'"écosystème informationnel vert" », *Sciences Eaux & Territoires*, 2019, p. 41.

qui est un droit réel opposable à tous. Il y aurait, ici, en réalité, une confusion entre propriété et confidentialité, car « *la confidentialité n'est […] jamais juridiquement à l'origine d'un droit de propriété* »[1586]. Par conséquent, celui qui organise la confidentialité des données qu'il détient n'en est pas pour autant propriétaire, il ne peut qu'engager la responsabilité du cocontractant qui ne respecte pas son obligation de secret. En revanche, une fois que les données sont diffusées, rien ne pourra contraindre les tiers à restituer et supprimer ces données. Mais encore, le fait de considérer une donnée comme un bien par la voie contractuelle implique de reconnaître sa valeur intrinsèque et impose d'établir une contrepartie financière en échange des données. Une telle évaluation n'est pourtant jamais envisagée dans les contrats qui prévoient une clause de propriété ou de copropriété[1587]. En définitive, cette clause ne présente que peu d'intérêt en pratique puisqu'elle ne produit aucun effet concret. Son utilité est limitée à l'aspect psychologique qu'elle procure à l'agriculteur à qui le contrat donne l'illusion d'être propriétaire et d'avoir la maîtrise des données brutes de son exploitation. Ce qui est bien loin de la réalité.

B. L'inefficacité du contrôle de l'équilibre contractuel sur l'usage des données agricoles

581- Le droit d'user de la chose revient au propriétaire de cette chose, il est également libre de la céder, d'en récolter les fruits ou bien de la détruire. Par conséquent, il est seul à pouvoir maîtriser l'usage du bien à travers un contrat. Puisque le droit de propriété n'est pas applicable aux données, la question se pose de savoir s'il existe néanmoins un droit d'usage sur les données (**1**) et s'il est possible d'en maîtriser l'usage au moyen du contrôle de l'équilibre contractuel (**2**).

1. L'absence de contrôle de l'usage des données agricoles

582- Le droit français reconnaît au propriétaire de la chose la possibilité de contrôler l'usage de son bien. Celui qui acquiert un bien au moyen d'un contrat de vente obtient l'usage qui ne peut être limité contractuellement[1588]. De même, le contrat de location portant sur un bien permet de transférer la jouissance de ce bien à autrui[1589]. Le preneur obtient un droit personnel de

[1586] *Ibid.*
[1587] TOMASSO, L., *Analyse juridique contractuelle des données de l'agriculture numérique*, Multipass, 29 nov. 2019.
[1588] C. civ., art. 544.
[1589] C. civ. arts. 1713 à 1778.

jouissance qui porte sur la chose, objet du contrat[1590], il en acquiert dès lors la maîtrise à titre précaire, dont il jouit de manière indépendante et exclusive. Le bailleur peut toutefois se réserver un droit d'usage dans le contrat qui est soumis à la liberté contractuelle. Le propriétaire peut également définir la destination de la chose louée par exemple, pour un bail immobilier, et il peut désigner l'usage qui peut être fait de ce bien (commercial ou privé). En droit d'auteur, l'auteur dispose également d'un droit de destination[1591] lui permettant de contrôler le sort des exemplaires de son œuvre dont il autorise la diffusion. Il peut interdire par exemple une utilisation commerciale de son œuvre, même une fois cédée. Le propriétaire de la chose a donc la maîtrise de l'usage de son bien. Ainsi, le droit français n'octroie un droit d'usage qu'au propriétaire d'un bien. Or, les données n'étant pas appropriables, leur détenteur ou producteur ne peuvent bénéficier d'un droit d'usage. Crier haut et fort que l'agriculteur dispose de la maîtrise de l'usage des données de son exploitation est inefficace tant qu'on ne met pas en place de véritables outils permettant d'assurer cette maîtrise. La liberté contractuelle a donc ses limites et n'offre pas les garanties nécessaires aux agriculteurs pour contrôler l'usage des données de leur exploitation.

2. Le devoir d'information sur l'usage des données

583- **Principe.** Au titre du devoir d'information régi par l'article 1112-1 du Code civil, la partie qui « *connaît une information dont l'importance est déterminante pour le consentement de l'autre* » doit l'en informer lors des négociations précontractuelles. Sont déterminantes « *les informations qui ont un lien direct et nécessaire avec le contenu et la qualité des parties* ». Par conséquent, un créateur ou un producteur de données peut porter une attention particulière à l'usage qui est fait de ses données au cours de la relation contractuelle. Néanmoins, la majorité des contrats de l'agriculture numérique a pour objet la mise à disposition d'un service ou d'une plateforme en contrepartie du paiement d'un prix. La collecte et l'utilisation des données ne sont que des éléments accessoires au contrat. Bien que les parties puissent en faire des éléments déterminants de leur consentement, il n'en demeure pas moins que les contrats de l'agriculture numérique sont également des contrats d'adhésion auxquels les agriculteurs s'engagent afin de pouvoir accéder auxdits services et plateformes. Par manque d'information ou de transparence, l'agriculteur ne lira pas toujours les astérisques et entre les lignes. De plus, si les entreprises se pliaient de manière précautionneuse à l'exercice et informaient les agriculteurs de l'usage

[1590] C. civ., art. 1709.
[1591] CPI, art. L. 122-1.

qu'elles souhaitent opérer sur leurs données, ces informations n'auraient que pour effet de laisser à l'agriculteur le choix de consentir ou non au contrat en connaissance de cause. La transparence dans le contrat ne permet pas à l'agriculteur d'obtenir une véritable maîtrise des données issues ou collectées sur son exploitation. Elle doit surtout permettre à l'agriculteur de « voir » ce qui se trouve derrière le contractant[1592]. S'agissant des données agricoles, les informations peuvent porter sur le lieu et l'organisme de stockage, les algorithmes utilisés, etc. Les contrats de l'agriculture sont encore trop opaques sur les questions qui ont trait au traitement des données. À moins de considérer le traitement des données comme l'objet même du contrat, il ne semble pas que le devoir d'information soit applicable aux données de l'agriculture numérique[1593].

584- **Absence d'effet du devoir d'information sur l'usage des données.** Trop peu de clauses portent effectivement sur la question de l'usage des données. Les fournisseurs de services et/ou de logiciels se contentent la plupart du temps de prévoir des clauses de propriété sans évoquer la question de l'usage. Par conséquent, les contrats restent silencieux sur la question du contrôle de l'usage des données. Puisque le droit ne prévoit pas de droit d'usage sur les données en faveur de son collecteur ou producteur, alors l'exploitant agricole qui entre dans cette catégorie ne peut pas imposer d'obligation au fournisseur de services et/ou de logiciels. Les contrats de l'agriculture numérique portent le plus souvent sur la mise à disposition d'un service en échange d'un paiement. L'usage des données n'entre donc pas dans l'équilibre du contrat.

585- **Conclusion de la section.** La régulation des activités liées à l'usage et au partage des données agricoles par les acteurs eux-mêmes a permis d'apporter un cadre salvateur grâce à la Charte Data-Agri et au Code de conduite de l'Union européenne, pour les entreprises de l'*AgTech*, au bénéfice des agriculteurs. Ce cadre fournit, ainsi, les orientations nécessaires afin de construire des contrats de prestation de services et de fourniture d'objets connectés équilibrés entre les droits et les obligations des parties quant à l'usage et au partage des données. Il faut bien reconnaître le mérite du droit souple de proposer un cadre aux acteurs du monde agricole. Néanmoins, bien qu'on note une prise en considération de ces enjeux par les entreprises concernées, il demeure que cette forme de régulation crée un risque de confusion en raison d'incohérences entre les textes et d'un manque de clarté. Ainsi, le droit souple n'apporte pas les garanties suffisantes pour s'imposer dans le secteur agricole. Le droit des contrats ne permet

[1592] AUBIN-BROUTE, R.-J., « Le contrat pour la maîtrise des données agricoles », *op. cit.*

pas non plus de remédier à l'absence de droit de contrôle de l'usage au bénéfice de l'agriculteur, puisque le contrat seul n'est pas suffisamment efficace pour contrôler l'usage d'une chose immatérielle. Le contrat pour être efficace, dans ce cas, doit en effet être accompagné par la technique.

586. **Conclusion du chapitre.** Bien que le contrôle de l'usage par l'agriculteur de ses données d'exploitation soit un objectif poursuivi par certains acteurs de l'agriculteur numérique, dans les faits, tant le droit que le contrat sont, pour l'heure, inefficaces afin d'assurer un tel contrôle par l'exploitant agricole. Le droit est silencieux sur la question et le contrat n'est pas suffisant à lui seul pour être efficace. Il en résulte qu'il est désormais primordial de régir l'usage des données agricoles brutes non personnelles, à l'image de ce qui est proposé par les acteurs du secteur agricole.

587. **Conclusion du titre.** Le législateur a pris en compte depuis 2018 les enjeux de la circulation et de la valorisation des données non personnelles. Si les données agricoles publiques peuvent être réutilisées librement, les données privées sont à la merci des acteurs qui les détiennent et qui en contrôlent l'accès. Il a été démontré en effet au cours de ce développement que le contrôle de l'accès permettait de contrôler l'usage des données. Néanmoins, en tant que générateur des données d'exploitation au moyen des objets connectés qu'il utilise, l'agriculteur devrait obtenir le droit de maîtriser l'usage de ces données. Or, ni le droit ni le contrat ne lui offre la possibilité d'obtenir un tel contrôle de l'usage des données qu'il génère. Il ne peut donc que compter sur la magnanimité des entreprises chez qui il souscrit son abonnement ou à qui il achète son matériel pour ne pas voir les données de son exploitation être utilisées à des fins contraires à ses intérêts. À l'image des pays pillés de leurs informations génétiques, les agriculteurs souhaitent également pouvoir contrôler l'usage des données qu'ils produisent et consentir avant toute utilisation ou tout partage de leurs données. C'est pourquoi un texte impératif, tel que l'accord de Nagoya pour les informations génétiques des pays, devrait encadrer efficacement le contrôle de l'usage par le générateur des données, tout en trouvant un équilibre entre circulation, valorisation et maîtrise des données agricoles.

Titre II. La maîtrise envisagée de l'usage des données d'exploitation par l'exploitant agricole

588. Les agriculteurs s'inquiètent de l'exploitation et du partage de l'ensemble des données collectées sur leur exploitation agricole, peu importe qu'elles aient un caractère personnel ou non. Ils attachent autant d'importance aux données à caractère non personnel qu'aux données personnelles qu'ils génèrent ou collectent sans distinction. Pourtant, le législateur a créé des régimes différents selon que les données sont identifiantes ou non. La maîtrise de l'usage des données comporte trois volets : la protection, la circulation et la valorisation des données. Les données publiques et les données d'intérêt général ont vocation à être partagées et diffusées au plus grand nombre. Une large diffusion de ces données doit permettre, notamment, le partage des connaissances, la transparence de la vie publique, la santé publique, mais aussi, l'innovation. En principe, ces données peuvent être réutilisées librement par les utilisateurs afin de favoriser l'émergence de nouveaux services et usages[1594]. Au contraire, les restrictions à la libre réutilisation doivent reposer sur des motifs d'intérêt général. De plus, ces restrictions doivent être proportionnées et ne pas avoir pour effet ou objectif de porter atteinte au libre jeu de la concurrence[1595]. Par conséquent, l'agriculteur, le fournisseur de services et/ou de matériels, ou encore les administrations et les plateformes, autrement dit, tous ceux qui pourraient revendiquer des droits sur ces données d'une manière ou d'une autre, ne pourront contrôler l'usage de ces données une fois diffusées. Il ne semble donc pas pertinent d'évoquer le contrôle de l'usage des données collectées et partagées dans l'intérêt public ou général.

589. La Commission européenne a adopté ces dernières années de nombreux textes portant sur les données[1596] pour poursuivre sa stratégie européenne[1597] dans l'objectif de construire une économie fondée sur les données[1598]. Jusqu'alors aucune réglementation ne permettait de contrôler l'usage des données à caractère non personnel. Une première étape dans le contrôle de l'usage des données avait été franchie avec le RGPD pour la maîtrise de l'usage des données à caractère personnel. Mais, aujourd'hui, une seconde étape s'apprête à être franchie avec la

---

[1594] Mission confiée par le Premier ministre à Éric Bothorel, *Pour une politique publique de la donnée*, déc. 2020, p. 27 ; CYTERMANN, L., ss. dir., *Rapport relatif aux données d'intérêt général*, *op. cit.*, p. 16.

[1595] https://guides.etalab.gouv.fr/juridique/reutilisation/#qu-est-ce-qu-une-reutilisation

[1596] Règl. n°2018/1807, préc. ; Dir. n°2019/1024 ; Proposition de règlement sur la gouvernance des données (DGA, 25 oct. 2020, COM(2020) 767 final) ; Règl. n°2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement n°2018/1724 (règlement sur la gouvernance des données) : *JOUE*, L 152/1, 3 juin 2022 ; Règl. général n°2016/679, 27 avr. 2016, sur la protection des données (RGPD)

[1597] Commission européenne, *Une stratégie européenne pour les données*, 19 févr. 2020, COM(2020) 66 final.

[1598] Commission européenne, *Créer une économie européenne fondée sur les données*, 10 janv. 2017, COM(2017) 9 final.

proposition de règlement de la Commission européenne nommée *Data Act*[1599] dont l'objectif est d'harmoniser les règles d'accès et d'utilisation des données. Jusqu'alors, seule leur circulation avait été réglementée au moyen du Règlement sur la libre circulation des données. Le Règlement général sur la protection des données et le Règlement établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne, forment un cadre global pour la libre circulation des données dans le marché européen. Pourtant, l'usage des données à caractère non personnel soulève de nombreuses questions, notamment, concernant les personnes autorisées à les utiliser ou encore la manière dont elles peuvent être utilisées. Un usage non contrôlé de ces données peut avoir d'importants impacts sur la concurrence et l'innovation mais aussi sur la confiance des utilisateurs d'objets connectés qu'ils portent sur les producteurs d'objets connectés et les prestataires de services de collecte et de traitement des données. Par conséquent, un travail doit être mené sur la recherche d'une réglementation pour le contrôle de l'usage des données d'exploitation à caractère non personnel (**Chapitre 1**). Concernant les données à caractère personnel, le droit de contrôle de l'usage a déjà été consacré par la législation sur les données personnelles (**Chapitre 2**).

[1599] Commission européenne, proposition de règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données - *Data Act*), COM(2022) 68 final, 2022/0047 (COD), 23 fèvr. 2022.

Chapitre 1. La consécration souhaitée du droit de contrôle de l'usage des données d'exploitation à caractère non personnel

590- Obtenir le contrôle de l'usage des données d'exploitation non personnelles est un jeu d'équilibriste sur le fil entre circulation et maîtrise. Ces deux injonctions contraires doivent composer le droit de contrôle de l'usage des données non personnelles. Si le Règlement sur la circulation des données a permis de répondre à l'injonction de la circulation puisqu'il régit la possibilité de stocker et de diffuser les données non personnelles n'importe où dans l'Union européenne, aucun texte ne réglemente pour l'heure la maîtrise de l'usage des données non personnelles. Les détenteurs de données — producteurs d'objets connectés et/ou fournisseurs de services — peuvent donc laisser libre cours à leur imagination dans les contrats portant sur l'exploitation des données agricoles qu'ils détiennent. Toutefois, la Commission européenne a présenté le 23 février 2022 une Proposition de règlement[1600] qui devrait offrir un cadre à l'accès et à l'usage des données non personnelles. Quelques pistes d'améliorations seront étudiées dans ce chapitre afin de prendre en compte les enjeux juridiques autour des données collectées ou produites sur les exploitations agricoles. Dans un premier temps, il sera donc nécessaire de présenter le principe du droit de contrôle de l'usage des données (**Section 1**). Dans un second temps, il faudra envisager l'esquisse du droit de contrôle de l'usage construit comme un droit granulaire (**Section 2**).

Section 1. Le principe du droit de contrôle de l'usage des données d'exploitation non personnelles

591- La création d'un nouveau droit suppose d'étudier ses fondements **(§1**), mais également ses contours **(§2**).

§1. *Les fondements du droit de contrôle de l'usage des données d'exploitation non personnelles*

592- Le droit de contrôle de l'usage repose sur plusieurs fondements. D'une part, ce droit doit offrir une meilleure maîtrise de l'usage des données issues des objets connectés dans un secteur

[1600] *Ibid.*

économique déséquilibré (**I**). D'autre part, il a pour vocation d'assurer une meilleure circulation des données non personnelles en offrant les outils juridiques qui permettent de renforcer le portage contenu dans le Règlement sur la libre circulation des données (**II**).

I. L'accroissement de la sécurité juridique

593- L'objectif premier du droit de contrôle de l'usage est de renforcer la maîtrise de l'usage des données non personnelles (**A**), en harmonisant les normes d'usage qui entourent les données (**B**).

A. Le renforcement de la maîtrise de l'usage des données non personnelles

594- Le droit tel qu'il est conçu aujourd'hui est favorable aux entreprises qui détiennent les données et qui en ont le contrôle par la technique et le contrat (**1**), ainsi, la création d'un droit de contrôle de l'usage des données non personnelles doit avoir pour objectif d'assurer l'autonomie des agriculteurs sur les données qu'ils génèrent (**2**).

1. Contrer le contrôle factuel de l'usage par les entreprises détentrices

595- À l'heure actuelle, le secret des affaires permet de protéger certaines informations à condition de mettre en œuvre les moyens juridiques et/ou techniques pour assurer cette protection[1601]. En effet, le détenteur légitime d'un secret d'affaires est celui qui a licitement le contrôle du secret. Or, les exploitants agricoles ne disposent pas des mêmes capacités de contrôle, sur les données qu'ils génèrent au moyen des objets connectés, que les entreprises qui détiennent effectivement ces données. Par conséquent, dans les faits, les agriculteurs ne peuvent jamais revendiquer un secret des affaires sur les données qu'ils génèrent lors de leurs activités et délèguent la protection de leurs données à leurs prestataires de services. C'est pourquoi la Proposition de règlement sur les données a pour objectif d'accroître la sécurité juridique afin d'encadrer l'utilisation et le partage des données industrielles[1602]. Pour cela, le règlement souhaite imposer des règles aux fabricants et aux concepteurs de produit afin qu'ils fassent preuve de transparence dans les contrats et que les données soient facilement accessibles et réutilisables.

[1601] Voir *supra*, n°351 et s.
[1602] *Ibid.*

La sécurité juridique est renforcée également en octroyant aux utilisateurs d'objets connectés le droit de partager les données qu'ils génèrent auprès de fournisseurs de services tiers.

2. Assurer l'autonomie des agriculteurs

596. L'instauration d'un droit de contrôle de l'usage des données en faveur des exploitants agricoles a pour objectif de fournir les outils nécessaires pour assurer l'autonomie des agriculteurs vis-à-vis des entreprises collectrices de données. Il devient primordial de créer un droit de contrôle de l'usage en faveur des exploitants agricoles au regard des comportements de certains industriels. Pour citer un exemple, des groupements industriels outre-Atlantique n'hésitent pas à revendre les données des méthodes d'élevages ou des techniques culturales des agriculteurs directement à leurs concurrents afin d'améliorer leurs rendements[1603]. Mais encore, les données des agriculteurs peuvent être utilisées à des fins spéculatives afin de faire baisser le prix d'achat des productions et influencer le cours des marchés[1604], le risque étant que les agriculteurs perdent peu à peu le contrôle de leur exploitation et que les grands groupes industriels prennent les décisions en lieu et place des agriculteurs, les reléguant au simple rôle de manutentionnaire. Les exploitants agricoles ne pourront plus faire valoir leurs connaissances pratiques de la terre et des animaux, les grands groupes industriels devenant l'Alpha et l'Omega de l'agriculture et de l'élevage.

B. L'harmonisation des normes d'usage sur les données non personnelles

597. La création d'un nouveau droit de contrôle de l'usage pour les données non personnelles doit participer à l'harmonisation des normes applicables à l'usage des données dans l'Union européenne. C'est le but principal poursuivi par la Commission européenne en date du 23 février 2022 dans sa *Proposition de règlement fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données*. Aussi, concernant l'aspect utilisation, l'objectif est de normaliser les règles applicables aux données non personnelles pour les consommateurs et les professionnels tout en préservant les investissements dans la valorisation des données. Il s'agit également d'harmoniser les transferts de données entre services par la mise en place de standards d'interopérabilité.

[1603] L'EFFET PAPILLON, « États-Unis : Les agro-hackeurs », Documentaire, 24 sept. 2017.
[1604] COCHELIN, P., « La poule aux œufs d'or échappera-t-elle aux agriculteurs ? », *Terre-net média,* 15 mai 2018.

II. L'amélioration de la circulation des données non personnelles

598. Au fil des ans, le droit à la portabilité[1605] a vu son champ d'application s'élargir. D'abord, cantonné à la transférabilité des numéros de téléphone dans les années quatre-vingt-dix[1606], ce n'est que récemment avec le Règlement général sur la protection des données[1607] que le droit à la portabilité s'est étendu aux données. Néanmoins, le droit à la portabilité ne s'applique pour l'heure qu'aux données à caractère personnel. Le législateur avait consacré dans la Loi pour une République Numérique le droit à la portabilité des données non personnelles pour les consommateurs, mais les difficultés de mise en œuvre l'ont poussé à rétropédaler en supprimant ce dispositif contenu dans le Code de la consommation[1608]. Or, aujourd'hui il existe de véritables enjeux à la portabilité des données à caractère non personnel. Il apparaît désormais primordial de reconnaître un droit général à la portabilité afin de favoriser la valorisation, la circulation et la maîtrise de l'usage des données. Les deux composantes du droit à la portabilité que sont le transfert des données à d'autres opérateurs et la récupération des données par le client permettent d'assurer à la fois une meilleure concurrence sur le marché et une meilleure maîtrise juridique des données non personnelles par l'agriculteur. Ce droit doit être associé à l'interopérabilité des systèmes d'information afin de permettre le partage technique des données.

599. Si le droit à la portabilité des données à caractère personnel repose sur le fondement de l'autodétermination informationnelle[1609], la question se pose de savoir sur quels principes reposeraient un droit à la portabilité sur les données agricoles non personnelles. Afin de répondre à cette question, il convient tout d'abord de se pencher sur les aspects concurrentiels du droit à la portabilité (**A**) pour ensuite s'intéresser au contrôle des données agricoles non personnelles (**B**).

[1605] Pour une définition, voir *supra*, n°541.
[1606] C. conso., art. L. 224-42-1.
[1607] Règl. n°2016/679 du 27 avr. 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 : *JOUE* L 119/1 du 4 mai 2016.
[1608] Loi n°2018-493, 20 juin 2018, relative à la protection des données personnelles : *JORF* n°0141 du 21 juin 2018, modif. Loi n°78-17, 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés : *JORF* du 7 janvier 1978.
[1609] Voir *infra*, n°680 et s.

A. Favoriser la concurrence

600- Le droit de contrôle de l'usage des données doit permettre, au moyen du développement du droit à la portabilité et de l'interopérabilité, de faciliter les transferts de données à d'autres fournisseurs de services (**1**), mais aussi de favoriser la multi-domiciliation (**2**).

1. Faciliter les transferts des données à d'autres fournisseurs de services

601- Le fait que l'exploitant agricole n'a pas la maîtrise de l'usage des données de son exploitation l'empêche de transférer ses données, de manière libre, à d'autres fournisseurs de services que celui avec lequel il a souscrit un contrat en première intention. Cette carence limite la libre circulation des données. De plus, les partenaires commerciaux des agriculteurs ont la possibilité de réserver l'accès des données qu'ils détiennent. En effet, les fournisseurs de services ont souvent des systèmes informatiques prioritaires qui empêchent les exploitants agricoles de partager les données qu'ils génèrent avec d'autres partenaires ou de les récupérer eux-mêmes. Ces comportements réservataires peuvent avoir de lourdes conséquences en termes concurrentiels et limiter les agriculteurs dans le choix de leurs partenaires commerciaux. Or, le droit à la portabilité repose sur un fondement économique qui est le droit de transférer les données à d'autres opérateurs. Le droit à la portabilité des numéros de téléphone reposait déjà sur le fondement de la libre concurrence[1610]. En réalité, le droit à la portabilité a une première composante, qui est de permettre à son titulaire de transférer ses données à un concurrent de son prestataire initial, ce qui doit favoriser le développement des marchés de données[1611]. Cela « *permet à un utilisateur de quitter un service qui abrite ses données pour une alternative plus séduisante en un minimum de temps* »[1612]. Les titulaires du droit à la portabilité ne sont donc plus prisonniers d'une relation contractuelle. Le droit à la portabilité sert de contre-pouvoir à la réservation économique[1613] des données, puisqu'il met « *fin aux silos qui enferment leurs clients dans une interface, une politique de confidentialité ou une base de données dont ils ne pourront plus jamais sortir* »[1614]. Il permet aux cocontractants générateurs de données de choisir leurs

[1610] LEDGER, M. et TOMBAL, T., « Le droit à la portabilité dans les textes européens ; droits distincts ou mécanisme multi-facettes ? », *RDTI*, n°72, 2018, pp. 25 à 44.
[1611] ZOLYNSKI, C., « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », *op. cit.* : « *La portabilité de ces données industrielles favoriserait le développement des différents marchés concernés en encourageant la concurrence entre fournisseurs de services et de solutions* ».
[1612] NETTER, E., « La portabilité, un droit à inventer », *Dalloz IP/IT*, 2020, n°352, 20 juin 2020.
[1613] MOUSSERON, J.-M. et VIVANT, M., « Les mécanismes de réservation et leur dialectique : le "terrain" occupé par le droit », *op. cit.*
[1614] NETTER, E., « La portabilité, un droit à inventer », *op. cit.*

partenaires commerciaux sur le fondement de la liberté d'entreprendre[1615]. Ce n'est qu'à cette condition que les entreprises peuvent jouir d'une compétition ouverte protégée par la liberté de la concurrence. Ainsi, les utilisateurs de données qui sont également fournisseurs peuvent au moyen du droit à la portabilité changer d'opérateur de manière rapide et gratuite. Pour cela, les données ne doivent pas nécessairement transiter par l'utilisateur, elles peuvent être transférées directement d'un opérateur à un autre. Sur ce point, la Proposition de règlement sur les données a pour objectif de créer un cadre pour le changement de fournisseur grâce à l'interopérabilité et la portabilité.

2. Favoriser les possibilités de multidomiciliation

602- Le droit à la portabilité offre la possibilité d'une multi-domiciliation des données qui pourraient être stockées chez plusieurs prestataires en même temps selon les besoins de l'utilisateur. Par conséquent, la portabilité des données est également vectrice d'innovation puisque « *de nouveaux services tiers fondés sur le croisement de plusieurs sources de données pourraient se développer grâce à la portabilité* »[1616]. Néanmoins, la portabilité ne doit pas être limitée aux données permettant d'assurer la continuité du service, elle devrait porter sur toutes les données générées ou fournies lors de la relation contractuelle.

B. Le renforcement de la maîtrise de l'usage des données non personnelles

603- Le droit à la portabilité doit permettre aux exploitants agricoles de récupérer les données générées par les objets connectés (**1**) afin de rééquilibrer l'asymétrie de pouvoir dans les contrats de l'agriculture numérique (**2**).

1. Récupérer des données générées par les objets connectés

604- Le droit à la portabilité dispose d'une seconde composante qui est de permettre aux utilisateurs-producteurs de données de récupérer les données qu'ils génèrent afin d'en faire usage eux-mêmes. Cet instrument est un complément au droit d'accès[1617] qui favorise la maîtrise juridique

[1615] ZOLYNSKI, C. et LE ROY, M., « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *Légicom*, n°59, 2017/2, pp. 105 à 113.
[1616] *Ibid.*
[1617] RGPD, art. 15 ; LEDGER, M. et TOMBAL, T., « Le droit à la portabilité dans les textes européens : droits distincts ou mécanisme multi-facettes ? », *op. cit.*

des données. En effet, il « *permet aux entreprises de récupérer l'intégralité des données générées et qui sont stockées et/ou traitées chez un fournisseur de services numériques [...]* »[1618]. Ainsi, la portabilité offre la possibilité pour l'utilisateur de récupérer les données qu'il a générées par l'utilisation d'un service ou d'un produit[1619], libre à lui ensuite d'en faire ce qu'il en souhaite.

2. Rééquilibrer l'asymétrie de pouvoirs entre utilisateurs et services de l'économie numérique

605- Au sujet du droit à la portabilité, Mme la professeure C. Zolynski et Mme Le Roy évoquent un « *instrument de rééquilibrage de l'asymétrie de pouvoirs entre utilisateurs et services de l'économie numérique* »[1620]. La portabilité permet donc à la fois « *de limiter les effets de verrouillage concurrentiel* » et « *de favoriser l'innovation en permettant aux participants des écosystèmes de bénéficier d'offres de services différenciés, mais performants* »[1621]. Par conséquent, le droit à la portabilité permet aux utilisateurs de changer de fournisseur de services librement et sans obstacle financier ou technique. Ce droit couteau suisse « *constitue [donc] un outil de maîtrise de données autant que de circulation* »[1622].

§2. *Les contours du droit de contrôle de l'usage des données d'exploitation*

606- Les contours du droit de contrôle de l'usage des données d'exploitation supposent d'envisager, tout d'abord, le titulaire et le débiteur de ce droit (**I**), pour ensuite en étudier l'objet (**II**).

I. Le titulaire et le débiteur du droit de contrôle de l'usage des données d'exploitation

607- Il est nécessaire d'étudier, tout d'abord, le titulaire (**A**), pour ensuite envisager le débiteur du droit de rendre accessibles et utilisables les données (**B**).

[1618] ZOLYNSKI, C. et LE ROY, M., « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *op. cit*.
[1619] ZOLYNSKI, C., « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », *op. cit.*
[1620] ZOLYNSKI, C. et LE ROY, M., *op. cit.*
[1621] MARTY, F., « Accès aux données, coopétition intra-plateforme et concurrence inter-plateformes numériques », *Revue d'économie industrielle*, 2020/1, n°169, pp. 221 à 246.
[1622] CARRE, S., « Libre circulation des données, propriété et droit à l'information (1) : à propos du règlement (UE) 2018/1807 du 14 novembre 2018 », *op. cit.*

A. Le titulaire du droit de contrôle de l'usage

608- Si la Commission européenne retient la notion d'« utilisateur » dans sa Proposition de règlement (**1**), il apparaît plus opportun de retenir la notion de « co-contractant générateur de la donnée » (**2**).

1. La notion d'« utilisateur » retenue par la Commission européenne

609- **Définition de l'utilisateur.** La Commission européenne a retenu la notion d'utilisateur (« *user* ») dans sa Proposition de règlement sur les données pour identifier la personne qui détient les droits sur les données industrielles. Elle définit l'utilisateur comme « *une personne physique ou morale qui possède ou loue un produit ou reçoit un service* »[1623], ce qui renvoie aux utilisateurs d'objets connectés et de services. La définition retenue de la notion de « produit »[1624] dans le règlement renvoie à la notion d'objets connectés.

610- **Les limites de la notion.** La notion d'« utilisateur » est étendue puisqu'elle peut concerner toute personne qui utilise la machine ou le logiciel. D'éventuels conflits peuvent naître d'une telle notion puisque plusieurs personnes pourraient revendiquer cette qualité entre celle qui a acheté l'objet connecté, celle qui le loue et celle qui l'utilise. Par exemple, dans le secteur agricole, un entrepreneur de travaux agricoles peut faire une récolte chez un agriculteur au moyen de sa propre moissonneuse-batteuse et récupérer des données de rendement du champ de l'agriculteur. Dans ce cas, l'entrepreneur de travaux agricoles en tant qu'utilisateur de l'objet connecté détiendrait les droits d'accès et d'usage sur ces données. Pourtant, les données sont bien issues de l'exploitation agricole. L'agriculteur est dans ce cas en dehors de la relation entre l'entrepreneur de travaux agricoles et le prestataire de services et ne serait donc pas considéré comme l'utilisateur de l'objet connecté au sens de la Proposition de règlement sur les données.

[1623] Règlement sur les données, préc., art.2.

[1624] *Ibid.* : « *Un objet mobilier corporel, y compris lorsqu'il est incorporé dans un bien immeuble, qui obtient, génère ou recueille des données concernant son utilisation ou son environnement, qui est en mesure de communiquer des données par l'intermédiaire d'un service de communications électroniques accessible au public et dont la fonction première n'est pas le stockage et le traitement de données* ».

2. La notion envisagée de co-contractant générateur de la donnée

611- La notion de « *co-contractant générateur de la donnée* » a été proposée par le CNNum[1625] pour identifier le titulaire du droit à la portabilité[1626]. Elle a été reprise par la doctrine[1627] qui ne l'a pas encore définie. Cette notion peut être envisagée afin d'identifier le futur titulaire du droit d'usage sur les données. En décomposant l'expression, deux notions apparaissent qui induiront le régime juridique applicable au droit à la portabilité, d'abord celle de « co-contractant », ensuite, celle de « générateur de la donnée ».

612- Définition de co-contractant. Le co-contractant est défini comme « *la partie avec laquelle on contracte* »[1628]. Ainsi, le droit à la portabilité et le droit de contrôle de l'usage naissent du contrat conclu entre une ou plusieurs parties. Le contrat répond aux conditions de validité de l'article 1108 du Code civil : les parties doivent être capables de contracter, avoir donné leur consentement et le contrat doit avoir un contenu certain et licite. Ce n'est qu'à cette condition que le contrat sera valable et pourra exercer ses effets entre les parties.

613- Contrat à distance. Dans le secteur agricole, un grand nombre de contrats est conclu en ligne. Le contrat peut donc prendre plusieurs formes, il peut s'agir d'un contrat de vente de matériel assorti à un abonnement assurant l'accès à une plateforme ou à une application. De même, dès lors que l'agriculteur accepte des conditions générales d'utilisation pour accéder à une plateforme, il sera engagé dans une relation contractuelle avec cette dernière. Néanmoins, les tiers au contrat ne pourront pas bénéficier du droit à la portabilité ou du droit d'usage puisqu'il s'agit d'un droit relatif et personnel qui naît de la relation contractuelle entre l'exploitant agricole et son partenaire. Par conséquent, la désignation du co-contractant ne pose pas de difficulté lorsque l'agriculteur acquiert ou loue le matériel agricole ou utilise le service de collecte de données et qu'il réalise lui-même ses travaux agricoles. En revanche, dans le cas de la réalisation des travaux par un tiers, il sera nécessaire de préciser dans un contrat qui, de l'entrepreneur de travaux agricoles, par exemple, ou de l'agriculteur, détient les droits sur les données produites ou collectées. En effet, lorsque l'agriculteur a recours à une prestation de services pour la réalisation de travaux agricoles, il est identifié dans le contrat qui le lie avec l'entrepreneur comme le maître d'œuvre et l'entrepreneur comme le prestataire de services. Ainsi, un contrat tripartite devrait être établi entre le fournisseur de matériels, l'agriculteur et

[1625] Conseil National du Numérique.
[1626] NETTER, E., « La portabilité, un droit à inventer », *op. cit.*, p. 1.
[1627] ZOLYNSKI, C. et LE ROY, M., « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *op. cit*.
[1628] GUILLIEN, R. et VINCENT, J., *Lexique des termes juridiques*, Dalloz, 16e éd., 2007, p. 125.

l'entrepreneur afin de désigner l'agriculteur comme la personne qui détient les droits sur les données collectées lors de la prestation de services réalisée par l'entrepreneur de travaux agricoles.

614- **Notion de « générateur de la donnée ».** Le droit de contrôle de l'usage est un droit personnel qui naît du contrat. Néanmoins, la question qui se pose est de savoir lequel des co-contractants bénéficie de ce droit. Le CNNum précise qu'il s'agit du « *générateur de la donnée* ». Ici, le CNNum s'éloigne des notions juridiques pour caractériser la personne qui génère la donnée. En effet, la seule occurrence en droit est le « fait générateur » qui est défini comme un « *événement qui déclenche la mise en œuvre d'une situation juridique* »[1629]. Il s'agit alors de se demander ce que signifie concrètement « générer la donnée ». Mais aussi, qui génère la donnée ? S'agit-il de l'entreprise qui a fabriqué le matériel qui collecte la donnée, du fournisseur de services qui a créé le logiciel, de l'entrepreneur qui réalise les travaux agricoles pour l'agriculteur ou bien encore de l'exploitant agricole qui utilise ces outils sur son exploitation ? Pour toute réponse, le CNNum fournit un exemple afin d'agrémenter la notion de co-contractant générateur de données. Selon lui, il s'agit de « *l'entreprise qui a contracté avec un fournisseur de service numérique afin de mettre en œuvre un dispositif pour générer de la donnée* »[1630]. Ainsi, la notion de générateur doit être entendue selon la définition du dictionnaire Larousse qui définit la notion de « générer » comme ce « *qui est la source, la cause de quelque chose* ». Le générateur des données est donc le co-cocontractant qui est à la source des données. Par conséquent, c'est celui qui par son activité, qu'il réalise lui-même ou qu'il confie à un autre, génère les données au moyen du dispositif mis en place au moyen d'un contrat conclu avec un fournisseur de services numériques ou un fournisseur de matériels. Le co-contractant générateur des données, dans le cadre de l'agriculture numérique, est donc l'exploitant agricole qui souscrit des contrats de prestations de services et/ou d'acquisition de matériels auprès de prestataires, ses co-contractants, afin de réaliser une prestation, qui peut être la fourniture d'un outil d'aide à la décision, l'accès à une application, etc. Les données d'exploitation sont la matière permettant la réalisation de ces prestations. En revanche, dans le cadre d'une prestation de service de réalisation de travaux agricoles, l'agriculteur est celui qui fait réaliser les travaux sur son exploitation par un tiers, l'entrepreneur de travaux agricoles réalise donc les travaux au

[1629] *Ibid.*, p. 300.

[1630] CNNum, *La consécration d'un droit à la portabilité des données non personnelles*, repris par ZOLYNSKI, C. et LE ROY, M., « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *op. cit.* : « *Par exemple, dans le cas des données produites par un capteur dans un bâtiment intelligent, le titulaire du droit à la portabilité serait celui qui génère la donnée et non l'installateur du dispositif ou son fabricant* ».

nom et pour le compte de l'agriculteur. Par conséquent, l'agriculteur qui confie ses travaux agricoles à un tiers — l'entrepreneur — est celui dont l'activité génère les données et peut être considéré comme le co-contractant générateur des données. Ces éléments devront être précisés dans le contrat tripartite qui lie l'entrepreneur de travaux, l'agriculteur et le fournisseur de matériels et/ou de services.

B. Le débiteur de l'obligation

615- La Commission européenne désigne le « détenteur de données » comme le débiteur de l'obligation de rendre accessibles les données. En effet, l'article 2 de la Proposition de règlement sur les données définit le détenteur de données comme étant « *une personne morale ou une personne physique qui […] a le droit ou l'obligation, ou dans le cas des données à caractère non personnel et par le contrôle de la conception du produit et des services liés, a la possibilité, de rendre disponibles certaines données à caractère personnel* ». Il semble donc que les entreprises, qui conçoivent des produits et qui fournissent des services liés dont l'utilisation par « l'utilisateur » génère des données, seront soumises à cette future réglementation. Aussi, les entreprises de l'agriculture numérique qui conçoivent des objets connectés et des services de collecte et d'exploitation des données agricoles à l'attention des agriculteurs, tels que SMAG, ou ITK par exemple, y seraient également soumises.

II. L'objet du droit de contrôle de l'usage des données d'exploitation

616- Le Règlement sur les données définit la notion de « donnée » à l'article 2 comme « *toute représentation numérique d'actes, de faits ou d'information et toute compilation de ces actes, faits ou informations, y compris sous forme d'enregistrement sonore, visuel, ou audiovisuel* ». Ce Règlement a vocation à s'appliquer à l'ensemble des données non personnelles industrielles produites par des objets connectés à l'Internet des objets (IOT)[1631]. Cependant, il ne distingue pas selon le niveau d'enrichissement des données. Certaines données devraient pourtant faire l'objet d'une protection particulière tandis que d'autres doivent circuler pour favoriser l'investissement. Ces différences doivent conduire à l'application d'un droit granulaire afin

[1631] *Ibid.*, p. 1 : « *Faire en sorte que la valeur des données soit répartie de manière mieux équilibrée et compatible avec la nouvelle vague de données industrielles à caractère non personnel et la prolifération des produits connectés à l'internet des objets reviendra à tirer parti de l'énorme potentiel existant pour stimuler une économie durable fondée sur les données en Europe* ».

d'offrir un régime sur mesure aux données plus ou moins ouvertes ou plus ou moins protégées. Le droit de contrôle de l'usage des données doit permettre de protéger les données selon leur niveau de sensibilité tout en assurant la circulation et la maîtrise des données brutes non personnelles. Il faut donc distinguer les données selon leur niveau d'enrichissement (**A**), mais aussi selon leur sensibilité (**B**).

A. La circulation et la maîtrise des données selon leur niveau d'enrichissement

617. Le Règlement sur les données ne distingue pas selon le niveau d'enrichissement des données. Or, la catégorie des données à caractère non personnel rassemble un grand nombre de données plus ou moins traitées. Il peut s'agir de données brutes produites par les machines agricoles — les données industrielles — ou encore de données saisies dans les logiciels de gestion ou enfin de données issues de traitements opérés par les fournisseurs de services. Quoi qu'il en soit, ces données ne permettent pas d'identifier ou de rendre identifiable une personne physique. Il s'agit alors de se demander si l'ensemble des données non personnelles seront soumises au Règlement sans distinction selon leur niveau d'enrichissement. Répondre à cette question suppose d'envisager, tout d'abord, l'inclusion de principe des données brutes, des données saisies et des métadonnées (**1**) pour, ensuite, porter une attention particulière à l'exclusion exceptionnelle des données enrichies (**2**).

1. L'inclusion de principe des données brutes, des données saisies et des métadonnées

618. **Principe.** Le droit de contrôle de l'usage et *a fortiori* le droit à la portabilité doivent porter sur toutes les données générées par l'activité de l'exploitant agricole au moyen des objets connectés — les données industrielles — ainsi que celles qu'il a saisies lui-même dans le cadre d'une relation contractuelle[1632].

619. **Données industrielles.** Selon le CNNum les données industrielles sont « *des données brutes collectées par des compteurs communicants* » qui sont « *générées par l'activité de l'entreprise, lorsqu'elle utilise un service ou un appareil connecté* »[1633]. La Commission européenne définit ces données comme celles « *produites par des machines […] générées sans intervention*

[1632] CNNum, *La consécration d'un droit à la portabilité des données non personnelles, op. cit.,* p. 6.
[1633] *Ibid.*
[1633] JUILLET-REGIS, H., « Quelle régulation pour les données agricoles ? », *op. cit.*

humaine directe, par des processus informatiques, des applications ou des services, ou par des capteurs qui traitent des informations reçues d'équipements, de logiciels ou de dispositifs virtuels ou réels »[1634]. Par conséquent, toutes les données non personnelles produites par des machines[1635] lors de l'activité de l'exploitant agricole et qui n'ont fait l'objet d'aucune forme de traitement[1636] par un prestataire intègrent la notion de données industrielles.

620- **Données saisies et métadonnées.** Le droit de contrôle de l'usage devrait concerner également les données saisies directement par l'exploitant agricole dans les logiciels de traitement de données. Dans ce sens, le CNNum inclut dans le champ d'application du droit à la portabilité toutes les données « *déclarées activement et consciemment par l'entreprise telles que les données fournies pour créer un compte en ligne* »[1637], et qui ne permettraient pas d'identifier une personne physique. Le CNNum évoque également les métadonnées d'utilisation du service pour les inclure dans le champ d'application du droit à la portabilité puisqu'elles permettent de contextualiser les données[1638]. Pour ces raisons, toutes ces données devraient également être incluses dans le droit de contrôle de l'usage.

2. L'exclusion des données enrichies

621- **Problématique.** Dans le Règlement sur les données, le législateur européen a retenu une définition très large de la donnée et vise directement les données industrielles. Ce qui laisse supposer que la Proposition de règlement ne s'appliquerait qu'aux données brutes. Pourtant, le droit a toujours jusqu'alors fait prévaloir l'investissement sur la provenance des données pour fonder la reconnaissance d'un droit de propriété. Dans le même sens, au sujet du droit à la portabilité, le CNNum propose d'exclure de son champ d'application les données enrichies significativement.

622- **Définition des données enrichies.** Toutes les données traitées, analysées, améliorées ou agrégées par le fournisseur de services ou le fabricant de matériels sont des données enrichies. Elles doivent être distinguées des données industrielles. Cette distinction avait déjà été retenue dans la Loi pour une République numérique de 2016 s'agissant du droit à la portabilité en faveur des consommateurs[1639]. L'article L. 224-42-3 du Code de la consommation qui avait codifié

[1634]Commission européenne, *Créer une économie européenne fondée sur les données,* préc., art. 3.1.
[1635] Zolynski, C., « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », *op. cit.*
[1636] JUILLET-REGIS, H., « Quelle régulation pour les données agricoles ? », *op. cit.*
[1637] CNNum, *La consécration d'un droit à la portabilité des données non personnelles, op. cit*., p. 6.
[1638] *Ibid.*
[1639] LRN, art. 48, abrogé par la Loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles.

l'article 48 de la Loi Informatique et Libertés de 1978[1640] prévoyait que les données enrichies significativement par le fournisseur de services sont exclues du droit à la portabilité, ainsi que les données dont la divulgation porterait préjudice à un secret des affaires et aux droits de la propriété intellectuelle[1641]. Par conséquent, toutes les données qui faisaient l'objet d'un secret des affaires, celles qui avaient été enrichies de manière significative ou celles qui étaient revêtues d'un caractère original dans leur disposition étaient exclues du champ d'application du droit à la portabilité. Cette exclusion a pour objet de préserver le travail et l'investissement de l'entreprise qui a fourni des moyens financiers, matériels et humains pour obtenir ces données enrichies et lui permettre de bénéficier d'un droit *sui generis* sur les bases de données qu'il produit[1642].

623- **Exclusion des données enrichies.** Certains auteurs proposent d'exclure les données enrichies d'un éventuel droit sur les données non personnelles. Notamment, Mme H. Juillet-Régis propose d'exclure les données « *traitées ou agrégées* » qu'elle définit comme des « *données manipulées, classées, combinées entre elles le cas échéant, et dont une ou plusieurs informations supplémentaires peuvent ainsi en être extraites* »[1643]. Ces données sont qualifiées de données primaires par les acteurs de l'agriculture numérique qui en retiennent la définition suivante : « *information issue de l'expertise ou de l'analyse d'une Donnée agricole brute et/ou information élaborée à partir d'une Donnée agricole brute* »[1644], ou de « *données brutes transformées en valeurs identifiables par d'autres personnes (traitement primaire). Par exemple, données de champ (parcelles, données géologiques, données sur les sols, l'eau, les cultures, la production — données relatives à une exploitation spécifique)* »[1645]. Néanmoins, il faut noter que ces données restent soumises au droit de la concurrence, au secret et à la propriété intellectuelle[1646]. C'est pourquoi, il peut être considéré comme anticoncurrentiel de transmettre des données enrichies à des fins d'utilisation par un concurrent[1647].

624- **Champ d'application de l'enrichissement significatif.** La question se pose de savoir quel type d'enrichissement doit permettre d'exclure les données enrichies du droit de contrôle de

---

[1640] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : *JORF* du 7 janvier 1978.
[1641] ZOLYNSKI, C. et LE ROY, M., « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *op. cit.* ; C. conso., art. L. 224-42-3 ; LRN, *id.*, art. 48 relatif à la portabilité et la récupération des données.
[1642] Voir *supra*, n°218 et s.
[1643] JUILLET-REGIS, H., « Quelle régulation pour les données agricoles ? », *op. cit.*
[1644] FNSEA et JA, *Valoriser et sécuriser les données des exploitations agricoles dans les contrats* et Charte Data-agri, préc.
[1645] COPA COGECA, *Code de conduite de l'UE relatif au partage des données agricoles par accord contractuel*, préc.
[1646] *Ibid.*
[1647] PELLEGRINI, F., « La portabilité des données et services », *RFAP*, n°167, 2018/3, pp. 513 à 523.

l'usage. En effet, la collecte et le traitement des données s'apparentent à une prestation de services pour l'exploitant agricole qu'il rémunère à l'entreprise collectrice. L'objectif d'une telle transaction est pour lui d'obtenir des informations précieuses pour ses activités agricoles. L'entreprise obtient en échange le paiement d'un abonnement et des données qui lui sont utiles afin d'améliorer les outils d'aides à la décision, les objets connectés ou encore les logiciels qu'elle fournit.

En premier lieu, il est primordial de déterminer ce qui est entendu par « *enrichissement significatif* » afin de préciser, en second lieu, les contours du champ d'application du droit de contrôle de l'usage des données non personnelles. L'absence de définition des données enrichies serait source d'insécurité juridique, chacun pouvant définir selon ses propres intérêts le terme « *significatif* ». La frontière entre données enrichies significativement et simplement enrichies pourrait être tracée en tenant compte de la qualification des données, leur analyse, leur transformation ou encore leur agglomération.

625- **Discussion de l'inclusion des données contenues dans les bases de données.** Une première limite existe en ce qui concerne l'agglomération des données sous l'empire du droit *sui generis* des bases de données. En effet, le législateur a créé le régime du droit *sui generis* des bases de données notamment pour déterminer la personne qui détient les droits sur la base. Ce régime spécifique permet de contourner la difficulté d'application de la théorie de l'accession aux bases de données et de déterminer légalement le titulaire des droits sur cette base. Le droit *sui generis* des bases de données évite l'écueil de la théorie de l'accession par exemple qui suppose que dès lors que « *des meubles appartenant à des propriétaires différents se trouvent unis, la loi règle la propriété de la chose ainsi créée sur le fondement de la règle de l'accessoire* »[1648]. En l'absence de régime spécifique, lorsque des données sont agglomérées dans une base de données, la balance devrait donc être faite entre le producteur de la base et les titulaires initiaux des droits sur les données qui y sont incluses. Cette théorie de l'accession permet d'attribuer au propriétaire de la chose principale le produit de l'union. De ce fait, si la création d'un produit à partir de la chose d'autrui entraîne en principe l'attribution du produit au propriétaire de la matière[1649], il en va différemment dès lors que la main-d'œuvre « *surpasse de beaucoup [sa] valeur* »[1650]. Dans ce cas, le produit final revient au spécificateur qui est tenu d'indemniser le

[1648] REVET, T. et ZENATI-CASTAING, F., *Les biens*, 3e éd., PUF, 1997, n°319, p. 213.
[1649] C. civ., art. 570 : « *Si un artisan ou une personne quelconque a employé une matière qui ne lui appartenait pas à former une chose d'une nouvelle espèce, soit que la matière puisse ou non reprendre sa première forme, celui qui en était le propriétaire a le droit de réclamer la chose qui en a été formée en remboursant le prix de la main-d'œuvre estimée à la date du remboursement* ».
[1650] REVET, T. et ZENATI-CASTAING, F., *Les biens*, *op. cit.*, n°140, p. 215.

propriétaire de la matière[1651] et dont la responsabilité peut être engagée[1652]. En échange de quoi le propriétaire initial de la matière perd tous droits sur celle-ci. Par conséquent, pour faire application du droit de l'accession aux bases de données, il aurait fallu distinguer celles pour lesquelles l'investissement dépasse la valeur des données qui y sont incluses, et inversement. En application du droit des biens, le producteur de la base serait alors tenu d'indemniser chacun des individus dont les données sont contenues dans la base et « déposséderait » de leur « droit » les détenteurs originaux des données brutes. Aussi, afin de déterminer de manière automatique le titulaire du droit sur la base de données et d'éviter l'écueil de la théorie de l'accession, le législateur a introduit le droit *sui generis*. Ce droit a donc permis de clarifier le régime applicable aux bases de données en identifiant directement le producteur de la base. Par conséquent, le producteur de la base détient de fait la maîtrise de l'usage des données incluses dans sa base sans avoir à indemniser les éventuels détenteurs originaux des données. Néanmoins, le législateur dans le Règlement sur les données de 2022 envisage de modifier cette réglementation en rendant inapplicable le droit *sui generis* sur les bases de données contenant des données obtenues ou générées par des objets connectés ou des services[1653]. Cette disposition permet de faire prévaloir la provenance des données et le droit des co-contractants générateurs de données sur celui des producteurs de bases de données. Le droit *sui generis* des bases de données ne s'appliquerait donc plus aux données industrielles et le générateur des données aurait, par principe, le droit d'accéder et d'utiliser les données agrégées dans la base contenant les données qu'il a générées au moyen de l'objet connecté qu'il utilise. Cela permettrait notamment de limiter les possibilités de réservation des données par les entreprises détentrices de données. Cette inclusion des données agrégées dans le droit d'accès et d'utilisation par le législateur européen permettrait également de favoriser la maîtrise de l'usage, mais aussi d'encourager la circulation et la valorisation des données industrielles.

626- **Droit au dividende de la donnée.** Une seconde question se pose au sujet des données enrichies intrinsèquement. Les données qui ont été traitées, analysées ou encore affinées entrent-elles dans le champ d'application du droit de contrôle de l'usage des données non personnelles ? Il s'agit donc de se demander si le savoir-faire de l'entreprise qui a enrichi intrinsèquement et de

---

[1651] C. civ., art. 571 : « *Si, cependant, la main-d'œuvre était tellement importante qu'elle surpassât de beaucoup la valeur de la matière employée, l'industrie serait alors réputée la partie principale, et l'ouvrier aurait le droit de retenir la chose travaillée, en remboursant au propriétaire le prix de la matière, estimée à la date du remboursement* ».

[1652] C. civ., art. 577 : « *Ceux qui auront employé des matières appartenant à d'autres, et à leur insu, pourront aussi être condamnés à des dommages et intérêts, s'il y a lieu, sans préjudice des poursuites par voie extraordinaire, si le cas y échet* ».

[1653] Règlement sur les données, préc., art. 35.

manière significative les données par leur traitement, leur analyse ou encore leur affinage doit prévaloir sur l'origine des données et les droits des co-contractants générateurs des données. Pour répondre à cette question, il faut se référer au droit civil. Au titre de l'accession par spécification de l'article 570 du Code civil, celui qui détient des droits sur la matière obtient la chose ainsi créée sauf si la main-d'œuvre surpasse de beaucoup la valeur de cette matière[1654]. Or, il est bien difficile d'établir la valeur de la main-d'œuvre sur le traitement d'une donnée ou même d'un ensemble de données. Les données n'ont de valeur que par leur usage, souvent, futur. En revanche, si la collecte et la production d'une donnée ne constituent pas un important volume de travail (« *le coût marginal [de la création d'une donnée]* s*'approche de zéro* »[1655]), la qualification des données, leur analyse et leur visualisation font considérablement augmenter la valeur de cette main-d'œuvre[1656]. Dans une telle situation, le spécificateur — le fournisseur de services — qui a créé la chose nouvelle, en l'occurrence les données transformées ou enrichies, devrait indemniser le propriétaire de la matière[1657] et obtenir des droits sur le résultat de son travail. Par conséquent, il semble que la question de la détention des droits sur les données enrichies de manière intrinsèque se pose dans les mêmes conditions que dans le cadre de leur agglomération dans des bases de données. À ce propos, Mme la professeure V.-L. Benabou propose de reconnaître « *un droit au dividende de la donnée* »[1658] pensé comme un apport en société. Cela permettrait, lorsqu'il y a un « *accroissement de la valeur liée à la donnée intrinsèque* » ou que la donnée a été « *mise en relation avec d'autres données au sein de cet ensemble* » que « *chacun dispose d'un droit sur la valeur d'ensemble créée* »[1659]. Ce qui permettrait entre autres dans le cadre d'un droit à la portabilité par exemple « *d'envisager le retrait de l'apport* »[1660]. Mais il faut relever néanmoins les difficultés de mise en œuvre technique d'un tel retrait. Le Règlement sur les données reste muet sur cette problématique. Pourtant, il semble que l'enrichissement intrinsèque des données doit relever du savoir-faire de l'entreprise qui valorise ces données. Par conséquent, le droit au dividende semble être un bon compromis afin de permettre aux co-contractants générateurs des données de récupérer celles qui sont brutes ou enrichies simplement et de laisser le résultat du travail de valorisation aux fournisseurs de services.

[1654] C. civ., art. 571.
[1655] CHIGNARD S. et BENYAYER L. -D., *Datanomics, op. cit.*, p. 42.
[1656] *Ibid.*
[1657] C. civ., art. 571.
[1658] BENABOU, V.-L., « Essai de prospective juridique sur les modes de valorisation des données : fonds informationnel, droit à la portabilité et dividende de la donnée », *op. cit.*, n°9, p. 201.
[1659] *Ibid.*, n°9, p. 202.
[1660] *Ibid.*

627- **Droit des contrats.** Dans l'attente de la reconnaissance d'un véritable droit sur les données enrichies, le droit des contrats permet de combler l'absence de règles impératives sur la question de la maîtrise de ces données. Ainsi, une chaîne de contrats, sous forme de blockchain[1661] par exemple, pourrait « *assurer une gestion optimisée des données par une organisation raisonnée de leurs usages* »[1662]. Pour cela, chaque personne dans la chaîne de valeur devrait pouvoir exploiter les données selon ses besoins sans pouvoir outrepasser ses droits.

B. La protection des données sensibles d'exploitation

628- Le Règlement sur les données de 2022 ne permet pas de faire de distinction entre les données sensibles et les données normales d'exploitation. En effet, le législateur a pris le parti de définir largement les données à caractère non personnel. Il a ainsi reconnu par principe un droit d'accès et un droit d'utilisation sur toutes les données industrielles sans distinguer les différents types de données existants. Pourtant, il semble que la proposition de différencier les données sensibles des données normales devrait faire l'objet d'un développement. Cette proposition a été faite par Mme H. Juillet-Régis qui envisage d'accorder une protection particulière aux données sensibles à caractère non personnel[1663]. Aussi, il faut opérer la distinction entre les données incluses dans la catégorie des données sensibles (**1**) de celles qui en sont exclues (**2**).

1. Les données sensibles d'exploitation

629- **Données agricoles sensibles.** Une protection particulière doit être envisagée pour les données sensibles d'exploitation. Il est nécessaire avant toute analyse de définir la notion de « données sensibles », afin d'identifier le champ d'application de cette protection. Or, il n'existe pas de définition unique du terme « sensible », la notion change selon la matière.

Le RGPD définit la notion de « données sensibles » comme « *une catégorie particulière de données à caractère personnel* »[1664]. Il s'agit des données qui « *engendrent un risque élevé pour les droits et libertés des personnes concernées* »[1665]. L'article 9 du RGPD précise ainsi que l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou

[1661] Voire *infra*, n°751.
[1662] ROBIN A., « Agriculture numérique, données et droit : topographie juridique de l'"écosystème informationnel vert" », *op. cit.*
[1663] JUILLET-REGIS, H., « Quelle régulation pour les données agricoles ? », *op. cit.*
[1664] RGPD, cons.10.
[1665] RGPD, cons. 91.

philosophiques ou l'appartenance syndicale, ainsi que les données génétiques, biométriques, celles concernant la santé ou encore la vie sexuelle ou l'orientation sexuelle d'une personne physique sont des données sensibles. Le RGPD interdit le traitement de ces données.

Sur le terrain du droit public, le Règlement sur la gouvernance des données de 2022[1666] prévoit que les données commercialement sensibles, les données couvertes par le secret statistique, les données protégées par le droit de la propriété intellectuelle détenues par des tiers y compris les secrets d'affaires et les données personnelles non accessibles en vertu d'une législation nationale ou de l'Union européenne particulière doivent être protégées. Par conséquent, ces données qui figurent dans des bases de données publiques ne peuvent pas être rendues accessibles même pour des activités de recherche ou d'innovation.

Sous l'angle du droit de la concurrence, sont considérées comme sensibles les informations dont le partage « *permet aux entreprises de prendre connaissance des stratégies de marché de leurs concurrents actuels ou potentiels* »[1667] (prix futurs, coûts de production, quantités, chiffres d'affaires, capacités). Aussi, le Règlement sur la gouvernance des données préconise pour les prestataires de services de prendre des mesures afin de veiller au respect du droit de la concurrence.

Également, la Chambre du commerce et de l'industrie a défini les données industrielles sensibles comme celles portant sur la propriété industrielle, les secrets des affaires ou encore « *toutes informations pouvant porter atteinte à la position concurrentielle de l'entreprise* »[1668].

Au vu de ces éléments, il apparaît donc que la notion de « données sensibles » recouvre de nombreuses réalités. Une définition trop précise aurait pour conséquence de rendre le droit de contrôle de l'usage inapplicable, alors qu'une définition trop large pourrait freiner l'innovation et le partage des données. Il serait ainsi potentiellement possible de définir la notion de « données sensibles » dans le cadre de l'agriculture numérique comme celles dont le traitement ou le partage auront pour effet de porter atteinte aux intérêts de l'exploitation que ce soit sur le terrain du commerce ou de la concurrence. Par exemple, les données sur les méthodes d'élevage ou sur les techniques culturales pourraient relever de la catégorie des données agricoles sensibles.

630- **Indifférence du niveau de traitement des données agricoles sensibles.** La question se pose de savoir si la catégorie des données sensibles devrait se limiter aux seules données brutes ou

[1666]Règl. n°2022/868 du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données) : *JOUE* L 152/1 du 3 juin 2022, cons. 6.
[1667] *Ibid.*, cons. 29
[1668] CCI, *Industrie du futur, Pratiques et attentes des entreprises françaises en matière de partage des données industrielles,* oct. 2021.

bien si elle devrait s'étendre à toutes les données même traitées du moment qu'elles contiennent des informations sensibles. Si la question de l'agglomération a pu être envisagée dans le développement précédent[1669], les données sensibles qui seront agglomérées dans une base de données excluront l'application du droit *sui generis* du producteur de bases de données. En revanche, s'agissant du droit au dividende des données, la question se pose de savoir si l'entreprise qui a enrichi les données de manière intrinsèque pourrait s'opposer aux droits de l'agriculteur sur ses données sensibles. Il apparaît que la protection des données sensibles devrait englober l'ensemble des données qu'elles soient brutes ou enrichies. En effet, le caractère sensible des informations contenues dans les données devrait être supérieur aux intérêts des prestataires de services et de leur savoir-faire. Ces données devraient donc être contrôlées par l'exploitant agricole tout au long du processus de leur collecte à leur traitement jusqu'à leur suppression. Il faudra néanmoins déterminer au préalable, au moyen d'un contrat, les données sensibles de l'exploitation dont le traitement pourrait porter préjudice à l'exploitant. Il faudra également distinguer la sensibilité des données selon les différents types de traitement.

2. Les données non protégées

631- **Limites de la catégorie des données sensibles d'exploitation.** La catégorie des données sensibles est limitée. Sont ainsi exclues les données dites « normales » de l'exploitation et les données d'intérêt général.

La protection des données sensibles ne devrait pas porter sur les données normales d'exploitation[1670]. Par opposition aux données sensibles, les données normales d'exploitation sont toutes les données non personnelles dont le traitement ne porte pas atteinte aux intérêts des agriculteurs. Il s'agit donc de toutes les données qui relèvent des informations « banales » sur les exploitations et qui ne relèvent pas d'un secret des affaires déterminé au préalable par l'exploitant agricole.

En ce qui concerne les données dont l'information est d'intérêt général, une balance devrait être faite entre la protection des données sensibles et l'intérêt général. Les données phytosanitaires[1671] sont un bon exemple de données dont le traitement et le partage peuvent porter atteinte aux intérêts des agriculteurs. La diffusion de ces informations peut potentiellement entraîner une perte de revenus pour l'agriculteur qui utilise ces produits dans

[1669] Voir *supra*, n°625.
[1670] JUILLET-REGIS, H, « Quelle régulation pour les données agricoles ? », *op. cit.*
[1671] Voir *supra*, n°159 et s.

le cas où ces informations seraient diffusées aux consommateurs. Néanmoins, les données phytosanitaires sont des données environnementales et ont trait à la santé publique. Il convient donc, dans cet exemple, de faire primer l'intérêt général sur l'intérêt personnel des agriculteurs quand il s'agit de santé publique.

632- **Conclusion de la section.** En souscrivant des contrats de prestation de services et d'achat de matériels, les agriculteurs cèdent bien souvent le contrôle de l'usage des données de leur exploitation à leurs prestataires de services ou fournisseurs de matériels. En effet, ces derniers détiennent les données des agriculteurs et rien, pour le moment, ne les oblige à utiliser les données selon la volonté des agriculteurs. Pourtant ces derniers sont à l'origine des données et devraient pour cette raison en avoir la maîtrise. C'est pourquoi les exploitants agricoles ne devraient plus aujourd'hui rester en retrait du contrôle de l'usage des données industrielles issues de leur exploitation, au profit des entreprises qui les détiennent. Il conviendrait donc de créer, en sus du droit d'accès, un véritable droit de contrôle de l'usage des données agricoles en faveur de l'exploitant complété d'un droit général à la portabilité. Ce droit de contrôle devrait prendre en compte les différents niveaux de sensibilité des données selon les intérêts en présence, de manière fine et granulaire. Néanmoins, les données enrichies significativement par l'entreprise devraient être exclues du champ d'application du droit de contrôle de l'usage. La future consécration du Règlement sur les données présenté par le législateur européen en février 2022 devrait, dans un premier temps, offrir plus de pouvoir aux utilisateurs d'objets connectés sur les données industrielles. Par conséquent, les agriculteurs seraient immédiatement visés par ces dispositions.

Section 2. L'esquisse du droit de contrôle de l'usage des données d'exploitation non personnelles

633- La Commission européenne a affirmé qu'il était important de construire un cadre autour de la circulation des données non personnelles afin « *[d']accroître l'accès et l'utilisation des données* »[1672]. Des outils devraient pour cela être mis en place afin que les exploitants agricoles puissent contrôler l'usage des données issues de leur exploitation. Ces outils ne devraient pas, toutefois, entraver totalement la circulation de ces données. À cette fin, les acteurs du secteur

[1672] Commission européenne, *Créer une économie européenne fondée sur les données*, 10 janv. 2017, COM(2075) 9 final.

agricole ont, de leur côté, souhaité renforcer le consentement des agriculteurs sur le même principe que le consentement pour le traitement des données à caractère personnel, à travers le CASDAR Multipass. Aujourd'hui, la Commission européenne, par sa Proposition de règlement sur les données de 2022[1673], envisage un nouveau cadre pour les contrats portant sur l'achat ou la location d'objets connectés et des services qui y sont liés. Également, le CNNum, la doctrine, et la Commission européenne envisagent la création d'un droit général à la portabilité, intrinsèquement lié à l'interopérabilité des services. L'association de la portabilité et de l'interopérabilité permet l'échange, mais aussi, la récupération des données non personnelles. Aussi, afin d'étudier les démarches pour la construction du cadre des données non personnelles, il est nécessaire d'envisager, dans un premier temps, les propositions concernant les aspects contractuels du contrôle de l'usage (**§1**) pour, dans un second temps, se concentrer sur les aspects techniques du contrôle de l'usage (**§2**).

§1. *Les aspects contractuels du contrôle de l'usage*

634- L'accès, l'utilisation et, de surcroît, le droit de contrôle de l'usage sont des droits personnels qui reposent sur une relation contractuelle[1674]. Par conséquent, réglementer le droit de contrôle de l'usage revient à réglementer les contrats portant sur l'achat ou la location d'objets connectés et de services liés, afin de régir, plus particulièrement les contrats de l'agriculture numérique. Ces contrats étant par nature déséquilibrés, il convient d'envisager, tout d'abord, les mesures qui visent à renforcer les droits et les obligations des parties (**I**), pour ensuite, s'intéresser aux mesures qui visent à prévenir les déséquilibres contractuels (**II**).

I. Les mesures visant à renforcer les droits et les obligations des parties

635- Si les acteurs de l'agriculture numérique ont, de leur côté, développé un droit souple autour de l'utilisation des données agricoles non personnelles, aujourd'hui, un véritable droit d'utilisation est en passe d'être consacré par l'Union européenne au moyen du *Data Act*. Quelques pistes d'améliorations peuvent, néanmoins, être évoquées. Le législateur européen propose, en effet, de renforcer les obligations des « détenteurs de données » (**A**), ainsi que les droits des « utilisateurs » d'objets connectés (**B**).

[1673] Règlement sur les données, préc.
[1674] Voir *supra*, n°466 et s.

A. Le renforcement des obligations des « détenteurs de données »

636- Le législateur européen ne prévoit pas, à proprement parler, de consentement de l'utilisateur de l'objet connecté pour l'utilisation ou le partage des données. En revanche, il envisage d'exiger du détenteur des données un devoir d'information (**1**) et d'imposer des obligations quant à l'utilisation et au partage des données (**2**).

1. Le devoir d'information précontractuel

637- Transparence sur la nature, le volume et la collecte des données. Le devoir d'information répond à l'exigence de transparence imposée dans les contrats conclus entre un détenteur de données et un utilisateur d'objets connectés[1675]. La fourniture de ces informations préalables devrait conforter le consentement de l'utilisateur de l'objet connecté ou du service lié avant la conclusion du contrat. Afin d'assurer la transparence de l'usage des données, l'article 3 de la Proposition de règlement imposerait au détenteur de données de fournir à l'utilisateur d'objet connecté ou de service des informations concernant « *la nature et le volume des données susceptibles d'être générées par l'utilisation du produit ou du service lié* ». Cette information permettrait à l'utilisateur, exploitant agricole, d'avoir une vue d'ensemble des données qui seraient collectées et utilisées au cours de la relation contractuelle. Également, l'« utilisateur » devrait obtenir l'information selon laquelle les « *données sont susceptibles d'être générées en continu ou en temps réel* ».

638- Informations liées à l'accès, à l'utilisation et au partage des données. Le détenteur des données devrait tenir informé l'utilisateur sur la manière dont il « *peut accéder à ces données* ». C'est en posant le principe de l'accès aux données que l'utilisateur pourra ensuite contrôler l'usage qui en est fait, l'accès étant le préalable de l'utilisation[1676].

Le détenteur de données devrait également donner l'information selon laquelle il « *a l'intention d'utiliser lui-même les données ou d'autoriser un tiers à les utiliser et, dans l'affirmative, les finalités pour lesquelles ces données sont utilisées* ». Ces informations sont, en effet, précieuses pour l'utilisateur qui pourrait accepter ou non de conclure un contrat avec un fournisseur de matériels ou de services selon l'utilisation qu'il souhaiterait en faire. De plus, la Proposition de règlement sur les données rejoint le RGPD en imposant au détenteur des

[1675] Règlement sur les données, préc., cons. 23.
[1676] Voir *supra*, n°177.

données de prévoir, au préalable, les finalités d'utilisation des données par lui-même ou par un tiers. Le *Data Act* ne précise pas, toutefois, contrairement au RGPD, les finalités sur lesquelles le fournisseur de services peut s'appuyer. Cela laisse supposer que les finalités ne seraient pas limitées et qu'il suffirait qu'elles soient précisées à l'utilisateur. Néanmoins, compte tenu du rapport de force entre les agriculteurs et les fournisseurs de matériels et de services dans le secteur agricole, ce simple devoir d'information ne suffit pas à rééquilibrer les contrats. En effet, l'agriculteur sera, dans cette situation, souvent contraint d'accepter des finalités qui ne lui conviennent pas afin d'obtenir l'accès à un service ou pour l'achat d'un objet connecté. Aussi, il serait opportun de prévoir, au moins en ce qui concerne les données sensibles d'exploitation, qui devraient être déterminées au préalable, plusieurs droits en faveur de l'utilisateur de l'objet connecté. Ce renforcement des droits sur les données sensibles permettrait de renforcer le contrôle de l'usage des données de l'exploitation de l'agriculteur vis-à-vis de l'entreprise qui détient ces données[1677].

Le législateur européen propose dans le Règlement sur les données que le détenteur de données ait l'obligation de fournir l'information selon laquelle il est effectivement le détenteur des données ou bien si c'est un tiers qui les détient, le cas échéant, il devrait donner les informations sur ce tiers et les moyens de communiquer avec lui. Il devrait aussi fournir l'information sur « *la manière dont l'utilisateur peut demander que les données soient partagées avec un tiers* ». La Commission européenne pose donc le principe selon lequel l'utilisateur peut demander le partage des données et le changement de fournisseur. Le détenteur de données devrait également informer l'utilisateur de son « *droit d'introduire une plainte pour violation* » de ces dispositions auprès de l'autorité compétente de l'article 31.

639- **Formalisme informatif *ad validitatem*.** La Proposition de règlement sur les données envisage que les informations développées précédemment soient fournies « *avant toute conclusion d'un contrat relatif à l'achat ou à la location d'un produit ou d'un service lié* ». Ces informations seraient fournies « *sous une forme claire et compréhensible* » à l'utilisateur. Il s'agirait donc d'une obligation pour le détenteur des données de rédiger des mentions écrites obligatoires dans les contrats[1678].

640- **Limites du devoir d'information et propositions d'améliorations.** Le devoir d'information tel qu'il est décrit dans la Proposition de règlement s'arrête à la phase précontractuelle. Or, certaines informations devraient être fournies en cours de relation à l'utilisateur de l'objet

[1677] Sur les droits des utilisateurs, voir *infra*, n°646 et s.
[1678] JUILLET-REGIS, H., « Quelle régulation pour les données agricoles ? », *op. cit.*

connecté, telles que les incidents et les failles de *cybersécurité*[1679]. De plus, le devoir d'information étant précontractuel, la Proposition de règlement n'impose pas au détenteur de données d'informer l'utilisateur en cours de relation contractuelle d'un changement de finalité. Il serait donc opportun de prévoir une clause qui impose au détenteur d'informer l'utilisateur en cas de changement de finalité de l'utilisation des données. Par analogie, le législateur européen a retenu dans le Règlement *Plateform to Business* (P2B)[1680] une obligation pour le fournisseur de services d'intermédiation en ligne d'informer clairement les entreprises utilisatrices de plateformes lorsque des données sont partagées avec des tiers selon les finalités qui ne sont pas nécessaires au bon fonctionnement des services d'intermédiation en ligne. L'entreprise utilisatrice de la plateforme a alors le droit de refuser un tel partage[1681]. Dans cet esprit, une mesure similaire pourrait être adoptée en faveur des utilisateurs d'objets connectés et, plus particulièrement, des agriculteurs.

2. Les obligations liées à l'utilisation et au partage des données

641- **Origine contractuelle de l'utilisation des données.** Selon la Proposition de règlement sur les données, les détenteurs des données, mais aussi les tiers, ne pourraient utiliser les données en dehors de toute relation contractuelle, ce qui leur imposerait de fournir au préalable toutes les informations précontractuelles prévues à l'article 3. En effet, aux termes de l'article 4 de cette Proposition de règlement, les détenteurs des données ne devraient pouvoir utiliser « *les données à caractère non personnel générées par l'utilisation d'un produit ou d'un service lié que dans le cadre d'un accord contractuel avec l'utilisateur* ».

642- **Interdiction d'utiliser les données à des fins contraires aux intérêts de l'utilisateur.** Le détenteur de données ne pourrait, également, utiliser les données qu'il détient « *pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production de l'utilisateur, ou sur l'utilisation que ce dernier fait du produit ou du service lié, qui sont susceptibles de porter atteinte à la position commerciale de l'utilisateur sur les marchés où celui-ci est actif* »[1682]. Cet article interdirait donc au détenteur des données d'obtenir des informations dans l'intérêt contraire à l'utilisateur. Par exemple, il pourrait s'agir de données collectées à des fins spéculatives pour influencer le cours des marchés. Cet article participe

[1679] *Ibid.*
[1680] Règl. n°2019/1150 du 20 juin 2019 promouvant l'équité et la transparence pour les entreprises utilisatrices de services d'intermédiation en ligne : *JOUE* L 186/57 du 11 juill. 2019.
[1681] *Ibid.*, art. 9 et cons. 34.
[1682] Règlement sur les données, préc., art. 4.

également à l'interdiction d'un partage des données aux concurrents de l'agriculteur. Aussi, le détenteur des données ne pourrait obtenir plus d'informations sur l'utilisateur que ce qui est nécessaire pour « *vérifier sa qualité d'utilisateur* », ainsi que celles relatives « *à la bonne exécution de la demande d'accès et à la sécurité et à la maintenance de l'infrastructure de données* »[1683].

643- **Confidentialité des secrets d'affaires.** La Proposition de règlement suggère aussi de mettre en œuvre les mesures nécessaires pour préserver la confidentialité des données commerciales confidentielles[1684], tels des secrets d'affaires[1685], concernant des données partagées notamment vis-à-vis des tiers[1686].

644- **Obligation de transfert aux tiers.** Aux termes de l'article 5, le détenteur des données aurait également l'obligation de transférer les données de l'utilisateur aux tiers, « *dans les meilleurs délais, sans frais pour l'utilisateur et, le cas échéant, en continu et en temps réel, […], à un niveau de qualité identique à celui dont lui-même bénéficie* ». En revanche, les plateformes considérées comme des contrôleurs d'accès ne pourraient solliciter les utilisateurs afin d'obtenir leurs données. Cette interdiction semble anecdotique dans le secteur agricole puisqu'aucune plateforme de l'agriculture numérique ne peut être considérée comme telle à l'heure actuelle[1687].

645- **Limites des obligations du détenteur des données.** La Proposition de règlement sur les données ne prévoit en revanche pas de principe de minimisation. Ce principe vise à n'obtenir que des données adéquates, pertinentes et limitées au regard des finalités pour lesquelles elles sont traitées[1688], pour le détenteur de données. Le législateur retient, néanmoins, qu'un tel principe devrait s'appliquer lorsque le traitement comporte des risques importants pour les droits fondamentaux des personnes[1689]. Aussi, le détenteur des données devrait au sens de la Proposition de règlement, respecter le principe de minimisation lorsque la collecte des données à caractère non personnel induit un risque de réidentification. Pourtant, il semble que cette obligation de minimisation devrait également être reconnue pour le traitement des données sensibles. De même, le principe de limitation de la conservation des données dans le temps qui

[1683] *Ibid.*, art. 4.2.
[1684] *Ibid.*, cons. 77.
[1685] *Ibid.*, art. 4, 3).
[1686] *Ibid*., art. 3.3.
[1687] Voir *supra*, n°283.
[1688] RGPD, art. 5. 1. c), voir *infra*, n°717.
[1689] *Ibid*., cons. 8 : « *Compte tenu de l'état des connaissances, toutes les parties au partage de données, y compris lorsque ce partage relève du champ d'application du présent règlement, devraient mettre en œuvre des mesures techniques et organisationnelles pour protéger ces droits* ».

vise à prévoir une durée limitée au-delà de laquelle les données doivent être archivées ou supprimées[1690] n'est pas mentionné dans le *Data Act* au sujet des données non personnelles. Cette Proposition de règlement ne prévoit qu'une obligation pour les tiers qui recevraient les données de les supprimer lorsqu'elles ne sont plus nécessaires à la finalité convenue avec l'utilisateur[1691]. Il semble, toutefois, que les données sensibles devraient bénéficier également d'une obligation de conservation limitée dans le temps afin de protéger les agriculteurs. Les données considérées comme sensibles devraient donc faire exception et n'être conservées que pour la durée nécessaire à leur traitement.

B. Le renforcement des droits des « utilisateurs »

646- L'étude des droits des utilisateurs d'objets connectés sur les données non personnelles qu'ils produisent suppose d'envisager le principe de ces nouveaux droits (**1**), ainsi que leurs limites (**2**).

1. Le principe des droits de l'utilisateur

647- Droit d'utilisation et de partage. La Proposition de règlement sur les données pose le principe d'un droit d'utilisation des données en faveur de l'utilisateur. Ce dernier pourrait également décider de partager les données générées par l'utilisation de l'objet connecté ou du service qu'il utilise avec des tiers, sans que le détenteur des données ne puisse s'y opposer. Le législateur introduit aussi dans cette proposition le principe du droit général à la portabilité des données. Dans les articles suivants, la Proposition de règlement pose les bases d'un droit général à la portabilité appliqué aux données non personnelles générées par les machines et l'interopérabilité des systèmes d'information. Pour cela, le législateur envisage d'imposer divers droits et obligations aux détenteurs de données et aux tiers au sujet de l'utilisation et du partage des données.

648- Droit de partage exclusif à l'utilisateur ? Il faut noter néanmoins que le considérant 31 de la Proposition de règlement précise que « *les données générées par l'utilisation d'un produit ou d'un service lié ne devraient être mises à la disposition d'un tiers qu'à la demande de l'utilisateur* ». Ce considérant laisse supposer que le détenteur des données ne pourrait de sa

[1690] RGPD, art. 13. 2, voir *infra*, n°728.
[1691] Règlement sur les données, préc., cons. 35 et art. 6.

propre initiative mettre à disposition d'un tiers les données de l'utilisateur, sauf exceptionnellement pour le secteur public[1692]. Pourtant, l'article 3 de la Proposition de règlement sur les données précise que dans les informations à fournir à l'utilisateur, le détenteur de données devrait l'informer lorsqu'il a l'intention d'autoriser un tiers à utiliser les données. Il faudrait préciser néanmoins dans quelle mesure le détenteur de données pourrait ou non autoriser un tiers à utiliser les données de l'utilisateur. Les données sensibles ne devraient, quoi qu'il en soit, jamais pouvoir être utilisées par un tiers sans une autorisation expresse et préalable de l'utilisateur d'objets connectés ou du service lié.

2. Les limites des droits de l'utilisateur

649- **Données sensibles.** Le législateur européen dans sa Proposition de règlement sur les données a limité les droits de l'utilisateur d'objets connectés aux droits d'accès, d'utilisation et de partage des données. Il n'est pas allé aussi loin que dans le RGPD pour contrôler l'usage fait des données par les détenteurs et les tiers. Aussi, l'utilisateur ne dispose pas d'un droit de rectification et d'effacement des données, d'un droit à la limitation du traitement par les détenteurs de données ou d'un droit d'opposition. Le détenteur de données n'a qu'une interdiction d'utiliser les données qu'il détient « *pour obtenir des informations sur la situation économique, les actifs ou les méthodes de production de l'utilisateur, ou sur l'utilisation que ce dernier fait du produit ou du service lié, qui sont susceptibles de porter atteinte à la position commerciale de l'utilisateur sur les marchés où celui-ci est actif* »[1693]. Or, pour compléter cette disposition et renforcer les droits de l'utilisateur d'objet connecté, ce dernier devrait disposer d'un droit d'opposition en cas de modification des finalités par le détenteur des données. Il devrait également obtenir un droit de rectification et d'effacement des données sensibles afin de contrôler l'utilisation de ces données.

650- **Indemnisation des utilisateurs d'objets connectés ou de services liés.** Certains acteurs du numérique, et en particulier dans le secteur agricole, ou même la doctrine,[1694] ont proposé de reconnaître un droit à l'indemnisation pour l'utilisation ou le partage des données en faveur de l'utilisateur de l'objet connecté. Pourtant, dans la Proposition de règlement sur les données, le législateur n'a pas retenu cette proposition. La mise en place d'un tel droit serait à la fois complexe et contreproductive. D'une part, un droit d'indemnisation serait difficile à mettre en

[1692] *Ibid.*
[1693] *Ibid.*, art. 4.
[1694] JUILLET-REGIS, H., « Quelle régulation pour les données agricoles », *op. cit.*

œuvre en raison de la difficulté d'évaluer la valeur de la donnée[1695]. D'autre part, la reconnaissance d'une indemnisation pour l'utilisateur aurait pour effet de limiter l'exploitation et la circulation des données et donc l'innovation. En effet, les entreprises seraient moins enclines à collecter et traiter des données si elles devaient chaque fois indemniser les utilisateurs d'objets connectés et des services liés.

II. Les mesures visant à prévenir les abus de déséquilibre contractuel

651- Le législateur européen a prévu dans sa Proposition de règlement sur les données des dispositions visant à contrôler les clauses dans les contrats d'achat ou de location d'objets connectés ou de services liés (**A**). Afin de rendre effectif le contrôle de ces clauses, le législateur a également prévu des mesures procédurales (**B**).

A. Le contrôle des clauses contractuelles

652- Tout d'abord, le législateur européen a identifié, au sein d'un chapitre, les clauses abusives relatives à l'accès aux données et à l'utilisation des données interentreprises (**1**). Ensuite, il a offert la possibilité de rédiger de clauses contractuelles par défaut (**2**).

1. Les clauses abusives

653- **Définitions.** En premier lieu, le législateur identifie, dans l'article 13 de la Proposition de règlement sur les données, les personnes morales susceptibles d'être soumises à une clause abusive, il s'agit des micro, petite ou moyenne entreprise[1696]. Il pose, également, le principe selon lequel une clause ne lie pas ces entreprises lorsqu'elle est « *imposée unilatéralement par une autre entreprise et qu'elle porte sur l'accès aux données et leur utilisation ou la responsabilité et les voies de recours en cas de violation ou de résiliation d'obligations*

[1695] Voir *supra*, n°517.

[1696] Au sens de l'article 2 de l'annexe de la recommandation 2003/361/CE : « *Effectif et seuils financiers définissant les catégories d'entreprises : 1. La catégorie des micros, petites et moyennes entreprises (PME) est constituée des entreprises qui occupent moins de 250 personnes et dont le chiffre d'affaires annuel n'excède pas 50 millions d'euros ou dont le total du bilan annuel n'excède pas 43 millions d'euros. 2. Dans la catégorie des PME, une petite entreprise est définie comme une entreprise qui occupe moins de 50 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 10 millions d'euros. 3. Dans la catégorie des PME, une microentreprise est définie comme une entreprise qui occupe moins de 10 personnes et dont le chiffre d'affaires annuel ou le total du bilan annuel n'excède pas 2 millions d'euros* ».

relatives aux données ». Une clause est donc abusive « *si elle est d'une nature telle que son utilisation s'écarte fortement des bonnes pratiques commerciales en matière d'accès aux données et d'utilisation de celles-ci, et qu'elle est contraire à la bonne foi et à la loyauté* ». De plus, le législateur définit la clause contractuelle imposée unilatéralement et retient qu'il s'agit d'une clause qui « *a été fournie par une partie contractante* » et que « *l'autre partie contractante n'a pas été en mesure d'influencer son contenu malgré une tentative de négociation* ». La charge de la preuve que la clause n'a pas été imposée unilatéralement revient à celui qui a fourni la clause.

654 **Clauses abusives.** En second lieu, le législateur liste les clauses considérées comme abusives ou réputées abusives.

Tout d'abord, une clause est abusive si elle a pour objet ou pour effet de dégager de sa responsabilité la partie qui a imposé unilatéralement une clause[1697] ou encore lorsque la partie à qui a été imposée la clause ne peut pas engager les voies de recours dont elle dispose[1698]. Sont également considérées comme abusives les clauses qui donnent le droit exclusif à une partie de déterminer si les données fournies sont conformes ou non au contrat ou d'interpréter toute clause du contrat[1699].

Ensuite, sont réputées abusives les clauses qui ont pour objet ou pour effet de limiter les voies de recours de manière inappropriée de la partie à laquelle la clause a été imposée[1700]. La clause est donc réputée abusive si elle a pour objet ou pour effet « *de permettre à la partie qui a unilatéralement imposé la clause d'accéder aux données de l'autre partie contractante et de les utiliser d'une manière qui porte gravement atteinte aux intérêts légitimes de l'autre partie contractante* »[1701]. Ainsi, l'accès par le détenteur des données ou par le tiers aux données de l'utilisateur d'objets connectés doit être autorisé par lui. De plus, les détenteurs de données ne peuvent pas imposer à l'utilisateur d'objets connectés un usage des données qui porterait atteinte à ses intérêts. Est également réputée abusive la clause qui permet d'empêcher ou de

---

[1697] Règl. sur les données, préc., art.13.3. : « *Une clause contractuelle est abusive si elle a pour objet ou pour effet : (a) d'exclure ou de limiter la responsabilité de la partie qui a unilatéralement imposé la clause en cas d'actes intentionnels ou de négligence grave* ».

[1698] *Ibid*., art.13.3. : « *Une clause contractuelle est abusive si elle a pour objet ou pour effet : (b) d'exclure les voies de recours dont dispose la partie à laquelle la clause a été unilatéralement imposée en cas d'inexécution d'obligations contractuelles ou la responsabilité de la partie qui l'a imposé unilatéralement en cas de manquement à ces obligations ».*

[1699] *Ibid*., art.13.3. : : « *Une clause contractuelle est abusive si elle a pour objet ou pour effet : (c) de donner à la partie qui a unilatéralement imposé la clause le droit exclusif de déterminer si les données fournies sont conformes au contrat ou d'interpréter toute clause du contrat* ».

[1700] *Ibid*., art.13.4. : « *Une clause contractuelle est réputée abusive si elle a pour objet ou pour effet : (a) de limiter de manière inappropriée les voies de recours en cas d'inexécution des obligations contractuelles ou la responsabilité en cas de manquement à ces obligations* ».

[1701] *Ibid.*

limiter l'utilisateur d'objets connectés dans l'utilisation des données, qu'il a fourni ou généré pendant la durée du contrat[1702]. Le législateur rappelle ici le principe selon lequel l'utilisateur a le droit d'utiliser lui-même les données qu'il fournit ou génère. Pareillement, la clause qui permet d'empêcher la partie de récupérer une copie de ses données en cours d'exécution du contrat ou après la résiliation est réputée abusive[1703]. Il s'agit là d'interdire les clauses qui porteraient atteinte au droit à la portabilité des données à caractère non personnel dont dispose l'utilisateur d'objets connectés. Enfin, une clause est réputée abusive lorsqu'elle permet à une partie de résilier le contrat dans un délai excessivement court[1704]. L'utilisateur d'objets connectés devrait donc pouvoir avoir le temps de changer de fournisseur de services, sauf en cas de motifs sérieux.

665- **Conséquences de la présence de clauses abusives.** Le législateur prévoit que lorsque la clause abusive est dissociable des clauses restantes du contrat, ces dernières restent contraignantes. Néanmoins, le contrôle des clauses abusives ne s'applique pas « *aux clauses contractuelles définissant l'objet principal du contrat ni aux conditions contractuelles déterminant le prix à payer* »[1705]. Enfin, le législateur a donné un caractère d'ordre public à cet article puisque les parties ne peuvent exclure son application, y déroger ou en modifier les effets[1706].

2. L'adoption de règles contractuelles par défaut

666- **Offrir un cadre légal aux contrats concernant l'accès et l'utilisation des données.** La Commission européenne a déjà proposé l'adoption de règles contractuelles par défaut dans sa communication « *Créer une économie européenne fondée sur les données* »[1707]. Ces règles doivent servir de référence lors de la conclusion des contrats portant sur l'accès et l'utilisation des données. Les entreprises seront alors tenues de respecter ces clauses dans les contrats qu'ils

---

[1702] *Ibid.*, art.13.4. : « *Une clause contractuelle est réputée abusive si elle a pour objet ou pour effet : (c) d'empêcher la partie à laquelle la clause a été unilatéralement imposée d'utiliser les données qu'elle a fournies ou générées pendant la durée du contrat, ou de limiter l'utilisation de ces données dans la mesure où cette partie n'est pas autorisée à utiliser, à capturer, à consulter ou à contrôler ces données ou à en exploiter la valeur de manière proportionnée* ».

[1703] *Ibid.*, art.13.4. : « *Une clause contractuelle est réputée abusive si elle a pour objet ou pour effet : (d) d'empêcher la partie à laquelle la clause a été unilatéralement imposée d'obtenir une copie des données qu'elle a fournies ou générées pendant la durée du contrat ou dans un délai raisonnable après la résiliation de celui-ci* ».

[1704] *Ibid.*, art.13.4. : « *Une clause contractuelle est réputée abusive si elle a pour objet ou pour effet : (e) "de permettre à la partie qui a unilatéralement imposé la clause de résilier le contrat dans un délai excessivement court, compte tenu des possibilités raisonnables de l'autre partie contractante de se tourner vers un service alternatif et comparable et du préjudice financier causé par cette résiliation, sauf s'il existe des motifs sérieux de le faire"* ».

[1705] *Ibid.*, art. 3.7.

[1706] *Ibid.*, art. 13.8.

[1707] Commission européenne, *Créer une économie européenne fondée sur les données*, préc., art 3.5.

concluent avec leurs clients. Cette solution a pour avantage de laisser à la fois une certaine liberté contractuelle selon la Commission tout en réduisant le déséquilibre significatif dans les contrats de l'agriculture numérique. La Commission européenne a renouvelé cette proposition dans le Règlement sur les données à l'article 34 dans lequel elle propose d'élaborer et de recommander « *des clauses contractuelles types non contraignantes concernant l'accès aux données et leur utilisation afin d'aider les parties à rédiger et à négocier des contrats garantissant l'équilibre des droits et obligations contractuels* ». Aussi, la Commission européenne recommande l'élaboration de clauses contractuelles qui permettraient de faciliter le changement de prestataire. Il s'agirait de clauses types qui obligeraient le prestataire de services à mettre en œuvre la portabilité des données des clients. Elles seraient, notamment, recommandées dans les contrats de l'agriculture numérique.

657- **Clauses types envisageables.** Sur le même principe que le Code de conduite de l'UE relatif au partage des données agricoles par accord contractuel[1708], les clauses contractuelles types pourraient prévoir que l'agriculteur générateur de données peut recevoir ou transférer les données qu'il produit « *dans un format structuré, courant et lisible sur ordinateur* » à condition que cette opération soit techniquement réalisable. Ainsi, il devrait pouvoir transférer ses données à un autre opérateur ou les récupérer lui-même. Également, une clause pourrait prévoir que le créateur n'est « *jamais […] limité lorsqu'il souhaite utiliser les données qu'il produit dans d'autres systèmes, plateformes ou encore applications* ». Aussi, les informations concernant les moyens de « *visualiser, corriger, récupérer [ou encore] extraire les données* » devraient toujours être fournies, à l'agriculteur, créateur de données. De même, son prestataire devrait lui fournir les informations concernant « *les moyens qui lui permettent de migrer les données relatives à ses activités agricoles vers d'autres services ainsi que les normes et formats d'échange des données électroniques pris en charge par [lui]* ».

658- **Obligations contractuelles pour le changement de fournisseur de services de traitement de données.** Afin de faciliter le changement de fournisseur de services, les fournisseurs de services de traitement de données seraient tenus de supprimer les obstacles commerciaux, techniques, contractuels et organisationnels qui freinent les clients dans les démarches de changement de fournisseur.

Au titre de l'article 23 de la Proposition de règlement, les fournisseurs de services devraient permettre à leurs clients de résilier leur accord contractuel, après un préavis maximal de 30 jours calendaires ; de conclure de nouveaux accords contractuels avec d'autres

[1708] Voir *supra* n°561 et s.

fournisseurs de traitement des données couvrant le même type de service ; de porter leurs données, applications et autres actifs numériques vers d'autres fournisseurs de services de traitement de données ; de maintenir l'équivalence fonctionnelle du service dans l'environnement informatique du ou des différents fournisseurs de services de traitement de données, couvrant le même type de service.

Sur le plan contractuel, l'article 24 imposerait que les droits et obligations du client et du fournisseur de services soient « *clairement énoncés dans un contrat écrit* ». Ce contrat devrait comporter au moins des clauses qui permettent au client de changer de fournisseur de services avec l'aide du fournisseur initial pour le changement lorsque cela est techniquement possible. Ce dernier devrait également assurer la pleine continuité dans la fourniture des fonctions ou services respectifs avant la fin du processus. Le contrat devrait également contenir une clause spécifiant de manière exhaustive toutes les catégories de données et d'applications exportables pendant le processus de changement de fournisseur. Enfin, une clause devrait prévoir une période minimale pour l'extraction des données d'au moins trente jours calendaires à compter de la fin de la période transitoire convenue entre le client et le fournisseur de services. Si le transfert dans la période transitoire est techniquement impossible, le fournisseur devrait informer le client dans un délai de sept jours ouvrables à compter de la présentation de la demande de changement de fournisseur de manière motivée et indiquer une nouvelle période transitoire qui ne pourrait excéder six mois.

La Commission européenne propose, en outre, de supprimer les frais de changement de fournisseur de manière progressive, afin que la portabilité des données soit gratuite pour le client.

659- **Clauses types sur l'utilisation des données sensibles.** Concernant les données sensibles, une clause devrait prévoir que les utilisateurs d'objets connectés, et notamment les agriculteurs, puissent modifier ou supprimer les données sensibles générées par les objets connectés et les services qu'ils utilisent, tout en étant informés des conséquences d'une telle modification ou suppression sur la continuité du service. L'exploitant agricole qui produit ou génère des données par son activité ou qui a confié cette tâche au fournisseur de données devrait pouvoir déterminer contractuellement les bénéficiaires d'un droit d'accès à ces données sensibles. Il devrait également pouvoir s'opposer à tout usage ou partage des données sensibles pour lequel il n'aurait pas consenti, au moyen du droit d'opposition. Les prestataires de services devraient également assurer un *Reporting* pour les exploitants agricoles. Ce *Reporting* consisterait à tenir l'exploitant agricole informé de chaque usage ou partage envisagé concernant les données sensibles d'exploitation. Enfin, les prestataires de services devraient être tenus

contractuellement d'assurer la sécurité des données sensibles agricoles en mettant en œuvre toutes les mesures techniques et juridiques nécessaires pour leur protection. L'ensemble de ces clauses devraient permettre de renforcer la loyauté des usages par le prestataire de services sur les données sensibles. Afin d'assurer l'effectivité de ces obligations, elles devraient faire l'objet d'une obligation de formalisme dans les contrats.

B. La mise en œuvre du contrôle du droit d'utilisation et de partage des données non personnelles

660- Afin de mettre en œuvre le droit applicable aux données à caractère non personnel, la Commission européenne propose de désigner une autorité compétente nationale pour traiter de futurs litiges (**1**) et de déterminer des sanctions applicables aux violations des règles d'accès et d'usage (**2**).

1. La désignation d'une autorité compétente nationale

661- Au titre de l'article 31 de la Proposition de règlement sur les données, chaque État membre devra désigner une ou plusieurs autorités compétentes responsables de la bonne application et de la mise en application de ce règlement, en créant une nouvelle autorité ou en s'appuyant sur des autorités existantes. En France, la CNIL est dédiée aux données à caractère personnel, une nouvelle commission pourrait être créée afin d'assurer la mise en œuvre du futur règlement en France sur les données à caractère non personnel. Des autorités par secteur d'activité[1709], tel que dans le secteur agricole, pourraient être désignées afin d'être au plus proche des problématiques de chaque secteur. Ainsi, les utilisateurs d'objets connectés pourraient introduire une procédure auprès de ou des autorité(s) compétente(s).

2. Les sanctions du non-respect de la réglementation

662- Au titre de l'article 33 de la Proposition de règlement sur les données, chaque État membre devra établir les règles relatives aux sanctions applicables aux infractions au règlement et prendre toutes les mesures nécessaires pour assurer leur mise en œuvre. Les sanctions prévues devraient être effectives, proportionnées et dissuasives. Ces sanctions devraient être calquées

[1709] Règlement sur les données, préc., art. 31, 2. b.

sur celles de la violation des règles du RGPD afin d'harmoniser les sanctions applicables aux traitements de données.

§2. *Les aspects techniques du contrôle de l'usage*

663- Les trois outils que sont la portabilité, la possibilité de multi-domiciliation et l'interopérabilité permettent à la fois de « *réduire la dépendance des complémenteurs et [de] préserver la concurrence interplateformes* »[1710], mais aussi d'assurer le contrôle de l'usage par les exploitants agricoles. Ainsi, l'effectivité d'un tel contrôle de l'usage ne peut se faire sans la création d'un régime contraignant pour les entreprises captatrices de données sur les mesures techniques à mettre en place. Pour ce faire, les fournisseurs de services et d'objets connectés devraient rendre leurs services interopérables. Aussi, il convient d'envisager, dans un premier temps, le principe de l'interopérabilité (**I**) pour, dans un second temps, envisager sa mise en œuvre (**II**).

I. L'interopérabilité des systèmes d'information et des services

664- Tout d'abord, il est nécessaire d'envisager les enjeux de l'interopérabilité (**A**) pour, ensuite, s'intéresser au contenu du droit à l'interopérabilité (**B**).

A. Les enjeux de l'interopérabilité

665- S'il convient d'étudier, en premier lieu, la lente consécration du droit à l'interopérabilité des données non personnelles (**1**), il faudra, en second lieu, analyser les obstacles liés à la notion d'interopérabilité (**2**).

1. La lente consécration du droit à l'interopérabilité des données non personnelles

666- Le droit à l'interopérabilité est le pendant de la portabilité des données. En effet, il permet de rendre effectif le transfert de données entre deux systèmes d'information, services ou encore objets connectés. Il a, dans un premier temps, été reconnu en droit d'auteur dans la loi du

[1710] MARTY, F., « Accès aux données, coopétition intra-plateforme et concurrence inter-plateformes numériques », *op. cit.*

1er aout 2006[1711] afin de permettre à des interfaces logiques de programmes de communiquer entre elles par le biais d'échanges d'informations et d'utilisation mutuelle des informations échangées[1712]. Aussi, le législateur a intégré à l'article L. 331-5 du CPI une disposition selon laquelle « *les mesures techniques ne doivent pas avoir pour effet d'empêcher la mise en œuvre effective de l'interopérabilité, dans le respect du droit d'auteur. Les fournisseurs de mesures techniques donnent l'accès aux informations essentielles à l'interopérabilité dans les conditions définies au 1° de l'article L. 331-31 et à l'article L. 331-32* ».

Afin de mieux répondre à l'objectif d'interopérabilité, certains auteurs préconisent d'en retenir une vision globale[1713]. En effet, jusqu'alors des règles étaient prises seulement secteur par secteur, à l'image du livre numérique[1714]. De plus, le droit souple n'est pas suffisamment efficace pour assurer de manière pérenne la portabilité et l'interopérabilité des données dans le secteur agricole, en raison notamment des enjeux concurrentiels liés à leur détention. Seule la norme peut avoir l'effet d'imposer la portabilité à tous les acteurs du secteur.

Aujourd'hui, l'interopérabilité est devenue un enjeu majeur pour les acteurs du numérique. Déjà en 2016, le Comité économique et social européen a, dans un avis, affirmé l'importance d'adopter des normes communes pour instituer la base d'un marché numérique efficace. Ces normes communes doivent garantir l'interopérabilité des technologies numériques[1715]. En 2017, dans un rapport concernant la mission sur l'interopérabilité des services numériques[1716], le CSPLA a également mis en avant l'interopérabilité comme l'un des enjeux cruciaux pour la mise en œuvre du marché numérique européen. La même année, la Commission européenne a, dans une communication[1717], soutenu la consécration d'un droit à la portabilité des données à caractère non personnel et a préconisé l'adoption de normes techniques afin d'améliorer l'interopérabilité des données. Elle préconisait aussi le recours à des tests sectoriels pour expérimenter les solutions envisageables dans le but de parvenir à une économie européenne fondée sur les données. Elle s'est engagée à soutenir ces normes appropriées pour assurer une meilleure intégration des travaux de communauté *Open Source* dans le processus d'élaboration des normes européennes, et ce, afin d'améliorer

[1711] Loi n°2006-961, 1er août 2006, relative au droit d'auteur et aux droits voisins dans la société de l'information : *JORF* n°178 du 3 août 2006.
[1712] BRUGUIERE, J.-M., « Le droit à l'interopérabilité », *CCE* n°2, févr. 2007, ét. 3.
[1713] MACREZ, F. et DUFLOT, F., « L'interopérabilité, principe incontournable des libertés numériques », *PI*, oct. 2017, n°65.
[1714] CSPLA, *Mission sur l'interopérabilité des services numériques*, Rapport établi par MOCHON, J.-P. et PETITDEMANGE, E., avr. 2017.
[1715] CESE, avis, 21 sept. 2016, Priorités pour la normalisation en matière de TIC dans le marché unique numérique, COM(2016)176 final : *JOUE* C 487/92 du 28 déc. 2016.
[1716] CSPLA, *Mission sur l'interopérabilité des services numériques*, *op. cit.*
[1717] Commission européenne, *Créer une économie européenne fondée sur les données*, préc.

l'interopérabilité, la portabilité et la sécurité des services informatiques en nuage[1718]. Cette proposition a été soutenue en France par le CNNum qui a publié en ce sens une communication sur la consécration d'un droit à la portabilité des données non personnelles[1719]. Il rappelle dans ce communiqué la nécessité de mener une « *réflexion approfondie sur les standards d'interopérabilité et les modes d'accès techniques aux données, notamment via des interfaces de programmation (API)* »[1720].

En 2018, le Règlement sur la libre circulation des données non personnelles[1721] établi par la Commission européenne n'a pas créé de régime juridique pour encadrer l'interopérabilité des données. Néanmoins, la commission a encouragé les acteurs des secteurs concernés à établir des standards d'interopérabilité pour favoriser le partage des données inter-secteurs[1722]. Elle n'a évoqué que de manière lapidaire l'interopérabilité à l'article 6 du Règlement sur la libre circulation des données non personnelles[1723]. En 2020, le législateur européen a rappelé l'importance de l'interopérabilité pour l'exploitation de la valeur des données dans le contexte du déploiement de l'intelligence artificielle dans sa Stratégie européenne pour les données[1724]. L'Assemblée nationale a, également, dans un rapport d'information[1725] en date du 24 juin 2020, opéré le même constat. Finalement, le 23 février 2022, la Commission européenne a posé les bases d'un régime juridique pour l'interopérabilité des services dans le but de rendre effective la portabilité des données. À cette fin, elle a permis de définir des « *spécifications d'interopérabilité ouvertes* » et des « *normes européennes pour l'interopérabilité des services de traitement des données afin de promouvoir un environnement en nuage multifournisseur continu* »[1726]. La consécration de ce règlement permettra d'offrir aux acteurs de l'agriculture numérique un meilleur contrôle de l'usage des données. Il permettra, également, de garantir les libertés numériques en assurant la portabilité et le transfert des données non personnelles d'un prestataire de services à un autre. De plus, l'adoption de cette réglementation aura l'effet bénéfique d'harmoniser le régime des données à caractère non personnel sur celui des données

[1718] *Ibid.*
[1719] CNNum, *La consécration d'un droit à la portabilité des données non personnelles*, *op. cit.*
[1720] *Ibid*., p. 4.
[1721] Règl. n°2018/1807 du 14 nov. 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne : *JOUE* L 303/59 du 28 nov. 2018.
[1722] Règl. n°2018/1807, préc., cons. 29 : « *La capacité de transférer des données sans entrave est un élément clé pour faciliter le choix de l'utilisateur et favoriser une concurrence effective sur les marchés pour les services de traitement des données* ».
[1723] *Ibid*., art. 6 sur le portage des données : « *Les bonnes pratiques facilitent le changement de fournisseurs de services et le portage des données dans des formats structurés, usuels et lisibles par machine, notamment dans des formats standard ouverts, lorsque le fournisseur de services obtenant les données le demande ou l'exige* ».
[1724] Commission européenne, *Une stratégie européenne pour les données*, préc.
[1725] AN, Rapport d'information n°3127 sur les plateformes numériques, préc.
[1726] Règlement sur les données, préc., art. 29.

à caractère personnel, ce qui facilitera les transferts d'ensembles de données mixtes préalablement collectés sur les exploitations agricoles.

2. Les obstacles dans l'appréhension de la notion d'interopérabilité

667- Une correspondance entre les logiciels, l'environnement technique et l'infrastructure matérielle permet, d'une part, d'assurer le libre jeu de la concurrence et l'innovation et, d'autre part, de reconnaître aux utilisateurs une plus grande maîtrise sur les données qu'ils fournissent ou génèrent. L'interopérabilité permet de faire circuler librement les données sans contraintes techniques, juridiques ou financières. L'objectif est donc de supprimer les barrières d'accès aux données, afin d'éviter que « *l'utilisation d'une technologie en mode fermé, plutôt qu'en mode ouvert, [soit] un facteur susceptible de restreindre le développement du marché en rendant les utilisateurs captifs de celle-ci* »[1727]. L'interopérabilité évite donc l'accaparement des données par les grandes entreprises de l'*AgTech*. C'est pourquoi l'interopérabilité est un objectif depuis longtemps poursuivi par l'Union européenne[1728] qui en a fait un des piliers de sa Stratégie numérique[1729]. Pourtant, il faut constater les difficultés du législateur à adopter une réglementation sur l'interopérabilité des données. La cause de ces difficultés peut être recherchée dans l'obstacle de l'appréhension de la notion d'interopérabilité. Effectivement, le législateur s'était, jusqu'alors, abstenu de définir cette notion en raison du fait qu'une définition trop précise ferait courir le risque d'un dépassement. Ceci aurait pour conséquence de limiter la portée de la disposition[1730]. En effet, le législateur confond bien souvent « *simple compatibilité* »[1731] et véritable « *capacité d'un contenu à être exploité indifféremment de son environnement* »[1732]. Néanmoins, dans le RGPD, en 2016, la Commission européenne a retenu comme définition pour l'interopérabilité qu'il s'agit de « *la capacité de diverses organisations*

[1727] ROBIN, A., « Les places de marché en ligne », *J-Cl com.*, fasc. 827, oct. 2019 : « *Une consultation publique réalisée par la commission européenne sur les plateformes en ligne et le marché unique européen, a montré qu'en raison des différentes conceptions des interfaces de programmation d'application (API) ou du changement des conditions d'accès aux places de marché, pouvait avoir pour effet, notamment, d'empêcher les utilisateurs professionnels de changer de plateforme* ».

[1728] D'importants débats avaient eu lieu déjà pour l'adoption de la directive 91/250/CEE, du Conseil, du 14 mai 1991, concernant la protection juridique des programmes d'ordinateur : *JO* L 122 du 17 mai 1991 pp. 0042 - 0046

[1729] Commission européenne, *Une stratégie pour un marché unique du numérique en Europe*, préc.

[1730] BRUGUIERE, J. -M., « Le droit à l'interopérabilité », *op. cit.* ; voir AN, Rapport n°3185, *relatif au droit d'auteur et aux droits voisins dans la société de l'information*, 22 juin 2006., p. 16.

[1731] MACREZ, F. et DUFLOT, F., « L'interopérabilité, principe incontournable des libertés numériques », *op. cit.*

[1732] *Ibid.* ; A. 20 avr. 2016, portant approbation du référentiel général d'interopérabilité : *JORF* n°0095 du 22 avril 2016, définition officielle du référentiel général d'interopérabilité : « *[l'] interopérabilité est la capacité que possède un produit ou un système, dont les interfaces sont intégralement connues, à fonctionner avec d'autres produits ou systèmes existants ou futurs, et ce sans restriction d'accès ou de mise en œuvre* ».

hétérogènes à interagir en vue d'atteindre des objectifs communs, mutuellement avantageux et convenus »[1733]. La Directive concernant certains aspects des contrats de contenus numériques[1734] retient, quant à elle, que l'interopérabilité est « *la capacité du contenu numérique à assurer toutes ses fonctionnalités en interaction avec un environnement numérique concret* ». En revanche, le Règlement sur la libre circulation des données non personnelles ne fournit pas de définition de l'interopérabilité. Ces différentes définitions, voire l'absence de définition, expriment les difficultés du législateur à appréhender cette notion. Finalement, la Commission européenne s'évertue à répondre au mieux aux conditions de la notion et retient finalement dans la Proposition de règlement sur les données la définition suivante : l'interopérabilité est « *la capacité de deux ou plusieurs espaces de données ou réseaux de communication, systèmes, produits, applications ou composants à échanger et à utiliser des données afin de remplir leurs fonctions* ».

B. Le contenu de l'interopérabilité

668. L'étude du droit à l'interopérabilité nécessite d'envisager son étendue (**1**), puis ses aspects techniques (**2**).

1. L'étendue de l'interopérabilité

669. Les données devraient pouvoir être transmises et exploitées sur n'importe quel ordinateur, dans n'importe quel système d'exploitation ou logiciel sans « *frontière technique* », ou du moins, lorsque cela est techniquement possible. Aussi, en plus d'imposer le droit à la portabilité pour les données non personnelles, il est nécessaire d'adopter « *des normes techniques appropriées afin de soutenir des politiques de portabilité efficaces* »[1735]. C'est à cette condition que la libre circulation des données pourra être effective. C'est pourquoi il était primordial dans la Proposition de règlement portant sur l'accès et l'utilisation des données de « *s'intéresser explicitement à l'environnement technique, l'infrastructure matérielle et logicielle qui permet à ces données de voyager* »[1736].

[1733] RGPD, cons. 68.
[1734] Dir. n°2019/770 du 20 mai 2019 relatives à certains aspects concernant les contrats de fourniture de contenus numériques et de services numériques : *JOUE* L 136, 22 mai 2019, non transposée, art. 2, 11).
[1735] Créer une économie européenne fondée sur les données, préc., art. 5.3.
[1736] MACREZ, F. et DUFLOT, F., « L'interopérabilité, principe incontournable des libertés numériques », *op. cit.*

2. Les spécifications techniques des standards ouverts

670- Afin d'assurer véritablement l'interopérabilité des données, les entreprises devraient être tenues de mettre en œuvre techniquement des standards ouverts. La Loi pour une République numérique définit le standard ouvert comme « *tout protocole de communication, d'interconnexion ou d'échange et tout format de données interopérables et dont les spécifications techniques sont publiques et sans restriction d'accès ni de mise en œuvre* »[1737]. L'objectif d'interopérabilité est suivi également par la Commission européenne qui préconise afin de faciliter la recherche et l'interopérabilité de « *disposer de métadonnées riches, normalisées et conformes à des vocabulaires établis* » par les acteurs du numérique[1738]. Elle cite ensuite en exemple la Directive Inspire[1739] concernant les données géographiques du secteur public qui établit une infrastructure d'informations géographiques dans la communauté européenne et permet d'assurer l'interopérabilité des données d'observations fournies par des capteurs. MM. F. Macrez et F. Duflot, soutiennent l'idée qu'il faut « *garantir l'interopérabilité by design des outils numériques […] pour permettre la fluidité des échanges dans le secteur numérique, éviter la captation des valeurs liées au numérique par les fournisseurs de solutions techniques et la cristallisation du marché autour d'un petit nombre d'acteurs souvent d'origine extraeuropéenne* »[1740].

Ainsi, il doit s'agir « *d'une obligation pour les acteurs économiques de proposer des solutions techniques respectant les composants fondamentaux de l'interopérabilité et notamment la publication d'interfaces et l'utilisation de standards ouverts* »[1741]. MM. F. Duflot et F. Macrez préconisent également d'imposer légalement une « *obligation positive de publier les spécifications techniques des standards rendant l'interopérabilité effective* »[1742]. D'ailleurs, l'Assemblée nationale dans un rapport d'information en date du 24 juin 2020, opère le même constat et propose « *[d'] élaborer de nouvelles règles et des standards communs pour favoriser la portabilité en vue de l'interopérabilité sous l'égide d'un régulateur* »[1743]. Comme pour les données personnelles, le format des données non personnelles devrait donc être structuré de sorte qu'elles puissent être lues par n'importe quelle machine ou n'importe quel logiciel.

[1737] LRN, art. 4.
[1738] Créer une économie fondée sur les données, préc., art. 5.2.
[1739] Dir. n°2007/2/CE établissant une infrastructure d'information géographique dans la Communauté européenne (Inspire) : *JOUE* L 108/1 du 25 avr. 2007.
[1740] MACREZ, F. et DUFLOT, F., « L'interopérabilité, principe incontournable des libertés numériques », *op. cit.*
[1741] *Ibid.*
[1742] *Ibid.*
[1743] AN, Rapport d'information n°3127, *sur les plateformes numériques*, *op. cit.*

Néanmoins, dans le RGPD « *aucun format n'est imposé en raison des variations observables dans la structuration des données dans les différents secteurs d'activité* »[1744]. Par conséquent, les acteurs du secteur agricole devraient adopter des standards communs pour atteindre la standardisation de l'agriculture numérique. La future consécration réglementaire concernant les données non personnelles permet d'encadrer la mise en œuvre de l'interopérabilité.

II. La mise en œuvre de l'interopérabilité

671- S'il faut d'abord s'intéresser à l'élaboration de standards ouverts par les acteurs du secteur agricole (**A**), il faudra ensuite envisager les futures exigences réglementaires encadrant l'interopérabilité (**B**).

A. L'élaboration de standards ouverts par les acteurs du secteur agricole

672- Afin de rendre effective l'interopérabilité entre les différents systèmes de collecte et de traitement de données, les acteurs de l'agriculture numérique ont créé et développé des standards et normes d'échanges de données (**1**). Néanmoins, l'interopérabilité des systèmes d'information et des services dans le secteur agricole est encore limitée (**2**).

1. Les développements du secteur agricole sur l'interopérabilité des données des exploitations

673- Dans le secteur de l'agriculture numérique, les acteurs se sont concertés et ont développé des standards communs afin de pouvoir échanger les données entre les équipements des agriculteurs[1745]. Tout d'abord, afin d'établir des standards communs, il faut dans un premier temps définir les standards de modélisation, les modèles de données et fournir des dictionnaires ou des référentiels de données et des standards d'échange. Ces problématiques ont été développées par des organisations telles qu'AEF, AgGateway et AgroEdi. De ces différentes initiatives sont nés des outils qui sont des standards d'échanges de données. Ils permettent d'échanger des données entre des équipements mobiles comme des semoirs ou des pulvérisateurs afin de remonter les données à des machines telles qu'un tracteur. Pour en citer

[1744] ROBIN, A., « Les places de marché », *op. cit*, n°110
[1745] Selon un article de LEROUX, C., *Standards et échanges de données dans le numérique Agricole*, sur le site Aspexit, https://www.aspexit.com/standards-et-echanges-de-donnees-dans-le-numerique-agricole/.

quelques-uns, il s'agit d'ADAPT, d'ISOXML, d'ISOBUS ou encore de DAPLOS. L'objectif de ces outils est de donner des instructions à l'objet connecté afin de réaliser son opération culturale par exemple. Ces normes également permettent d'échanger des données entre machines, logiciels et autres solutions télématiques, telles que des logiciels de gestion parcellaire. D'autres initiatives de différents groupements ont développé des standards et d'autres solutions afin d'améliorer l'interopérabilité des services. Pour en citer quelques-uns, c'est le cas notamment de Numagri chargé de créer un langage commun de l'agriculture numérique en vue de faciliter les échanges de données. Il est possible de citer également la solution Agrirouter portée par DKE chargé de connecter les logiciels de gestion parcellaire et les machines agricoles. De même encore, F4F de Proagrica est spécialisé dans les standards et la connectivité. Enfin, les API qui peuvent être définies comme « *un format d'échange normalisé, documenté* »[1746] assurent l'accès aux données et leur contrôle. Ce sont des « *prise(s) de courant pour les données* »[1747]. C'est sur ce modèle qu'AgdataHub a développé la plateforme API-AGRO qui permet d'échanger des données en mode SaaS (*Service as a Software*) basée sur la technologie DataExchange de Dawex.

2. Les limites de l'interopérabilité dans le secteur agricole

674- Les besoins en interopérabilité dans le secteur agricole sont très importants afin de favoriser les échanges de données entre tous les acteurs du secteur[1748]. Néanmoins, le constat est qu'aujourd'hui, l'interopérabilité n'est pas complètement opérationnelle pour diverses raisons. D'abord, les coûts importants que la mise en œuvre de l'interopérabilité des systèmes et des services engendre, ainsi que les difficultés techniques que les acteurs rencontrent, constituent des obstacles au développement des standards ouverts. Ensuite, malgré les efforts des acteurs du secteur, il existe encore un manque d'harmonisation des standards et des définitions qui limite le partage des données. Enfin, il faut évoquer la recherche de compétitivité des acteurs qui préfèrent conserver un monopole sur les actifs qu'ils détiennent. Cependant, la tendance générale va plutôt vers la valorisation des données grâce aux échanges, mais aussi pour les agriculteurs qui souhaitent utiliser des outils et des logiciels de marques différentes.

[1746] BABINET G., *Transformation digitale : l'avènement des plateformes. Histoires de licornes, de Data et de nouveaux barbares…,* Le passeur, 2016, p. 151.
[1747] *Ibid.*
[1748] Tels que les éleveurs, vétérinaires, conseils, génétiques, grandes distributions, dans le monde animal et entre agriculteurs, conseils, organismes de collectes et de stockage, grandes distributions, filières, consommateurs dans le monde végétal.

B. Les futures exigences réglementaires en matière d'interopérabilité

675- Afin de régir les règles applicables à l'interopérabilité, la Commission européenne apporte un cadre pour l'interopérabilité dans sa Proposition de règlement sur les données. Aussi, il est nécessaire d'envisager le contenu des exigences d'interopérabilité (**1**) ainsi que les mesures envisagées pour sa mise en œuvre dans l'Union européenne (**2**).

1. Le contenu des exigences d'interopérabilité

676- Les opérateurs d'espaces de données devront respecter les exigences du Règlement pour faciliter l'interopérabilité des données, les mécanismes de partage de données et des services[1749]. À cette fin, plusieurs éléments devraient être suffisamment décrits afin de permettre au destinataire de trouver les données, d'y accéder et de les utiliser : « *le contenu des données, les restrictions d'utilisation, les licences, la méthode de collecte des données, la qualité des données et l'incertitude sur les données* ». De plus, certaines informations devraient être décrites de manière qu'elles soient cohérentes et accessibles au public. Il s'agit des structures de données, de leurs formats, des vocabulaires, des systèmes de classification, des taxinomies et des listes de codes. Également, les moyens techniques d'accès aux données, leurs conditions d'utilisation et leur qualité de service devraient être suffisamment décrits « *pour permettre l'accès automatique aux données et leur transmission automatique* ». Enfin, les exploitants d'espaces de données devraient prévoir « *les moyens permettant l'interopérabilité des contrats intelligents dans le cadre de leurs services et activités* ». Ainsi, les exploitants d'espaces de données devraient respecter certaines exigences, dont l'obligation de décrire tous les éléments qui devraient permettre d'accéder et de transférer les données. Pour assurer l'effectivité de l'interopérabilité par les parties intéressées, la proposition européenne délègue sa mise en œuvre technique aux organismes de normalisation européens[1750]. Plus spécifiquement, les règles de l'interopérabilité concernant les prestations de traitement de données[1751] devraient être performantes pour assurer l'interopérabilité entre les différents services de traitement qui couvrent le même type de service. Ces règles devraient améliorer la portabilité des actifs numériques entre les différents services et garantir, lorsque c'est techniquement possible, l'équivalence fonctionnelle entre différents services. Enfin, concernant

[1749] Règlement sur les données, préc., art. 28.
[1750] *Ibid.*, arts. 28 et 29.
[1751] *Ibid.*, art. 29.

les *Smart contracts*[1752], la Proposition de règlement prévoit également certaines exigences de robustesse afin d'éviter les erreurs de fonctionnement et pour résister aux manipulations des tiers. Le vendeur devrait donc prévoir des mécanismes et des fonctions internes qui permettent de résilier et d'interrompre le contrat en toute sécurité, ainsi que l'archivage et la continuité des données pour conserver l'enregistrement des opérations effectuées (vérifiabilité). Enfin, il devrait prévoir des mécanismes de contrôle d'accès pour protéger le *Smart contract* au niveau de la gouvernance et des *Smart contracts* eux-mêmes.

2. Mise en œuvre de l'interopérabilité dans l'Union européenne

677.- Dans l'objectif de mettre en œuvre l'interopérabilité des données, la Commission européenne pourrait demander à des organisations européennes de normalisation d'élaborer des normes harmonisées qui répondront aux exigences du Règlement[1753]. En l'absence de normes harmonisées ou lorsque ces normes ne répondent pas aux exigences du Règlement, la Commission européenne prévoit d'adopter par des actes d'exécution des spécifications communes[1754]. Aussi, la Commission européenne pourrait adopter des lignes directrices afin d'établir des spécifications d'interopérabilité. Il pourrait s'agir de règles et d'accords juridiques d'exécution ou de normes techniques[1755].

678.- **Conclusion de la section.** Le droit de contrôle de l'usage devrait être un droit personnel. Par conséquent, il devrait s'appuyer sur le contrat et les clauses qui encadrent les droits et les obligations de chaque partie. Ainsi, les agriculteurs devraient pouvoir obtenir le droit de contrôler l'usage des données qu'ils génèrent lorsqu'ils achètent un objet connecté ou qu'ils s'abonnent à un service lié. Le législateur européen prévoit à ce titre d'organiser les droits et les obligations de chaque partie dans les contrats tout en contrôlant les éventuels déséquilibres significatifs. La technique contractuelle devrait néanmoins être complétée de mesures techniques en imposant l'obligation de rendre interopérables les systèmes d'information et les services. Ce n'est qu'à ces conditions que le contrôle de l'usage des données à caractère non personnel pourra être effectif pour l'utilisateur d'objets connectés, en général, et pour l'exploitant agricole, en particulier.

[1752] *Ibid.*, art. 30.
[1753] *Ibid.*, arts., 28, 29 et 30.
[1754] *Ibid.*
[1755] *Ibid.*, art. 28.

679- **Conclusion du chapitre.** Seul un véritable droit de contrôle de l'usage permettra de renforcer l'équilibre dans les relations contractuelles entre l'exploitant agricole et ses partenaires commerciaux. La consécration du futur Règlement sur les transferts de données non personnelles des utilisateurs d'objets connectés permettra de combler, en grande partie, ce vide juridique. Il permettra notamment de renforcer les droits des utilisateurs d'objets connectés et des services liés sur les données qu'ils génèrent et contraindra les entreprises détentrices de données à fournir les outils techniques et juridiques afin de rendre effectif ce droit. Il n'en demeure pas moins qu'un véritable droit de contrôle de l'usage en faveur des exploitants agricoles devrait être étudié. En effet, un tel droit permettrait de prendre en compte de manière plus fine et granulaire les spécificités du secteur agricole. Il s'agirait, en effet, de prendre en considération la sensibilité des données issues des exploitations agricoles tout en assurant la circulation des données « normales » non personnelles et la réservation des données enrichies significativement par l'entreprise. Par conséquent, ce droit de contrôle de l'usage des données agricoles devrait permettre de tendre vers un équilibre entre les entreprises de l'*AgTech* et les exploitants agricoles.

Chapitre 2. La consécration actée du droit de contrôle de l'usage des données d'exploitation à caractère personnel

680- Les données à caractère personnel peuvent avoir « *une valeur économique ou un intérêt pour la recherche* »[1756]. Déjà en 2009, certains auteurs se demandaient si la réutilisation de certaines données sensibles, en l'occurrence les données de santé, ne pouvait pas « *poser de graves questions sur le respect des droits des personnes concernées ? Le droit positif en vigueur comme la technique informatique permettront-ils une véritable anonymisation de ces données ? Sont-ils à même de rendre effectif le respect du droit à l'oubli ? Ne faudrait-il pas aménager d'autres formes de régulation pour assurer, d'une part, les intérêts privés des patients à leur droit à l'autodétermination et, d'autre part, permettre la circulation et l'exploitation des données au service de l'intérêt général et de la recherche ?* »[1757]. Si ces questions se posaient en ces termes s'agissant des données de santé, les mêmes questions se posent aujourd'hui concernant les données des agriculteurs. La question de la protection des données personnelles du secteur agricole a pris de l'envergure en raison, d'une part, de l'ampleur que prennent de nos jours les usages des données issues des exploitations agricoles, d'autre part, de la création d'une chaîne de confiance dans le secteur agricole[1758].

681- D'aucuns affirment que « *tout est devenu donnée personnelle* »[1759]. Il est, en effet, aujourd'hui, de plus en plus difficile de distinguer les données à caractère personnel de celles qui n'en sont pas. Dans le secteur agricole, le patrimoine personnel de l'exploitant se mêle souvent avec celui de sa société. Par conséquent, il semble que de nombreuses données personnelles sont collectées dans les exploitations agricoles et appellent une protection accrue. La question alors se pose de savoir comment se manifeste la maîtrise des données à caractère personnel par l'exploitant agricole en tant que générateur de la donnée.

Certains auteurs, tels que ceux participant au *Think Tank* Génération Libre[1760], préconisent une monétisation de la donnée personnelle afin d'assurer une maîtrise des données par les personnes physiques. Selon eux, la monétisation des données permettrait d'assurer une contrepartie de l'exploitation des données pour les personnes concernées. Pourtant, il apparaît

---

[1756] LAMBERTERIE (de) I., « Les ressources informationnelles en jouissance partagée : quels modèles propriétaires ? », *op. cit.*, p. 78.
[1757] *Ibid.*
[1758] TOMASSO L., LAUGA B. et PINET F., « Chaîne de confiance : des données partagées en transparence et en sécurité », *Perspective agricole*, 1er juin 2021.
[1759] ROCHFELD, J., « Contre l'hypothèse de la qualification des données personnelles comme des biens », *Les biens numériques*, CEPRISCA, 2015, p. 222.
[1760] THINK TANK GENERATION LIBRE, *Mes Data sont à moi, op. cit.*, p. 83

que cette solution n'est pas envisageable compte tenu de la valeur infime d'une donnée personnelle et du risque de perte d'appropriation des données vendues. Néanmoins, une entreprise a surfé sur cette idée et a développé une application TaData[1761] qui propose à de jeunes gens de vendre leurs données personnelles. Ces données sont donc monétisées. L'association Internet Society France a alerté la CNIL[1762] des agissements de la société TaData afin qu'elle mène une enquête sur le respect du Règlement général sur la protection des données (RGPD)[1763] de 2016 lors de la réalisation de ses activités. Étonnamment, la CNIL a mis fin à la procédure d'enquête en considérant, d'une part, que « *le service n'était pas encore déployé au niveau national* », mais surtout, d'autre part, que « *les travaux menés par le CEPD[1764] sur l'articulation entre la monétisation et le droit fondamental de la protection de la vie privée ne permettent pas à ce stade de considérer que le RGPD interdit la mise en œuvre de tels traitements* »[1765]. L'entreprise peut donc, pour le moment, poursuivre son activité. Pourtant cette décision semble aller à l'encontre même de la politique en vigueur pour les données personnelles. En effet, ces données font l'objet d'un régime de protection en droit français et en droit européen. Elles sont considérées comme l'émanation de la personne et le principe dominant est celui de l'autodétermination informationnelle. Il s'agit d'un principe consacré de manière implicite, mais « bienvenu » puisqu'il « *permet de donner à l'individu les moyens de demeurer libre de conduire son existence dans une société où le numérique prend une place croissante, une société qui l'amène à laisser, de plus en plus souvent, trace de ses données personnelles* »[1766]. Ce principe assure « *l'autonomie de décision de l'individu* ». Aussi, les données sont considérées comme une émanation de la personne, s'en dessaisir en les vendant serait vu par certains comme antinomique.

En outre, les données identifiantes des personnes physiques ne peuvent pas faire l'objet d'un droit de propriété[1767]. Reconnaître un tel droit mènerait à une impasse[1768]. D'ailleurs, le

---

[1761] ROZENFELD, S., « Données personnelles : Un pas vers la monétisation des données », *Expertises*, nov. 2020, n°462, p. 364.
[1762] Commission nationale informatique et libertés.
[1763] Règl. n°2016/679 du 27 avr. 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 : *JOUE* L 119/1 du 4 mai 2016.
[1764] Comité européen de la protection des données.
[1765] https://www.nextinpact.com/lebrief/44078/la-cnil-met-fin-au-controle-visant-tadata-pour-moment
[1766] MARTIAL-BRAZ, N., « Les nouveaux droits des personnes concernées », *Rev. Aff. Eur.*, 2018-1, pp. 7 à 17.
[1767] PADOVA, Y., « Entre patrimonialité et injonction au partage : la donnée écartelée », *op. cit.* ; MATTATIA, F. et YAICHE, M., « Être propriétaire de ses données personnelles (1ère partie) : peut-on recourir aux régimes traditionnels de propriété ? », *op. cit.* ; QUEMENER, M., *Le droit face à la disruption numérique, op. cit. ;* 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 », *RFDA*, n°6, 2015, p. 1157.
[1768] ANCIAUX, A. et FARCHY, J., « Données personnelles et droit de propriété : quatre chantiers et un enterrement », t. XXIX : *RIDE*, 2015/3, p. 307, spéc. pp. 329 à 330.

Conseil d'État dans son rapport de l'année 2014 sur le numérique et les droits fondamentaux propose que la protection de ces données soit vue comme un droit à la détermination personnelle plutôt qu'un droit de la propriété. De même, le Conseil National du Numérique estime, dans son avis de 2014, portant sur la neutralité des plateformes, que les données ne peuvent pas faire l'objet d'un droit d'exclusivité par leur appropriation « *parce qu'elle renvoie à l'individu la responsabilité de gérer et protéger ses données, renforce l'individualisme et nie le rapport de force entre consommateurs et entreprises ; parce qu'elle ne pourrait que générer des revenus anecdotiques pour les usagers et susciter à l'inverse un marché de la gestion protectrice des données numériques ; parce qu'elle déboucherait à un renforcement des inégalités entre citoyens en capacité de gérer, protéger et monétiser leurs données et ceux qui, par manque de littératie, de temps, d'argent ou autre, abandonneraient ces fonctions au marché* ». En outre, le droit des données personnelles est autonome et n'empêche pas pour autant d'appliquer des droits de propriété intellectuelle[1769]. Le traitement de données à caractère personnel suppose cependant de mettre en œuvre leur protection au regard de la personne physique identifiée ou identifiable. Cette protection permet aux personnes concernées d'obtenir la maîtrise juridique de leurs données à caractère personnel. Il semble alors primordial de soulever les problématiques liées spécifiquement à l'exploitation de telles données dans le secteur agricole. Ce qui conduit à envisager, tout d'abord, la maîtrise de l'usage des données à caractère personnel de l'exploitation agricole (**Section 1).** Cette analyse permettra, ensuite, de considérer les solutions envisageables pour le traitement des données à caractère personnel dans le secteur agricole (**Section 2**).

Section 1. La maîtrise de l'usage des données à caractère personnel de l'exploitation agricole

682- Tout d'abord, la mise en œuvre du droit des données à caractère personnel suppose d'identifier son objet, c'est-à-dire, les données à caractère personnel du secteur agricole **(§1**). Ensuite, il faudra envisager la mise en œuvre de la protection des données à caractère personnel **(§2**).

[1769] VIVANT M., « Données personnelles et propriété intellectuelle », *PI*, n°75, avr. 2020, pp. 58 à 67.

§1. *L'objet de la protection : les données à caractère personnel de l'exploitation agricole*

683. L'étude des données à caractère personnel du secteur agricole nécessite d'étudier, dans un premier temps, la notion de données à caractère personnel (**I**), pour, dans un second temps, envisager la condition de leur qualification, c'est-à-dire, l'identification d'une personne physique (**II**).

I. La notion de données à caractère personnel

684. Si la qualification des données à caractère personnel ne pose pas de difficulté, il semble, par ailleurs, que certains auteurs font l'amalgame entre données personnelles et vie privée. Aussi, il faudra se demander si la notion de donnée personnelle est toujours synonyme de vie privée. Il convient, donc, d'envisager, tout d'abord, leur qualification (**A**) pour, ensuite, s'intéresser à ce qui les distingue de la notion de vie privée (**B**).

A. La qualification de données à caractère personnel

685. La Loi Informatique et Liberté de 1978 renvoie désormais au RGPD pour la définition des données à caractère personnel[1770]. Il s'agit donc de « *toute information se rapportant à une personne physique identifiée ou identifiable* »[1771]. Cette définition laisse entendre une interprétation relativement large de la notion. Ainsi, il s'agit de « *toute information se rapportant à une personne physique* » (**1**) et cette identification peut être directe ou indirecte (**2**).

1. Toute information se rapportant à une personne physique

686. **Définition.** L'emploi de l'expression « *toute information* » exprime clairement la volonté du législateur d'en donner le sens le plus large possible. La loi ne distingue pas, selon la nature, le contenu, le format, la finalité ou encore les effets de l'information traitée. Elle peut donc être

[1770] Ord. n°2018-1125 du 12 déc. 2018 prise en application de l'article 32 de la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles : *JORF* n°0288 du 13 déc. 2018.
[1771] LIL, art. 2 renvoi au RGPD, art. 4.

de toute sorte[1772] et de toute forme. Il n'existe pas de limites d'interprétation et il importe peu que l'information soit issue d'un texte, d'une image, d'un dessin, d'un son ou, bien encore, d'une information GPS.

De plus, la loi ne distingue pas non plus selon le caractère objectif ou subjectif de l'information. Par conséquent, il pourrait tout aussi bien être question d'informations objectives portant sur l'âge, l'adresse ou encore le sexe d'une personne, que sur des informations subjectives portant sur un avis ou une appréciation de cette personne. Par ailleurs, la Cour de justice de l'Union européenne a eu l'occasion de valider cette interprétation élargie de la notion dans un arrêt du 20 décembre 2017[1773]. Ainsi, peu importe que les données se rapportent à des objets[1774] tant que cette chose matérielle est reliée à une personne physique. C'est le cas notamment de la plaque d'immatriculation d'un véhicule[1775] ou bien d'un plan cadastral ou d'une base géographique de référence[1776] qui lie la chose, le véhicule ou le terrain à la personne physique qui en est propriétaire.

687- **Individualisation de la personne concernée.** L'emploi des termes « *se rapportant* » laisse entendre que la donnée doit concerner la personne en cause. Celle-ci doit pouvoir être individualisée. Pour que cette condition soit satisfaite, les juges retiennent qu'il faut « *[qu'] en raison de son contenu, sa finalité ou son effet, l'information [soit] liée à une personne déterminée* »[1777]. Ainsi, le G29 devenu le Comité européen de la protection des données (CEPD) retient qu'il peut s'agir des « *données concernant une personne si elles ont trait à l'identité, aux caractéristiques ou au comportement d'une personne ou si cette information est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée* »[1778].

688- **Exclusion des personnes morales.** La loi fait référence uniquement à la « *personne physique* ». En effet, depuis la directive de 1995, les personnes morales sont exclues du champ d'application de la loi sur la protection des données à caractère personnel. La donnée doit donc nécessairement porter sur une personne physique, mais cette condition peut comporter des subtilités qu'il conviendra d'analyser plus loin[1779].

[1772]Groupe de travail « Article 29 » sur la protection des données, *avis n°4/2007 sur le concept de données à caractère personnel*, 20 juin 2007, WP 136, p. 7
[1773] CJUE, 20 déc. 2017, *Peter Nowak* c/ *Data Protection Commissioner*, aff. C-434/ 16.
[1774] Groupe de travail « Article 29 » sur la protection des données, *avis n°4/2007*, *op. cit.*, p. 10.
[1775] CNIL, délib. n°2008-001 du 10 janv. 2008 et n°2008-466 du 27 nov. 2008.
[1776] CNIL, délib. n°2007-301 du 25 oct. 2007 portant avis sur un projet d'arrêté relatif à la mise en place d'un traitement de données à caractère personnel dénommé « Service de consultation du plan cadastral — SCPC ».
[1777] CJUE, 20 déc. 2017, arrêt préc., pt 35.
[1778]G29, *Document de travail sur les questions de protection des données liées à la technologie RFID*, (radio-identification), WP 105, 19 janv. 2005, p. 9.
[1779] Voir *infra*, n°705 et s.

2. Une identification directe ou indirecte

689- **Étendue de l'identification.** S'agissant de l'identification de la personne physique, celle-ci peut être identifiée ou seulement identifiable. Ce qui signifie qu'elle peut être identifiée « *directement ou indirectement* »[1780]. L'article 4 du RGPD prévoit plusieurs exemples d'identification directe ou indirecte « ***notamment**, par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale* » [nous soulignons][1781]. Cette liste n'est pas exhaustive, il s'agit simplement d'une liste exemplative.

690- **Critère d'appréciation de l'identification**. Le critère retenu par le RGPD pour déterminer si une personne physique est identifiée ou identifiable réside dans les « *moyens raisonnablement susceptibles d'être utilisés* » par le responsable de traitement. Ces moyens s'apprécient au regard de l'ensemble des « *facteurs objectifs* », tels que le coût de l'identification et le temps nécessaire utilisé, « *en tenant compte à la fois des technologies disponibles au moment du traitement et de l'évolution de celles-ci* »[1782]. De toute évidence, l'interprétation de la notion est suffisamment large pour que son application soit la plus étendue possible.

B. La distinction des notions de vie privée et de données à caractère personnel

691- La question se pose de savoir si le caractère professionnel du secteur agricole empêche de reconnaître l'existence de données à caractère personnel pour celles que ce secteur génère. En effet, certains auteurs font le lien entre vie privée et données personnelles et estiment que la vie privée n'a pas lieu d'être dans le secteur agricole. C'est ainsi que Mme Simone Van der Burg, de l'Université de Wageningen, aux Pays-Bas, retient que la vie privée n'entre pas dans l'éthique de l'agriculture numérique. De ce principe ces auteurs en tirent la conclusion que les données agricoles ne sont, généralement, pas considérées comme des données à caractère personnel[1783]. Ils font donc le lien entre respect à la vie privée et protection des données à caractère personnel. Or, il semble que si ces deux notions se complètent, elles restent, malgré tout, autonomes. Le régime des données personnelles pourrait ainsi s'appliquer sans qu'il y ait

[1780] RGPD, art. 4, 1er.
[1781] *Ibid.*
[1782] RGPD, cons. 26.
[1783] GODAN, *Webinar: Farmers rights on Data and ownership issues*, 18 sept. 2018.

nécessairement une atteinte au respect à la vie privée lors de leur exploitation. Ainsi, plusieurs problématiques doivent être identifiées. La première suppose de se questionner sur le lien existant entre vie privée et protection des données à caractère personnel (**1**). Cette analyse permettra d'envisager la seconde problématique qui consiste à se demander si la protection de la vie privée est autonome de la protection des données à caractère personnel (**2**).

1. Vie privée et protection des données à caractère personnel

692- **Notion de vie privée**. Afin d'analyser l'application de la vie privée aux données personnelles, il convient d'envisager d'abord la notion de vie privée. Or, il n'existe pas de définition légale de cette notion[1784]. La doctrine en a fourni des éléments de définition. M. le Professeur J. Carbonnier, par exemple, définit la vie privée comme « *une sphère secrète de vie où [l'individu] aura le pouvoir d'écarter les tiers* »[1785]. M. le Professeur G. Cornu la définit comme « *la sphère d'intimité de chacun* »[1786]. La jurisprudence a, également, donné des éléments de définition de cette notion. En effet, l'avocat général Me J.-P. Cabanes a défini le droit à la vie privée dans un arrêt de la Cour d'appel de Paris de 1970, comme « *le droit pour une personne d'être libre de mener sa propre existence avec le minimum d'ingérence extérieure* »[1787].

Malgré l'absence de définition, le droit au respect de la vie privée a été consacré dans de nombreux textes internationaux[1788]. Ce n'est qu'en 1970 que le législateur français a « *de façon solennelle* »[1789] introduit cette protection à l'article 9 du Code civil[1790]. Il s'agit, donc, d'une notion primordiale érigée en droit fondamental. Par ailleurs, le droit à la vie privée ne fait pas de distinction entre une personne physique et une personne morale, il s'applique à toutes les personnes.

693- **Notion de protection de données à caractère personnel.** Concernant le droit à la protection des données à caractère personnel, il s'agit de la protection des informations se rapportant à une personne physique identifiée ou identifiable.

Si ces notions de vie privée et de protection des données à caractère personnel se complètent, il n'en demeure pas moins que leurs régimes sont distincts. En effet, il est fait

---

[1784] FERAL-SCHUHL, C., ss. dir, *Cyberdroit*, *op. cit.*, n°713.42.
[1785] CARBONNIER, J., *Droit civil, Les personnes*, t.1, PUF,2017, n°278, p. 518.
[1786] CORNU, G., *Vocabulaire juridique*, 12e éd., PUF, 2018.
[1787] Concl. de l'avocat général J. Cabanes, CA Paris, 7ème ch., 15 mai 1970.
[1788] DUDH, art. 12 ; Conv. EDH, art. 8 ; Conv. EDH, art. 17 ; Pacte international relative aux droit civils et politiques ; Charte des droits fondamentaux, art. 7.
[1789] STIRN, B., *Les libertés en question*, 8e éd. LGDJ, 2013, p. 26.
[1790] C. civ., art. 9 : « *Chacun a droit au respect de sa vie privée* ».

mention à l'article 1er de la Loi Informatique et Liberté[1791] que « *l'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la* ***vie privée****, ni aux libertés individuelles ou publiques* » [nous soulignons]. À la lecture de cet article, le droit au respect à la vie privée n'est que l'un des droits fondamentaux auxquels l'informatique ne doit pas porter atteinte au même titre que le droit à la protection des données personnelles. Ainsi, ce dernier a *« acquis une place autonome parmi les droits fondamentaux* »[1792], il a été consacré aux articles 8, §1 de la Charte des droits fondamentaux de l'Union européenne et 16, §1 du Traité sur le Fonctionnement de l'Union européenne. C'est pourquoi « *des informations susceptibles d'être considérées comme portant atteinte à la "vie privée"* ***peuvent*** *aussi relever du statut des "données personnelles"* » [nous soulignons][1793] mais ce lien n'est pas systématique. Si des informations portent atteinte à la vie privée, elles ne sont pas forcément couvertes par le droit des données personnelles et inversement.

2. Caractère autonome de la protection des données personnelles

694 **Autonomie des régimes de protection.** Si le droit à la protection des données personnelles peut être un prolongement du droit au respect de la vie privée[1794] et que la notion de vie privée est parfois sous-jacente à la question de la protection des données à caractère personnel, il apparaît, néanmoins, que ces deux notions ne sont pas synonymes[1795]. Ceci implique que le régime de la protection des données à caractère personnel peut trouver à s'appliquer même s'il n'y a pas d'atteinte à la vie privée. Il suffit qu'une personne physique soit identifiée ou identifiable pour que la protection des données à caractère personnel s'applique.

Ainsi, « *la référence au droit à la vie privée n'est pas toujours justifiée* »[1796] dans les affaires ayant pour objet la protection de données à caractère personnel. En effet, parfois, dans de telles affaires, l'atteinte à la vie privée ne fait pas débat. Cette position a été confirmée

[1791] Loi n°78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés : *JORF* du 7 janv. 1978.
[1792] CLEMENT-FONTAINE, M., « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *Légicom*, 2017/2, n°59, p. 64.
[1793] 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*, n°48, (dossier vie privée), juin 2015, pp. 21 à 33.
[1794] TINIERE, R., « L'apport de la Charte des droits fondamentaux à la protection des données personnelles dans l'Union européenne », *Rev. Aff. Eur.*, 2018/1, pp. 29 à 34.
[1795] FERAL-SCHUHL, C., ss. dir., *Cyberdroit*, *op. cit.*, n°111.132.
[1796] CLEMENT-FONTAINE, M., « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *op. cit.*

notamment dans un arrêt de la CJUE du 17 juillet 2014[1797]. Dans cet arrêt, la collecte d'informations à caractère personnel n'entraînait aucun risque d'atteinte à la vie privée, ce qui n'empêchait pas pour autant de faire application du droit à la protection des données à caractère personnel. Pour supprimer tout doute, la jurisprudence a admis que « *les données relatives à la vie professionnelle d'un individu ou à ses activités commerciales* »[1798] relèvent du champ des données personnelles sans qu'il y ait pour autant atteinte à la vie privée. Il en va de même pour les noms et prénoms des fonctionnaires européens et des personnes figurant sur les listes de réserve des concours de recrutement organisés par l'Union européenne[1799]. Les juges ont donc admis que la vie privée des individus n'entrait pas dans les conditions d'application de la protection, il suffit qu'une personne physique soit identifiée ou identifiable. De toute évidence, le droit à la protection des données à caractère personnel est autonome vis-à-vis du droit à la vie privée.

695- **Application de la protection des données personnelles au secteur agricole.** En ce qui concerne les données du secteur agricole, et pour reprendre l'étude menée par le *Think tank* Renaissance Numérique[1800], les données collectées sur les exploitations agricoles concernent avant tout des informations nécessaires pour l'activité professionnelle[1801]. Il peut s'agir de données sur les semences et intrants, des données de terrain ou encore des données parcellaires. Ces données reflètent avant tout une activité professionnelle et ne concernent pas directement une personne physique. Pourtant, en y regardant de plus près, et comme il le sera démontré plus loin[1802], la plupart de ces données lors de leur traitement vont permettre l'identification d'une personne physique.

696- ***Ubi lex non distinguit nec nos distinguere debemus***. Selon cette maxime latine, là où la loi ne distingue pas, il n'y a pas lieu de distinguer. Par conséquent, dès lors que la loi ne fait pas référence à une exception quant à l'application du régime des données à caractère personnel, toute information se rapportant à une personne physique identifiée ou identifiable doit être considérée comme telle. C'est pourquoi les données générées ou produites sur les exploitations agricoles permettant d'identifier une personne physique devront être traitées dans le respect du

[1797] CJUE, 17 juillet 2014, aff. jtes C-141/12 et C-372/12, pt 54 renvoie aux arrêts *Connolly* c/ *Commission*, C-274/99 P, pt 37 ; *Österreichischer Rundfunk* e. a., C-465/00, C-138/01 et C-139/01, pt 68, ainsi que *Google Spain* et *Google*, C-131/12, EU:C:2014:317, pt 68.
[1798] TERWANGNE (de), C. et ROSIER, K., *Le règlement général sur la protection des données (RGPD/GDPR)*, Analyse approfondie, Larcier, 2018.
[1799] TPI, 7 juill. 2011, *Gregorio Valero Jordana* c/ *Commission*, T-161/04, pt 91.
[1800] THINK TANK GENERATION LIBRE, *La valeur des données agricoles*, *op. cit.*
[1801] Voir Tableaux de la note du *Think tank* Renaissance numérique sur la valeur des données agricoles, févr. 2018.
[1802] Voir *infra*, n°698 et s.

droit à la protection des données personnelles. Par ailleurs, la CNIL avait retenu que la « *circulation d'informations concernant une personne peut avoir de graves conséquences sur* ***sa vie privée et professionnelle****, parfois plusieurs années après les faits* » [nous soulignons][1803]. Cette affirmation conforte, un peu plus, l'idée selon laquelle la protection des données à caractère personnel ne s'arrête pas à la protection de la vie privée, mais peut bien porter atteinte, entre autres, à la vie professionnelle de l'individu identifié. Il faut relever toutefois que l'atteinte à la vie professionnelle, par le traitement des données à caractère personnel, n'est pas une condition de l'application de la protection. Il s'agit seulement d'une conséquence de ce traitement.

II. La condition *sine qua non* de la protection : l'identification d'une personne physique

697. Au vu des éléments précédemment évoqués, il apparaît que la protection des données à caractère personnel ne se réfère qu'à la simple identification d'une personne physique. Il est donc nécessaire de caractériser ce qu'est une personne physique (**A**). Toutefois, l'exclusion de principe des personnes morales doit être nuancée (**B**).

A. La caractérisation d'une personne physique

698. Afin de caractériser au mieux les données agricoles se rapportant à une personne physique (**2**), il faut, tout d'abord, se référer aux éléments d'identification de cette personne (**1**).

1. Les éléments d'identification d'une personne physique

699. **Critères d'identification des personnes physiques.** Les informations sont des données à caractère personnel lorsqu'en raison de leur contenu, de leur finalité ou de leur résultat[1804] elles sont liées à une personne physique déterminée. Il peut donc s'agir des « *données concernant une personne si elles ont trait à l'identité, aux caractéristiques ou au comportement d'une*

[1803] CNIL, « Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles », 34e rapport d'activité, *La documentation française*, 2013, p. 16.
[1804] G29, *avis 4/2007, op. cit.*, pp. 11 à 13.

personne ou si cette information est utilisée pour déterminer ou influencer la façon dont cette personne est traitée ou évaluée »[1805].

700- **Liste exemplative de données personnelles**. À la lecture de la jurisprudence, une liste de données identifiantes, toujours plus étendue, peut être exposée. Ainsi, la personne physique peut directement être identifiée par un nom, un sexe, une date et un lieu de naissance ou une nationalité[1806]. Elle peut être identifiée également de manière indirecte par des références d'un passeport ou d'une carte nationale d'identité, ou des coordonnées personnelles et/ou professionnelles[1807], d'un matricule interne[1808], de coordonnées électroniques[1809], mais aussi, de photographies, de vidéos ou encore de voix enregistrées. De même, un numéro de sécurité sociale, un numéro de référence, des coordonnées bancaires, des habitudes de vie, des comportements de consommation ou bien des informations relatives à la situation géographique[1810] doivent être considérés comme des données à caractère personnel. Il faut aussi noter que les données se rapportant à un véhicule tel qu'un numéro de série, un identifiant unique de pièce ou une plaque d'immatriculation sont des données à caractère personnel dès lors qu'elles permettent d'identifier une personne physique[1811]. La CJUE a par ailleurs considéré l'adresse IP comme une donnée personnelle[1812] et la CNIL a fait de même avec les données d'une chaîne de blocs[1813]. Pour finir, les données pseudonymisées sont également considérées comme personnelles. Seules les données anonymisées seront en définitive exclues de cette catégorie.

701- **Identification relative à des considérations extérieures**. En réalité, les éléments d'identification des données à caractère personnel dépendent des circonstances de la collecte des informations et des moyens d'identification. À titre d'exemple, un nom de famille répandu

---

[1805] *Ibid.* ; *Document de travail sur les questions de protection des données liées à la technologie RFID, op. cit.*, p. 9.

[1806] CJUE, 20 déc. 2017, *Peter Nowak* c/ *Data Protection Commissioner*, préc. ; CJUE, 29 juin 2010, *Commission* c/ *Bavarian Lager*, aff. C-28/ 08 P ; CJCE, 16 déc. 2008, *Heinz-Huber* c/ *Bundersrepublik Deutcshland*, aff. C-524/06.

[1807] CJUE 9 mars 2017, *Camera di Commercio, industria, Artigianato e Agricoltura di Lecce c/ Salvatore Manni*, aff. C-398/15.

[1808] CJUE, 3e ch., *Worten*, aff. C-342/ 12.

[1809] Crim., 14 mars 2006, n°05-83.423.

[1810] CNIL, délib. n°2006-067, 16 mars 2006 ; CNIL, délib. n°2010-096, 8 avr. 2010 ; Soc., 3 nov. 2011, n°10-18.036, CNIL délib. med.-2018-022/023.

[1811] CNIL, *Pack de conformité : véhicules connectés*, oct. 2017 pp. 5-6. EDPB, Guideline 1/2020, 28 janv. 2020, p. 7, pt. 28.

[1812] CJUE 19 oct. 2016, *Patrick Breyer c/ Bundesrepublic Deutschland*, aff. C-582/ 14 et C. cass., 1ere civ., 3 nov. 2016, n°15-22.595.

[1813] CNIL, *Blockchain et RGPD : Quelles solutions pour un usage responsable en présence de données personnelles ?*, 24 sept. 2018.

à l'échelle nationale ne sera pas identifiant, alors que dans un secteur restreint il pourra l'être. Par conséquent, un grand nombre de données permettent d'identifier une personne physique.

2. Les données identifiantes du secteur agricole

702- **Étendue des données à caractère personnel du secteur agricole.** Un grand nombre de données collectées sur les exploitations agricoles peuvent être considérées comme personnelles du moment qu'une personne physique est identifiée ou identifiable. Dans ce sens, les syndicats agricoles affirment que « *les données au niveau de l'exploitation sont collectées par les agriculteurs eux-mêmes et peuvent contenir des données à caractère personnel* »[1814]. À titre d'exemple, les données GPS d'une machine agricole, une immatriculation ou encore des habitudes professionnelles peuvent se révéler identifiantes. De même, une culture de banane dans le Sud de la France sera assez unique pour permettre l'individualisation et l'identification de l'exploitant agricole.

703- **Enjeux de la protection des données à caractère personnel du secteur agricole.** En ce qui concerne les enjeux de la protection des données à caractère personnel, il est opportun d'envisager l'exemple des données collectées au moyen des ruches connectées. En effet, les balances connectées situées dans les ruches[1815] envoient des informations précieuses aux apiculteurs concernant le poids de la ruche afin de connaître le moment idéal pour collecter le miel. Ces ruches sont directement liées aux systèmes informatiques des apiculteurs, ce qui en fait des données à caractère personnel dès lors que la personne physique est identifiable. Ces données sont d'autant plus sensibles qu'elles donnent des renseignements sur le lieu où se situe la ruche et font craindre un risque accru de vol de ces ruches. Par conséquent, le partage de ces informations peut avoir de lourdes conséquences sur l'activité des apiculteurs.

704- **Qualification des données agricoles au cas par cas.** Parfois, il arrive que les pouvoirs publics ou les acteurs du secteur agricole eux-mêmes qualifient certains jeux de données de personnels. C'est le cas notamment des données génétiques des animaux d'élevage et des données de télédétection. Il faut s'interroger alors sur la validité des qualifications générales.

En ce qui concerne les données génétiques, un arrêté émanant du ministère de l'Agriculture du 24 mars 2015[1816], aujourd'hui abrogé, soumettait en son article 5 l'accès des

[1814] COPA COGECA, *Grands principes de la collecte, de l'utilisation et de l'échange des données agricoles*, 2016.
[1815] Projet Miellées soutenu par ITSAP : Mise en place d'un outil de valorisation des données par l'élaboration d'un portail pour le partage des données des balances connectées, voir *supra*, n°459 et s.
[1816] Arrêté du 24 mars 2015 relatif aux systèmes nationaux d'information génétique des espèces bovine, ovine, caprine et porcine : *JORF* n°0083 du 9 avr. 2015, art. 5 : « *Les données mentionnées à l'article 2 du présent arrêté*

personnes et organismes intéressés par les données portant sur les informations génétiques des espèces bovine, ovine, caprine et porcine au respect des dispositions relatives à la protection des données personnelles, au sens de la Loi Informatique et Libertés (LIL) de 1978. La formulation laissait entendre que toutes les données de cette catégorie devaient être protégées au titre de la LIL et présumait de leur caractère personnel. Or, de prime à bord, les données génétiques ne sont pas nécessairement identifiantes dès lors qu'aucune personne physique n'est identifiable lors de leur traitement. Un arrêté du 16 janvier 2019[1817] a abrogé ces dispositions et prévoit désormais dans ses dispositions générales à l'article 1 que « *les apporteurs ou utilisateurs des données du système national d'information génétique mettent en œuvre les dispositions nécessaires au respect du règlement (UE) 2016/679 et de la loi n°78-17 du 6 janvier 1978, modifiée en dernier lieu par la loi n°2018-493 du 20 juin 2018* ». Il semble qu'il faille y lire une application plus mesurée de la réglementation sur les données à caractère personnel. La nouvelle formulation de l'article rappelle simplement que le rapporteur ou l'utilisateur des données génétiques doit respecter les dispositions sur les données à caractère personnel dès lors qu'elles sont présentes dans le système national d'information génétique. Ainsi, les apporteurs et les utilisateurs doivent faire application de cette réglementation lorsqu'ils accèdent au système national d'information génétique. Par conséquent, aujourd'hui, la publication des données génétiques de l'élevage doit se faire dans des systèmes nationaux d'information génétique des espèces bovine, ovine, caprine et porcine, en *Open Data*, dans le respect de la réglementation sur les données à caractère personnel.

S'agissant des données de télédétection, la Copa Cogeca distingue les données collectées au niveau de l'exploitation qui pourraient avoir un caractère personnel de celles qui sont « *issues de la télédétection […] collectées à l'aide d'infrastructures publiques* ». Celles-ci ne seraient « *pas considérées comme privées* »[1818]. Pourtant cette supposition est erronée puisque le caractère public de l'infrastructure permettant de collecter les données n'induit pas le régime applicable à ces données. Ainsi comme il l'a été démontré par ailleurs[1819], le caractère privé ou public d'une donnée ne présume pas de son caractère personnel ou non. Par conséquent, dès lors que les données télédétectées permettront d'identifier une personne physique, si tant est que ce soit possible, alors il pourra s'agir de données à caractère personnel.

---

sont accessibles aux personnes et organismes suivants, dans le respect des dispositions relatives à la protection des données personnelles fixées par la loi du 6 janvier 1978 susvisée ».

[1817] *Ibid.*

[1818] COPA COGECA, *Grands principes de la collecte, de l'utilisation et de l'échange des données agricoles*, *op. cit.*

[1819] Voir *supra*, n°694.

Le caractère public de la collecte pourra, dans certains cas, servir de base légale pour justifier cette collecte.

Ces exemples permettent de démontrer l'importance d'analyser au cas par cas les données collectées afin de rechercher leur potentiel caractère personnel. *A priori* de nombreuses données collectées dans le secteur agricole pourront être considérées comme personnelles, ce qui impliquera nécessairement pour les responsables de traitement de respecter le RGPD.

B. L'exclusion nuancée des données de la personne morale

705- Si les personnes morales ont toujours été exclues du champ d'application de la loi sur la protection des données à caractère personnel (**1**), il n'en demeure pas moins qu'en analysant plus finement les données, il apparaît que la personne physique est la plupart du temps identifiable à travers la forme sociétale (**2**).

1. Une exclusion de principe

706- **Exclusivité des personnes physiques.** Le considérant 14 du RGPD prévoit que « *le présent règlement ne couvre pas le traitement des données à caractère personnel qui concernent les personnes morales, et en particulier des entreprises dotées de la personnalité juridique, y compris le nom, la forme juridique et les coordonnées de la personne morale* ». Ainsi, le législateur refuse « *[l'] élargissement du champ d'application de la loi aux personnes morales* »[1820]. Ces dernières sont donc exclues par principe de la réglementation sur les données à caractère personnel alors qu'elles ne le sont pas de la notion de vie privée. Par conséquent, seules les personnes physiques peuvent bénéficier de la protection applicable au titre du RGPD.

707- **Exclusion des sociétés agricoles.** Dans le secteur agricole, de nombreux exploitants ont une forme sociétale. Il peut s'agir d'un groupement agricole d'exploitation en commun (GAEC), d'une exploitation à responsabilité limitée (AERL), d'une société civile d'exploitation agricole (SCEA) ou encore d'une société anonyme (SA), d'une société à responsabilité limitée (SARL), d'une coopérative, d'un groupement de fait, etc. Dès lors que l'exploitation est organisée en société, le patrimoine de celle-ci est distinct de celui de la personne physique. Toutes les données collectées qui auront trait seulement à la personne morale ne pourront donc pas entrer dans la catégorie des données à caractère personnel. Au contraire, les exploitations agricoles

[1820] BENABOU, V.-L., « L'extension du domaine de la donnée », *Légicom*, 2017/2, n°59, pp. 3 à 17.

exploitées à titre individuel ou autrement dit en nom propre voient leurs patrimoines personnel et professionnel mélangés. Dans ce cas, l'entreprise individuelle ne bénéficie pas de la distinction des personnes (chef d'entreprise et personne morale). Par conséquent, les données collectées sur une telle exploitation pourront plus facilement bénéficier de la protection des données à caractère personnel puisque la personne physique sera plus aisément identifiable. Néanmoins, il semble que cette exclusion de principe des personnes morales soit relativement limitée.

2. Une exclusion limitée

708- **Identification incidente des personnes physiques.** En analysant de plus près les données relatives aux personnes morales, l'identification des personnes physiques peut souvent se faire de manière incidente. Comme le relève un avis du G29[1821], le traitement des données des personnes morales permet parfois d'identifier les personnes physiques, notamment par les noms, prénoms, coordonnées personnelles des dirigeants ou d'autres responsables qu'ils soient administratifs ou financiers[1822]. Dès lors, les personnes physiques identifiées pourront bénéficier des droits qui leur sont accordés, tels que la portabilité ou l'accès à ces données.

709- **Contours de la détermination d'une personne physique à définir.** Les contours de la détermination des données d'une personne physique doivent encore être délimités par la pratique et la jurisprudence. Un arrêt de la Cour de justice de l'Union européenne du 9 novembre 2010[1823] au sujet de l'invalidité partielle de la réglementation de l'Union sur la publication des informations relatives aux bénéficiaires de fonds européens agricoles a eu l'occasion de préciser à ce sujet que « *le respect du droit à la vie privée à l'égard du traitement des données à caractère personnel, reconnu par la charte des droits fondamentaux de l'Union européenne, se rapporte à toute information concernant une personne physique identifiée ou identifiable […] les personnes morales ne peuvent se prévaloir de la protection des articles 7 et 8 de la charte à l'égard d'une telle identification que dans la mesure où le nom légal de la personne morale identifie une ou plusieurs personnes physiques* »[1824].

[1821] Avis 4/2007, *op. cit*., p. 26.
[1822] CNIL, dél. n°84-28, 3 juill. 1984 *D.* 1984 ; CJUE, 9 nov. 2010 *Volker und Markus Schecke GbR et Hartmut Eifert c/ Land Hessen*, Aff. jointes C-92/09 et C-93/09 ; CJUE 9 mars 2017 *Camera di Commercio*, préc.
[1823] CJUE, 9 nov. 2010, *Volker*, préc.
[1824] CAQUE, S., « Réflexions juridiques autour de l'articulation entre l'ouverture des données publiques et la protection des données personnelles », in BOURCIER, D. et FILIPPI (De), P., ss. dir., *Open Data & Big Data, Nouveaux défis pour la vie privée*, mare & martin, 2016, p. 205.

710- **Identification circonstanciée.** Comme le relève un auteur « *l'identification d'une personne physique est donc indirectement possible après avoir fait ressortir ses liens avec une personne morale* »[1825]. En outre, une personne morale dont le nom est celui de l'agriculteur en totalité ou en partie permet une identification[1826]. Tout dépendra des moyens raisonnablement utilisés pour l'identification des personnes physiques. Néanmoins, lorsque seule la personne morale est identifiée ou identifiable, il n'y a pas lieu d'appliquer le droit des données personnelles. La société peut faire « écran » aux personnes physiques. Les agriculteurs y voient, d'ailleurs, un risque d'injustice[1827], puisque ceux qui sont installés en tant que personnes physiques bénéficieront automatiquement du régime de protection du RGPD dès lors que les données de leur exploitation permettront de les identifier, alors que ceux installés en forme de société ne bénéficieront pas de la protection si seulement la société est identifiable. Cependant, bien souvent dans le secteur agricole, le nom de l'agriculteur se retrouve dans le nom de la société, les données identifiant la personne morale rendront donc identifiable la personne physique.

Ainsi, l'existence de données à caractère personnel dans le secteur agricole ne laisse aucun doute. Il faut alors se demander quels sont les effets de la protection des données à caractère personnel dans le secteur agricole.

§2. *La mise en œuvre de la protection des données à caractère personnel*

711- Si d'un côté les responsables de traitement voient leur responsabilité engagée (**I**), les personnes concernées disposent, d'un autre côté, de droits accrus sur leurs données (**II**).

I. La responsabilisation des entreprises de l'*AgTech* en tant que responsables de traitement

712- Tout d'abord, les responsables de traitement doivent respecter le principe de licéité de l'opération de traitement. Il faudra donc envisager les effets de ce principe dans le secteur agricole (**A**). Ensuite, les responsables de traitement sont soumis à certaines obligations qui leur incombent (**B**).

[1825] *Ibid.*
[1826] BEGUIN-FAYNEL, C., « La problématique de l'appropriation des données agricoles », *op. cit.*
[1827] BRUN, F., « Quelles opportunités et craintes sur les échanges de données de données agricoles ? Points de vue des agriculteurs », *Multipass,* 14 janv. 2019.

A. Le principe de licéité de l'opération de traitement

713- La protection des données à caractère personnel suppose l'existence d'un traitement (**1**) qui repose sur une cause licite (**2**).

1. Le traitement des données à caractère personnel

714- Définition de l'opération de traitement. L'article 2 de la LIL[1828] renvoie aux définitions de l'article 4 du RGPD[1829], sauf disposition contraire. L'opération de traitement est ainsi définie comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou à des ensembles de données à caractère personnel* ». La LIL est applicable à la fois aux traitements automatisés et non automatisés, par conséquent, les données à caractère personnel peuvent tout aussi bien figurer dans des bases de données que dans des fichiers. Le fichier étant, ici, défini comme « *tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés* »[1830]. Le RGPD fournit des exemples de traitements dans une liste non exhaustive, il peut s'agir de « *la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

Ainsi, toute opération sur des données à caractère personnel peut être considérée comme un traitement de données à caractère personnel au sens du RGPD. C'est, en effet, ce que la CJUE a admis dans l'arrêt *Google Spain* du 13 mai 2014[1831]. Aussi, comme l'affirme Mme la professeure V.-L. Benabou, « *les cas d'application sont nombreux et couvrent des*

[1828] LIL, art. 2 : « *Traitements automatisés en tout ou partie de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, lorsque leur responsable remplit les conditions prévues à l'article 3 de la présente loi, à l'exception des traitements mis en œuvre par des personnes physiques pour l'exercice d'activités strictement personnelles ou domestiques* ».

[1829] RGPD, art. 4 : « *Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou à des ensembles de données à caractère personnel telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».

[1830] LIL, art. 2, al. 2.

[1831] CJUE, *Google Spain SL, Google Inc. c/ Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, 13 mai 2014, aff. C-131/ 12 : *JO* C 212 du 07 juill. 2014, p. 4.

activités devenues essentielles dans l'économie de l'information telles que les activités de référencement, de préconisation ou encore de géolocalisation »[1832].

715- **Traitements exclus.** Certaines opérations de traitement sont exclues de la protection des données à caractère personnel, telles que les opérations de traitement « *mis en œuvre par des personnes physiques pour l'exercice d'activités strictement personnelles ou domestiques* »[1833]. Ainsi, lorsque le traitement de données à caractère personnel a vocation à rester confidentiel, le RGPD ne sera pas applicable.

716- **Limite technologique.** Il existe une limite concernant l'évolution des technologies qui permettent d'identifier une personne physique. À ce sujet, certains auteurs évoquent un « *flou technologique* » de la notion de données à caractère personnel[1834]. À cette fin, le considérant 26 du RGPD précise que l'identification de la personne physique doit se faire « *aux moyens raisonnablement susceptibles d'être utilisés par le responsable de traitement ou par toute autre personne* »[1835]. Le caractère raisonnable doit s'apprécier au regard de « *l'ensemble des facteurs objectifs tels que le coût de l'identification et le temps nécessaire, mais également des technologies disponibles au moment du traitement et de l'évolution de celles-ci* »[1836]. Or, avec l'évolution des technologies, « *les traitements qui étaient excessivement complexes et coûteux deviennent désormais suffisamment simples pour être rentables et permettre des identifications à partir de données pleines de "bruit"* »[1837]. De fait, l'identification de données personnelles est de plus en plus simple. La notion est aujourd'hui étendue « *à de nouvelles formes d'identification des individus et aux traces de leurs échanges numériques* »[1838]. Néanmoins, il ne faut pas oublier que si elle évolue, la technologie demeure une limite aux possibilités de traitement. Ainsi, seules les données anonymisées rendant impossible l'identification d'une personne physique ne sont pas considérées comme des données personnelles. Ces données ne supposent donc pas l'application des règles du RGPD.

[1832] BENABOU, V. -L., « L'extension du domaine de la donnée », *op. cit.*, p. 8.
[1833] LIL, art. 2.
[1834] MANCOSU, G., « La transparence publique par l'ouverture des données personnelles ? Focus sur les systèmes juridiques italien et français », in BOURCIER D. et FILIPPI (De) P., ss. dir., *op. cit.*, p. 69.
[1835] RGPD, cons. 26.
[1836] *Ibid.*
[1837] BENABOU, V. -L., « L'extension du domaine de la donnée », *op. cit.*, p. 6.
[1838] *Ibid.*

2. La cause licite du traitement

717- **Conditions de licéité.** La cause du traitement doit être licite, ce qui signifie qu'elle doit s'appuyer sur des finalités déterminées, explicites et, entre autres, légitimes[1839]. Les données ne doivent pas non plus être « *traitées ultérieurement de manière incompatible avec ces finalités* »[1840]. Dans ce cas, tout traitement ultérieur doit faire l'objet d'un test de compatibilité[1841] avec le traitement initial des données personnelles, sauf si le responsable de traitement a obtenu le consentement de la personne concernée ou que le traitement est fondé sur le droit de l'Union ou le droit d'un État membre. En cas d'incompatibilité, le traitement ultérieur est illicite. Il faut noter qu'il existe une présomption de compatibilité avec le traitement initial concernant les traitements ultérieurs à des fins de recherche scientifique ou à des fins statistiques[1842]. Ce traitement ultérieur à des fins de recherche doit néanmoins être exécuté de sorte que les personnes concernées ne soient pas ou plus identifiées[1843] par la pseudonymisation ou l'anonymisation. Également, il faut que des garanties soient prises quant aux mesures techniques et organisationnelles *« en particulier pour assurer le principe de minimisation des données* »[1844]. Le principe de minimisation oblige à n'obtenir que des données adéquates, pertinentes et limitées au regard des finalités pour lesquelles elles sont traitées[1845].

718- **Notion de finalité.** À la lecture du RGPD et de la LIL, la notion de finalité n'a pas été définie. Cette notion irrigue pourtant la protection des données à caractère personnel. Le G29 a apporté une définition à la notion de finalité dans un avis de 2014 et a retenu « *[qu'] en matière de protection des données, la "finalité" est la raison spécifique pour laquelle les données sont traitées : le but ou l'intention de leur traitement* »[1846].

Ce sont les articles 6 du RGPD et 5 de la LIL qui fixent de manière limitative six finalités envisageables par le responsable de traitement pour faire reposer son opération de traitement. Ainsi, le traitement est licite si la personne concernée a donné son consentement ou bien si le traitement est nécessaire à l'exécution d'un contrat, au respect d'une obligation légale, à la

[1839] RGPD, art. 5 et LIL, art 4.2.
[1840] *Ibid*.
[1841] RGPD, art.4.
[1842] RGPD, cons. 50 et LIL, art. 4 et art. 79 ; Pour un exemple, voir *supra*, n°161.
[1843] RGPD, cons. 156.
[1844] RGPD, art. 89.
[1845] RGPD, art. 5. 1. c).
[1846] G29, *avis n°06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, WP217, adopté le 9 avril 2014, p. 26.

sauvegarde des intérêts vitaux, à l'exécution d'une mission d'intérêt public, à des fins d'intérêts légitimes[1847].

Il est à noter que la recherche scientifique n'a pas été retenue comme une finalité autorisant un traitement de données à caractère personnel dispensant de l'obtention du consentement de la personne physique. Par conséquent, les organismes et instituts de recherche doivent, en principe, faire reposer leur traitement sur le consentement de la personne concernée. Toutefois, le CEPD a reconnu que l'intérêt légitime pouvait servir de base légale dans certains cas comme fondement pour un traitement à des fins de recherche scientifique. Il s'agit d'un contexte dans lequel la question de l'intérêt légitime peut en effet se poser[1848]. Cependant, pour que l'intérêt de la recherche scientifique puisse être considéré comme légitime, le traitement ne doit pas porter atteinte aux intérêts de la personne concernée, tels qu'au droit au respect à la vie privée ou à la liberté d'entreprendre. Une balance entre l'intérêt légitime du responsable de traitement et les intérêts de la personne concernée doit être faite dans ce cas. En revanche, le traitement ultérieur à des fins de recherche scientifique est présumé compatible avec le traitement initial, ce qui peut laisser imaginer la mise en place de partenariats de recherche entre des organismes ou des instituts de recherche et des responsables de traitement qui auraient collecté des données de manière licite[1849]. Cela permettrait aux chercheurs de ne pas collecter les données eux-mêmes et de contourner l'obligation d'obtenir le consentement des personnes concernées.

B. Une responsabilisation renforcée des responsables de traitement

719- La protection des données à caractère personnel incombe aux responsables de traitement de l'agriculture numérique. Aussi, il semble nécessaire d'envisager la notion de responsable de traitement (**1**), avant d'envisager les obligations qui sont à sa charge (**2**).

[1847] RGPD, art. 6.1 : « *Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie : a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ; b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ; c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ; e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant* ».

[1848] G29, *avis n°06/2014, op. cit.*

[1849] MAUREL L., « Données personnelles et recherche scientifique : quelles articulations dans le RGPD ? », S. I.LEX, 18 juill. 2018.

1. La notion de responsable de traitement

720- **Définition de responsable de traitement.** L'article 4 du RGPD définit l'ensemble des personnes[1850] gravitant autour des opérations de traitement des données à caractère personnel. Le responsable de traitement est désigné comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* »[1851]. C'est le responsable de traitement qui « *décrit l'objectif en vue duquel les données sont traitées* »[1852]. C'est donc lui qui décide les raisons pour lesquelles les données seront traitées et c'est sur lui que repose l'obligation de mettre en œuvre des « *mesures techniques et organisationnelles appropriées pour s'assurer et être en mesure de démontrer que le traitement est conforme au règlement* »[1853]. Il se peut également que les objectifs du traitement soient déterminés par une ou plusieurs autres personnes, auquel cas ils seront chacun responsable du traitement et nommé « *responsable conjoint* »[1854].

La CJUE, dans un arrêt du 10 juillet 2018, a précisé que « *la notion "de responsable de traitement" peut concerner plusieurs acteurs participant à ce traitement, chacun d'entre eux devant alors être soumis aux règles du droit de l'Union en matière de protection des données à caractère personnel. Ces acteurs peuvent être impliqués à différents stades du traitement et à des degrés divers, de telle sorte que le niveau de responsabilité de chacun d'entre eux doit être évalué en tenant compte de toutes les circonstances pertinentes en cas d'espèce* ». Ainsi, « *une personne physique ou morale qui influe, à des fins qui lui sont propres, sur le traitement des données à caractère personnel et participe, de ce fait, à la détermination des finalités et des moyens de ce traitement peut être considérée comme étant responsable de traitement* ». Par conséquent, plusieurs personnes peuvent être simultanément responsables de traitement à des degrés différents. Chacun d'entre eux répond aux exigences du RGPD sur les traitements des données à caractère personnel.

721- **Critères de détermination.** Trois critères de détermination des responsables de traitement ont été dégagés par le G29[1855]. Tout d'abord, pour identifier le ou les responsable(s) de traitement, la préférence revient aux organismes, sauf si la personne physique agissant au sein d'une personne morale utilise des données à des fins personnelles, en dehors des activités de la

[1850] Responsable de traitement, Responsable conjoint, Sous-traitant, Tiers.
[1851] RGPD, art. 4, al. 7.
[1852] FERAL-SCHUHL, C., ss. dir., *Cyberdroit, op. cit.*, n°113.11.
[1853] RGPD, art. 24.
[1854] RGPD, art. 26, al. 1.
[1855] G29, *avis n°1/2010 sur les notions de « responsable de traitement » et de « sous-traitant »*, WP169, 16 févr. 2010.

personne morale. Ensuite, c'est celui qui est responsable de traitement qui définit les finalités du traitement, alors que la détermination des moyens de traitement peut être déléguée au sous-traitant. Enfin, l'identification de la personne ayant joué un rôle décisionnel dans le choix des finalités de traitement doit s'apprécier de manière concrète et pratique. Par conséquent, toutes les personnes qui traitent des données personnelles et en déterminent les objectifs sont considérées comme des responsables de traitement.

Ainsi, tous les collecteurs et agrégateurs de données du secteur agricole qui traitent par la suite des données pour en tirer une information ou bien qui les transmettent gratuitement ou contre rémunération à d'autres opérateurs – considérés alors comme des tiers – seront des responsables conjoints de traitement. En cas de responsables conjoints, leur responsabilité ne sera « *limitée qu'à l'opération ou l'ensemble des opérations de traitement des données à caractère personnel dont il détermine effectivement les finalités et les moyens* »[1856]. Aussi, la responsabilité du traitement ne s'arrête qu'aux opérations qu'il effectue. Il ne peut être tenu responsable des traitements ultérieurs des données opérés par les destinataires de ces données.

722- **Extension de la notion de responsable de traitement.** L'extension effectuée par le RGPD de la notion de responsable de traitement s'explique par le fait que les traitements de données personnelles se généralisent et se banalisent[1857]. Ainsi, de plus en plus « *de personnes sont éligibles à la qualité de responsable de traitement* »[1858]. Par conséquent, la large notion de traitement permet sans difficulté d'affirmer que, même dans le secteur de l'agriculture numérique, les acteurs procèdent à des traitements de données à caractère personnel. Sur l'ensemble des données collectées et traitées dans le secteur agricole, nombre d'entre elles permettent en effet d'identifier une personne physique. Les acteurs du secteur agricole se muent donc parfois, voire souvent, en responsables de traitement.

2. Les obligations à la charge du responsable de traitement

723- **Changement de paradigme.** L'adoption du RGPD a permis un changement de paradigme pour les principes relatifs à la protection des données à caractère personnel. Si auparavant la LIL reposait sur une logique de formalités préalables, le règlement européen repose sur une logique de responsabilisation renforcée des acteurs tout au long du traitement. Par conséquent, les

[1856] CJUE, 29 juill. 2019, *Fashion ID GmbH & Co.KG* c/ *Verbraucherzentrale NRW eV, Facebook Ireland Ltd* et autre n° C-40/17.
[1857] CLEMENT-FONTAINE, M., « La plasticité de la notion de responsable de traitement », *Rev. Aff. Eur.*, 2018-1, pp. 35 à 42.
[1858] *Ibid.*

démarches préalables de déclaration, de consultation et d'autorisation sollicitées auprès de l'autorité de contrôle qui existaient sous l'ancien régime ne sont plus exigées.

724- **Règles de formalisme.** Dorénavant, le traitement de données à caractère personnel oblige le responsable de traitement à respecter un certain nombre de règles de formalisme. En outre, il doit fonder son traitement sur une cause licite, mais aussi minimiser les données, l'accès à celles-ci et limiter leur conservation dans le temps. Il doit aussi informer les personnes concernées sur les destinataires des données, il peut s'agir simplement de catégories de destinataires, soit parce qu'ils participent à la chaîne du traitement initial, soit en qualité de tiers et dans ce cas, ils seront en dehors de la chaîne de traitement initial. Si ce tiers procède à un nouveau traitement, il sera lui-même qualifié de responsable de traitement et devra déterminer les nouvelles finalités.

725- **Obligation de sécurité.** Le responsable de traitement a l'obligation de notifier les failles de sécurité à l'autorité de contrôle, telle que la CNIL, ainsi qu'à la personne concernée dans les meilleurs délais[1859]. À titre exceptionnel, l'obligation de notification peut ne pas être exécutée lorsqu'elle est susceptible de présenter un risque pour la sécurité nationale, la défense nationale ou la sécurité publique. Aussi, le délit de négligence s'agissant « *des précautions utiles pour préserver la sécurité de ces informations, et notamment d'empêcher qu'elles ne soient communiquées à des tiers non autorisés* »[1860] est puni d'une peine de cinq ans d'emprisonnement et de 300 000 euros d'amende[1861]. Le juge administratif a également le pouvoir de contrôler le respect de l'obligation de sécurité lorsque le traitement est assuré par une personne publique[1862], au titre de l'article 77 du RGPD.

726- **Conditions du respect des règles de formalisme.** Le responsable de traitement doit se conformer à ces règles dès la conception et tout au long de la vie de la donnée par le moyen de « *mesures techniques ou organisationnelles appropriées* »[1863]. C'est ce que la réglementation nomme le *Privacy by design*. Il doit également mettre « *en œuvre [d]es mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées* »[1864]. Il s'agit du *Privacy by default.* Aussi, il doit être en mesure de démontrer qu'il respecte bien les principes relatifs au traitement de données à caractère personnel de l'article 5

[1859] RGPD, art. 33 et s.
[1860] ROBIN, A., *Droit des données de la recherche, op. cit.*, p. 280.
[1861] C. pén., art. 226-17.
[1862] ROBIN, A., *op. cit.*
[1863] RGPD, art. 25 § 1.
[1864] RGPD, art. 25 § 2.

du RGPD, au titre de l'*Accountability*[1865]. Il doit être enfin en mesure de démontrer cette conformité à tout moment, au nom de la *Compliance*.

727- **Responsabilité du responsable de traitement.** Le responsable de traitement de données à caractère personnel engage sa responsabilité en cas de non-respect de ces obligations. La LIL prévoit un certain nombre de mesures correctrices et de sanctions pouvant être mis en œuvre par le Président de la CNIL aux articles 20 et suivants. Notamment, le président de la CNIL, après un avertissement au responsable de traitement, peut envoyer une mise en demeure ou saisir la formation restreinte pour faire appliquer des mesures provisoires dans le cas où le traitement représenterait une violation des droits et libertés et qu'il y aurait urgence à intervenir.

728- **Clauses contractuelles obligatoires.** Les obligations de formalisme se traduisent par l'obligation de rédiger certaines clauses dans les contrats conclus entre un responsable de traitement (entreprise collectrice de données) et une personne physique (l'agriculteur générateur de données). Les clauses devant obligatoirement figurer dans un contrat portant sur le traitement de données à caractère personnel ont été présentées dans une étude que nous avons réalisée pour le CASDAR Multipass sur l'analyse juridique des contrats en agriculture numérique[1866].

Clause sur la base légale. Tout d'abord, comme il a été vu précédemment, le responsable de traitement doit définir la base légale sur laquelle il fait reposer l'opération portant sur des données à caractère personnel. Cette mention fait l'objet de la clause sur la base légale. Elle peut ainsi porter sur le consentement libre et éclairé de la partie concernée[1867] ; sur l'exécution d'un contrat ou de mesures précontractuelles nécessitant le traitement de données à caractère personnel[1868] ; sur une obligation légale[1869] ; sur la sauvegarde des intérêts vitaux d'une personne[1870] ou enfin, sur une mission d'intérêt public ou d'autorité publique[1871].

Clause sur l'étendue du traitement des données personnelles. Ensuite, le responsable de traitement doit déterminer dans le contrat qui le lie à l'exploitant agricole, la ou les finalités du traitement des données des personnes concernées[1872]. À cette fin, le responsable de traitement expose les objectifs pour lesquels les données seront collectées. Cette obligation est combinée avec celle qui consiste dans le fait de réaliser un traitement de manière licite et loyale pour des

[1865] RGPD, art. 5. 2 et RGPD, art. 24.
[1866] TOMASSO, L., *Analyse juridique des contrats en agriculture numérique, op. cit.*
[1867] RGPD, art. 6. 1. a.
[1868] RGPD, art. 6. 1. b.
[1869] RGPD, art. 6. 1. c.
[1870] RGPD, art. 6. 1. d.
[1871] RGPD, art. 6. 1. f.
[1872] RGPD, art. 13. 1. c.

finalités strictement déterminées, explicites et légitimes[1873]. Par conséquent, les entreprises doivent communiquer des informations claires et sans ambiguïté sur la façon dont sont traitées les données[1874].

Clause sur la durée de conservation des données personnelles. Mais aussi, une clause doit prévoir la durée pendant laquelle les données devront être conservées, durée au-delà de laquelle les données seront archivées, supprimées ou anonymisées[1875]. De plus, cette conservation doit être faite sous une forme permettant l'identification des personnes concernées[1876].

Clause sur les destinataires des données personnelles. Une clause doit également prévoir « *les destinataires ou les catégories de destinataires des données à caractère personnel, s'ils existent* »[1877]. Le responsable du traitement doit donc détailler précisément les personnes qui auront accès aux données personnelles, autrement dit, « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers* ». Toutefois, les autorités publiques « *qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement* »[1878].

Clause sur l'existence ou non de la fourniture des données personnelles. De même, le responsable de traitement doit prévoir contractuellement si la personne concernée est tenue de fournir ses données personnelles ou non. Cette obligation repose sur l'article 13. 2. e. du RGPD qui dispose que le responsable de traitement doit fournir « *des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données* ».

D'autres mentions obligatoires doivent apparaître dans le contrat. Le responsable de traitement doit indiquer son identité et ses coordonnées[1879], le cas échéant, les coordonnées du

[1873] RGPD, art. 5.
[1874] RGPD, art. 12.
[1875] RGPD, art. 13. 2. a.
[1876] RGPD, art. 5. a.
[1877] RGPD, art. 13. 1. e.
[1878] RGPD, art. 4., 7e.
[1879] RGPD, art. 13. 1. a.

délégué à la protection des données[1880]. Mais aussi, « *l'existence du droit de demander au responsable du traitement l'accès aux données à caractère personnel, la rectification ou l'effacement de celles-ci, ou une limitation du traitement relatif à la personne concernée, ou du droit de s'opposer au traitement et du droit à la portabilité des données* »[1881], de même pour « *le droit d'introduire une réclamation auprès d'une autorité de contrôle* »[1882].

II. Des droits accrus pour l'agriculteur en tant que personne concernée

729- Le droit des données à caractère personnel constitue un véritable outil d'autodétermination informationnelle pour les personnes physiques concernées par les données (**A**), mais c'est également un outil pour le renforcement de la maîtrise juridique des données (**B**).

A. Un outil d'autodétermination informationnel

730- Tout d'abord, les personnes physiques disposent d'un panel de droits sur les données qui les concernent (**1**). Ensuite, il faut relever que ces droits sont propres à la personne concernée (**2**).

1. L'étendue des droits sur les données personnelles

731- **Droit de la personnalité.** Selon un auteur « *la question de la revendication d'une maîtrise sur ses données doit se placer sur le terrain des droits de la personnalité et non pas sur celui des modèles propriétaires* »[1883]. En effet, les droits sur les données à caractère personnel sont attachés à la personne concernée par ces données. Ainsi, cette dernière peut définir comme elle l'entend la circulation des données qui la concernent directement ou indirectement. À ce titre la personne concernée par les données à caractère personnel dispose de divers droits : un droit à l'information[1884] pour plus de transparence, un droit d'accès, un droit de rectification et d'effacement, un droit à la limitation du traitement, un droit d'opposition, mais également un droit à la portabilité. L'ensemble de ces droits permet à la personne concernée de conserver la

[1880] RGPD, art. 13. 1. b.
[1881] RGPD, art. 13. 2. b.
[1882] RGPD, art. 13. 2. d.
[1883] LAMBERTERIE (de), I., « Les ressources informationnelles en jouissance partagée : quels modèles propriétaires ? », *in Les modèles propriétaires*, Actes du colloque international organisé par le CECOJI, PUJP, 2009, p. 78.
[1884] RGPD, arts. 12, 13 et 14.

maîtrise sur les données qui la concernent. Pour rendre effectifs ces droits, des voies de recours juridictionnelles[1885] y sont attachées. Le but est d'obtenir réparation pour la personne physique des préjudices qu'elle aurait subie de l'utilisation de ses données par le responsable de traitement ou le sous-traitant[1886].

2. Des droits propres à la personne concernée

732- L'exclusivité des droits personnels implique que les données de la personne physique ne sont accessibles que par elle. La CNIL a eu l'occasion d'affirmer que les droits de la personne « *s'éteignent après [sa] mort* »[1887]. Ainsi, même les ayants-droits de la personne concernée ne peuvent avoir accès aux données de celle-ci après son décès. Le contrôle et l'usage des données personnelles ne peuvent donc être exercés que par la personne qui est identifiée ou identifiable. Les droits n'étant pas cessibles, il est impossible pour le responsable de traitement d'échapper à ces obligations.

B. La portabilité : un outil de renforcement de la maîtrise juridique sur les données à caractère personnel

733- La protection des données à caractère personnel constitue un fort outil d'autodétermination[1888] informationnelle pour les agriculteurs, qui ont le droit « *de décider et de contrôler [les] usages qui sont faits des données à caractère personnel les concernant* »[1889]. Ainsi, le droit à la portabilité permet de renforcer un peu plus la maîtrise juridique des agriculteurs sur les données à caractère personnel issues de leur exploitation. De cette manière même après avoir donné son consentement l'agriculteur ne reste pas « pieds et mains liés » au responsable de traitement des données. Aussi, il est nécessaire, dans un premier temps, d'envisager le contenu du droit à la portabilité (**1**) afin d'analyser, dans un second temps, les effets du droit à la portabilité (**2**).

[1885] RGPD, arts. 77 à 80.
[1886] RGPD, art. 82.
[1887] CNIL, *Mort numérique ou éternité virtuelle : que deviennent vos données après la mort ?*, 31 oct. 2014.
[1888] MALLET-POUJOL, N., « Protection des données personnelles et droit à l'information », *Légicom*, n°59, 2017/2, p. 51.
[1889] Ord. n°2018-1125, 12 déc. 2018 prise en application de l'article 32 de la loi n°2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel : *JORF* n°0288 du 13 décembre 2018, art. 1, al. 2.

1. Le contenu du droit à la portabilité

734- **Naissance du droit à la portabilité.** Jusqu'alors, un droit de récupération des données avait été posé par la Loi pour une République Numérique du 7 octobre 2016[1890], mais il ne s'adressait qu'aux consommateurs et visait les données associées au compte utilisateur et aux fichiers mis en ligne[1891]. De plus, il n'avait « *vocation à s'appliquer qu'aux fournisseurs de services les plus importants* »[1892]. Le RGPD a ainsi proposé d'aller plus loin en imposant un véritable droit à la portabilité pour toutes les personnes physiques identifiées ou identifiables par des données à caractère personnel. Cette prérogative permet, entre autres, à l'utilisateur d'un service numérique de changer d'opérateur. Ainsi, le fait de pouvoir transférer les données instaure une dynamique sur le marché et contraint les grandes plateformes et les services numériques à changer de *Business models*[1893]. Ces modifications sont donc salutaires pour les utilisateurs d'objets connectés et de services liés.

735- **Définition et conditions du droit à la portabilité.** Le droit à la portabilité trouve sa définition à l'article 20 du RGPD[1894]. Ce droit permet à la personne concernée de récupérer ses données et de changer de prestataire sans difficulté. Concernant les conditions du droit à la portabilité, en premier lieu, si le droit d'accès[1895] dispose d'un champ d'application large puisqu'il porte sur toutes les données de l'utilisateur, le droit à la portabilité quant à lui est beaucoup plus restreint. En effet, le droit à la portabilité ne porte que sur les données à caractère personnel fournies par la personne concernée et traitées sur la base du consentement ou de l'exécution du contrat. Pourtant comme le relèvent Mme la Professeure C. Zolynski et Mme M. Le Roy « *son champ d'application pourrait néanmoins être largement entendu si l'on suit l'interprétation extensive de la notion de "données fournies" retenue par le groupe de travail de l'article 29 dans ses lignes directrices* »[1896]. En effet, la notion pourrait concerner en plus « *[d]es données*

[1890] *JORF* n°0235 du 8 oct. 2016.
[1891] C. conso., art. L. 224-42-3.
[1892] C. conso., art. L. 224-42-4 ; cité in ZOLYNSKI, C. et LE ROY, M., « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *op cit.*, p. 107.
[1893] ZITTRAIN, J. L., *The future of the Internet, And How to Stop It*, Yale University Press & Penguin, UK, 2008 : « *La possibilité offerte aux utilisateurs de pouvoir transférer leurs données conduira à des changements de business models des grandes plateformes et des services numériques au bénéfice des consommateurs* » traduction par ZOLYNSKI, C. et LE ROY, M., « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *op. cit*., p. 108.
[1894] RGPD, art. 20, 1. : « *Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle* ».
[1895] Voir *supra*, n°169 et s.
[1896] ZOLYNSKI, C. et LE ROY, M., « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *op. cit.*

activement et sciemment fournies par la personne concernée », ainsi que « *les données observées fournies par la personne concernée grâce à l'utilisation du service ou du dispositif* »[1897]. Par conséquent, les données collectées au moyen d'objets communicants pourraient selon ces autrices faire l'objet d'un droit à la portabilité. En revanche, il faut noter que sont exclues « les "*données déduites" et les "données dérivées" […] créées par un prestataire de services* ». En second lieu, le droit à la portabilité ne s'applique que pour les données « *traitées de manière automatisée* »[1898] et seulement lorsque les opérations de traitement sont fondées « *sur le consentement de la personne concernée* » ou « *sur un contrat sur lequel la personne concernée est partie* »[1899]. En dehors de ces situations, le droit à la portabilité ne s'applique pas aux données à caractère personnel. En dernier lieu, le CEPD relève une troisième et dernière condition selon laquelle « *le droit à la portabilité des données ne doit pas porter atteinte aux droits et libertés des tiers* »[1900]. Par ailleurs, l'exercice du droit à la portabilité n'empêche pas les personnes concernées de jouir des autres droits dont elles disposent sur leurs données à caractère personnel. De plus, au titre de l'article 12 du RGPD, le responsable de traitement a l'interdiction d'exiger un paiement pour la fourniture des données à moins que les demandes soient manifestement infondées ou excessives « *notamment en raison de leur caractère répétitif* »[1901]. Le responsable de traitement destinataire des données doit également respecter certaines obligations, il « *est chargé de garantir que les données portables fournies sont pertinentes et ne sont pas excessives au regard du nouveau traitement des données* »[1902]. Il doit également « *indiquer clairement et directement la finalité du nouveau traitement avant toute demande de transmission de données portables* »[1903] et il doit respecter globalement toutes les obligations de l'article 5 du RGPD en tant que nouveau responsable de traitement.

[1897] G29, *Lignes directrices relatives au droit à la portabilité des données*, 13 déc. 2016, version révisée et adoptée, le 5 avr. 2017, WP 242 rev. 01, p. 12.
[1898] ZOLYNSKI, C. et LE ROY, M., *op. cit*.
[1899] G29, *Lignes directrices relatives au droit à la portabilité des données*, adoptées le 13 décembre 2016, version révisée et adoptée le 5 avril 2017, WP 242 rev. 01, p. 12
[1899] ZOLYNSKI, C. et LE ROY, M., *op. cit.*
[1900] *Ibid.*
[1901] RGPD, art. 12.5.
[1902] G29, *Lignes directrices relatives au droit à la portabilité des données, op. cit.*
[1903] RGPD art. 14 ; *ibid.*, p. 8.

2. La mise en œuvre du droit à la portabilité

736- **Conditions techniques de la portabilité**. D'un point de vue technique et comme il l'a été vu plus haut[1904], le droit à la portabilité ne peut s'exercer sans l'interopérabilité des systèmes. Ce n'est que de cette manière que les responsables de traitement pourront assurer les transferts de données et leur réutilisation. À cette fin les données devront être restituées dans un format « *structuré, couramment utilisé et lisible par machine* ». Néanmoins, aucun format n'a été imposé par le RGPD, chaque secteur peut donc fixer le format qui lui convient le mieux. Aujourd'hui, le droit à la portabilité est encore trop sous-exploité[1905] du fait notamment de cette « *absence de normes permettant la fourniture des données dans un format lisible par machine* »[1906]. Cette mise au pas devait se faire progressivement afin de laisser le temps aux acteurs du numérique de s'adapter. L'objectif étant de parvenir à un écosystème dans lequel les données peuvent circuler et être réutilisées librement. Pour cela, des outils doivent être adoptés afin de rendre effective la portabilité des données. Il peut s'agir « *[d'] outils de gestion du consentement et [d'] applications de gestion des informations à caractère personnel* »[1907]. Le CEPD (ex. G29) a fait deux propositions dans ce sens en invitant à la mise en place « *d'un service d'export depuis le compte client ainsi que d'une interface de programmation (API)* »[1908]. Il propose, également, de prendre des « *mesures contraignantes pour les interfaces techniques et les formats lisibles par machine pour permettre la portabilité des données en temps réel* »[1909]. Aujourd'hui, dans sa Proposition de règlement sur les données du 23 février 2022, la Commission européenne tend vers une harmonisation des standards d'interopérabilité[1910].

737- **Maîtrise de l'usage des données à caractère personnel.** Le droit à la portabilité des données à caractère personnel permet aux personnes concernées d'en avoir une meilleure maîtrise[1911]. À cette fin, des outils techniques sont envisagés pour proposer aux utilisateurs un moyen de conserver la maîtrise de l'usage des données qui les concernent. Il s'agit par exemple des « *Personnal Information Management Systems* » ou PIMS[1912], ou bien d'un *Cloud* personnel tel

---

[1904] Voire *supra*, n°537 et 663 et s.
[1905] BERTRAND, B., « Perfectibilité de la protection des données personnelles », *RTD Eur.*, 2021, p. 143.
[1906] *Ibid.*
[1907] *Ibid.*
[1908] G29, *Lignes directrices relatives au droit à la portabilité des données, op. cit.*
[1909] BERTRAND, B., « Perfectibilité de la protection des données personnelles », *op. cit.*
[1910] Voir *supra*, n°537.
[1911] ROBIN, A., « Les places de marché en ligne », *op. cit.*, n°109 : « *Le droit à la portabilité permet d'asseoir l'objectif d'autodétermination informationnelle et de renforcer la maîtrise des personnes sur leurs données* ».
[1912] CNNum, *Ambition Numérique, Pour une politique française et européenne de la transition numérique, op. cit.* pp. 53 à 54 : Les PIMS « *proposent notamment aux utilisateurs d'héberger leurs informations où ils le souhaitent,*

qu'il est proposé par *Cozy cloud* qui permet de « *regrouper toutes ses données dans un système unique* »[1913]. Il s'agira, par exemple, « *[d'] un serveur personnel ayant vocation à devenir un assistant personnel qui permettra de piloter des périphériques et objets connectés, notamment afin d'automatiser des tâches habituelles* »[1914]. Mais encore, il est proposé que le droit à la portabilité soit exercé à titre collectif tel qu'il est pratiqué en Angleterre avec les *Group privacy*. De cette manière, des groupes de personnes peuvent mettre en commun leurs données et les mettre à disposition d'acteurs publics selon des finalités prédéfinies par le biais du droit à la portabilité.

738- **Conclusion de la section.** Le droit des données à caractère personnel ne les distingue pas selon leur nature ou leur origine. À partir du moment où les données collectées ou produites permettent d'identifier une personne physique, alors la protection s'applique. Par conséquent, force est de constater qu'un très grand nombre de données de l'agriculture numérique sont identifiantes et doivent être protégées à ce titre. Les entreprises de *l'AgTech* qui traitent ces données sont donc considérées comme des responsables de traitement et ont des obligations envers les personnes concernées qui voient, eux, leurs droits renforcés. Toutefois, des solutions de traitement de données à caractère personnel existent pour les entreprises de l'agriculture numérique.

Section 2. Les solutions de traitement des données à caractère personnel issues des exploitations agricoles

739- Afin d'exploiter des données à caractère personnel du secteur agricole, les responsables de traitement doivent nécessairement baser leur traitement sur l'une des finalités prévues par le RGPD. Si cinq de ces finalités reposent sur la nécessité du traitement de ces données (intérêts vitaux, intérêts légitimes, exécution d'un contrat, mission de service public, obligation légale), il existe néanmoins deux alternatives pour le responsable de traitement. Il peut en effet soit recueillir le consentement de la personne concernée (**§1**), soit procéder à une anonymisation des données à caractère personnel **(§2**). L'objectif est de trouver un équilibre dans le marché des données personnelles, en prenant toutes les mesures nécessaires afin de ne pas créer de

de maîtriser la distribution de ces informations vis-à-vis des tiers (particuliers, entreprises, etc.) et de créer eux-mêmes les connexions logiques entre les services : facture d'énergie, listes de courses, billets de train, mails, etc. ».

[1913] ZOLYNSKI, C. et LE ROY, M., *op. cit.*, p. 109.

[1914] *Ibid.*

préjudice pour les personnes concernées « *sans constituer pour autant un obstacle excessif au marché de la réutilisation des données* »[1915].

§1. *Le recueil du consentement*

740- Le consentement peut paraître comme un outil fort utile afin de renforcer la maîtrise de l'exploitant agricole sur les données qui le concernent (**I**). Pour autant, il ne faudra pas manquer de relever les limites d'un tel outil (**II**).

I. Les principes du recueil du consentement

741- Tout d'abord, il est nécessaire d'envisager la notion de consentement (**A**), avant d'en analyser les effets (**B**).

A. La notion de consentement

742- La première étape consiste à étudier la définition du consentement retenue par le RGPD (**1**). La seconde étape nécessitera d'exposer les caractères du consentement (**2**).

1. La définition du consentement

743- **Définition légale.** Le consentement est défini par le RGPD comme « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* »[1916]. Ce consentement peut être donné pour « *une ou plusieurs finalités spécifiques* »[1917] et pour être valable, il doit faire l'objet « *[d'] un accord explicite et éclairé* »[1918].

[1915] PUCHERAL, P., RALLE, A., ROCHELANDET, F. et ZOLYNSKI, C., « Le *Privacy by design* : une fausse bonne solution aux problèmes de protection des données personnelles soulevés par l'*Open Data* et les objets connectés », *Légicom*, 2016, p. 89.
[1916] RGPD, cons. 6.
[1917] RGPD, art. 6.
[1918] FERAL-SCHUHL, C., ss. dir., *Cyberdroit*, *op. cit.*, n°113.31.

2. Les caractères du consentement

744- Caractère éclairé. Le consentement doit être éclairé, ce qui signifie que le responsable de traitement a l'obligation d'informer, préalablement à son recueil, la personne concernée. Le responsable de traitement doit répondre à cette obligation « *afin de permettre [aux personnes concernées] de prendre des décisions en toute connaissance de cause, de comprendre ce à quoi elles consentent et d'exercer leur droit de retirer leur consentement* »[1919]. Le principe de transparence suppose de rendre facilement accessibles les traitements de données à caractère personnel et à procéder à toute information et communication concernant le traitement de la personne concernée. Cette communication doit se faire sous forme intelligible et en des termes clairs et simples. De cette manière, la personne concernée peut contrôler le traitement fait sur ses données[1920]. Le consentement ne doit donc pas se fondre dans un document, par exemple des conditions générales ou une politique de confidentialité[1921]. Dans les faits, de telles conditions sont difficiles à mettre en œuvre[1922].

745- Caractère univoque. Le consentement doit être donné sans ambiguïté, c'est-à-dire, de manière univoque. Dès lors, doivent être écartés les consentements exprimés par des cases précochées ou préactivées ou encore l'accord implicite résultant de l'absence de réponse à une demande ou la poursuite de l'utilisation du service[1923]. Le consentement doit donc être explicite, ce qui impose une déclaration expresse de la personne concernée. Il peut s'agir d'une case de recueil du consentement, d'une déclaration écrite signée par la personne concernée, l'envoi d'un courriel ou bien d'un dispositif sécurisé de vérification.

746- Caractère spécifique. Le consentement doit être donné de manière distincte pour chaque finalité du traitement. Le responsable de traitement doit, donc, prévoir de recueillir un consentement distinct afin que les utilisateurs puissent donner leur consentement spécifiquement pour chacune des finalités[1924]. Par conséquent, il ne peut y avoir de consentement groupé pour un ensemble de finalités. Il faut toutefois soulever une subtilité en faveur de la recherche scientifique : dans le cas d'une collecte de données dans un objectif de recherche scientifique[1925], le RGPD reconnaît que les finalités sont parfois difficiles à

[1919] *Ibid*, n°113.71.
[1920] RGPD, cons. 32 et 55.
[1921] RGPD, cons. 32 et art. 7.2.
[1922] NETTER, E., « À quoi sert le principe de transparence en droit des données personnelles ? », *Dalloz IP/IT*, 2020. 611.
[1923] RGPD, cons. 32 : « *Il ne saurait y avoir de consentement en cas de silence, de cases cochées par défaut ou d'inactivité* ».
[1924] RGPD, cons. 43.
[1925] RGPD, cons. 159.

déterminer en amont et assouplit l'obligation d'une finalité précise et distincte. En effet, le considérant 33 du RGPD prévoit qu'il n'est pas toujours possible de déterminer entièrement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données. La seule précision du domaine de la recherche peut donc suffire afin de valider le consentement de la personne concernée, dans le respect toutefois des normes éthiques reconnues en matière de recherche scientifique. Les personnes concernées devraient donc « *pouvoir donner leur consentement uniquement pour ce qui est de certains domaines de la recherche ou de certaines parties de projets de recherche, dans la mesure où la finalité visée le permet* »[1926].

747- **Caractère libre.** La dernière condition consiste pour la personne concernée de refuser de donner son consentement sans que cela n'entraîne pour elle un quelconque préjudice. Peu importe que ce préjudice soit de nature pécuniaire ou qu'il s'agisse de la rupture de la continuité du service.

Ainsi, le refus de consentir ne doit pas avoir pour effet d'empêcher l'exécution du contrat ou l'accès au service[1927]. Autrement dit, les données à caractère personnel collectées sur le fondement du consentement ne doivent pas être nécessaires à l'exécution d'un contrat ou d'une prestation de services. Les entreprises collectrices de données sur les exploitations agricoles ne peuvent donc pas faire reposer le traitement des données à caractère personnel qu'ils collectent sur la base du consentement de l'agriculteur dès lors que la collecte de ces données a pour objet l'exécution d'une prestation de services.

La personne concernée doit par conséquent être libre de choisir les finalités du traitement et libre de retirer son consentement à tout moment et aussi facilement qu'elle l'a donné. Ce n'est que dans le respect de ces conditions que le consentement pourra produire des effets.

B. Les effets du consentement

748- L'obtention du consentement induit un renforcement de la maîtrise des données à caractère personnel par la personne concernée, d'abord, parce que le fait de demander son accord à l'exploitant agricole, personne physique, suppose une certaine forme de contrôle sur l'exploitation de ses données à caractère personnel (**1**), ensuite, parce que pour rendre effective

[1926] RGPD, cons. 33.
[1927] RGPD, art. 7.

la maîtrise sur les données, le responsable de traitement doit respecter un certain nombre de règles de formalisme (**2**).

1. Le contrôle de la personne concernée sur ses données à caractère personnel

749- La personne concernée qui consent au traitement de ses données à caractère personnel dispose de certains droits sur celles-ci. Ainsi, il acquiert une forme de maîtrise sur ses données[1928]. Le CEPD détermine, en effet, les différents droits de la personne concernée par le traitement de ses données à caractère personnel reposant sur le consentement.

Comme pour les autres bases légales, la personne concernée bénéficie du droit à la portabilité des données[1929], mais aussi, du droit à l'effacement lorsque le consentement a été retiré, du droit à la limitation, du droit de rectification et du droit d'accès[1930].

En revanche, la personne qui a consenti au traitement de ses données à caractère personnel ne dispose pas du droit d'opposition, puisque par définition il a donné son consentement à ce traitement. Néanmoins, le droit de retrait, comme le rappelle, le CEPD, entraîne « *un résultat similaire* »[1931].

De même, afin de rendre plus effective la maîtrise sur les données de la personne physique, le responsable de traitement doit se soumettre à certaines modalités pour le recueil du consentement. Ce qui conforte les droits de la personne concernée.

2. L'effectivité du contrôle sur les données à caractère personnel

750- **Modalités du recueil du consentement.** Le responsable de traitement est contraint de respecter certaines modalités pour le recueil du consentement. Il a notamment « *la charge de la preuve que la personne concernée a effectivement consenti au traitement* »[1932]. Mais il doit également présenter la demande de consentement de la manière la plus accessible possible pour la personne concernée. Le responsable de traitement doit déterminer et mettre en place les mesures « *techniques et organisationnelles* » nécessaires pour assurer les droits et libertés des personnes

---

[1928] LAMBERTERIE (de), I., « Les ressources informationnelles en jouissance partagée : quels modèles propriétaires ? », *op. cit.*, p. 78.
[1929] RGPD, art. 20.
[1930] G29, *Lignes directrices sur le consentement au sens du règlement 2016/679*, adoptées le 28 nov. 2017, Version révisée et adoptée le 10 avril 2018, p. 35.
[1931] *Ibid.*
[1932] FERAL-SCHUHL, C., ss. dir., *Cyberdroit, op. cit.*, n°113.31 ; RGPD, art. 7.

concernées[1933]. À cette fin, il doit mettre en œuvre le « *dispositif requis pour être en mesure de prouver que la personne concernée a bien donné son consentement dans un cas spécifique, préalablement à la mise en œuvre du traitement des données* »[1934]. Ces éléments de preuve doivent permettre de démontrer que le consentement a bien été donné de manière libre, spécifique, éclairée et univoque. Le renouvellement du consentement n'est pas exigé sauf si les finalités changent. Une fois l'activité de traitement terminée, « *la preuve du consentement ne devrait pas être conservée plus longtemps que la durée strictement nécessaire pour respecter une obligation légale ou à la constatation, à l'exercice ou à la défense de droits en justice* »[1935]. Pour conserver la preuve du recueil des consentements, le responsable de traitement peut tenir un registre ou conserver une trace des échanges avec la personne concernée : informations fournies, déclarations de consentement reçues, copie des enregistrements audio, etc.

751- **Outils pour la validité du consentement.** Plusieurs outils peuvent être utilisés afin de recueillir le consentement dans les conditions du RGPD.

D'abord, il faut évoquer la *Blockchain* ou bloc de chaîne, qui est « *un mode d'enregistrement de données produites en continu, sous forme de blocs liés les uns aux autres dans l'ordre chronologique de leur validation, chacun des blocs et leur séquence étant protégés contre toute modification* »[1936]. Elle permet de nombreuses fonctionnalités telles que la création d'un registre décentralisé (conservation de données et registres), le déclenchement des *Smart contracts* avec des instructions automatisées, ou encore, la création et le transfert des actifs numériques[1937]. Mais aussi, et surtout, elle est souvent évoquée afin de servir de gestionnaire des consentements[1938]. Cependant, son caractère irréversible peut constituer un frein à la mise en place d'une chaîne de bloc à cet effet. La conservation du consentement, aux termes du RGPD, doit en effet être limitée dans le temps. Il faudra donc trouver des solutions techniques pour que les informations contenues dans la chaîne de bloc ne puissent plus être lisibles. L'anonymisation pourrait s'avérer utile afin de respecter cette obligation.

Ensuite, un outil a été mis en place par des prestataires dans le marché des données à caractère personnel, il s'agit des *Consent Management Platform*. Ce sont « *des plateformes technologiques dédiées spécifiquement à la collecte et à l'enregistrement du consentement et utilisées par un site Web, qu'il s'agisse d'un média, d'un e-commerçant ou d'une entreprise*

[1933] RGPD, cons. 32.
[1934] FERAL-SCHUHL, C., *ibid*.
[1935] *Ibid.*, n°112.71 ; RGPD, art. 17.
[1936] LEGEAIS, D., *Blockchain et actifs numériques*, LexisNexis, 2e éd., 2019, p. 17.
[1937] LEGEAIS, D., « Bienvenue aux actifs numériques », *RJC*, mars/avr. 2020, p. 111.
[1938] LEGEAIS, D., *Blockchain et actifs numériques,* LexisNexis, 2e éd., p. 87.

lambda, pour permettre d'assurer l'expression, la restitution et l'attestation des consentements des utilisateurs »[1939]. Les prestataires de services qui proposent ce type de plateforme tiennent le rôle de tiers de confiance afin de permettre aux acteurs d'horodater les consentements des utilisateurs. La CNIL a eu l'occasion de préciser le contenu des CMP pour respecter les conditions d'un consentement libre, spécifique, éclairé et non équivoque dans la décision du 30 octobre 2018 mettant en demeure la société Vectaury[1940]. Il est à noter que si la CMP prend part à la détermination des finalités, alors le prestataire à l'origine de la CMP sera considéré comme responsable de traitement.

Enfin, au Québec, certains juristes ont développé la théorie des fiducies de données[1941] dont l'objectif est de fournir aux utilisateurs un certain contrôle sur leurs données à caractère personnel. En effet, la personne physique qui consentirait à mettre ses données à caractère personnel en fiducie délèguerait dans le même temps son consentement pour les futures finalités de traitement à un fiduciaire. Ce fiduciaire pourrait être le responsable de traitement lui-même. Cet outil consisterait à imposer au responsable de traitement d'agir au profit des personnes concernées, en respectant les finalités de traitement et les modalités de collecte. La fiducie de données suppose donc une relation de confiance entre le fiduciaire et le constituant. Plusieurs écueils peuvent être soulevés s'agissant des fiducies de données. D'abord, les données n'entrent pas dans les catégories de chose pouvant faire l'objet d'une fiducie en droit français. En effet, l'article 2011 du Code civil dispose que la fiducie permet le transfert de biens, de droits ou de sûretés. Or, pour des raisons déjà évoquées[1942], les données n'entrent pas dans la catégorie des biens. Ensuite, la délégation du consentement aurait pour effet de fragiliser un peu plus le consentement de la personne concernée, laissant plus de liberté encore au responsable de traitement[1943] dans des relations déséquilibrées. Le RGPD offre assez de garanties en Europe pour éviter les écueils de la fiducie de données.

752- **Sanctions en cas d'invalidité du consentement.** Le responsable de traitement s'expose à de lourdes sanctions dans le cas où il ne respecterait pas les conditions de validité du RGPD : jusqu'à 20 millions d'euros d'amende ou 4 % de son chiffre d'affaires mondial[1944]. La société Google a inauguré l'application de telles sanctions. En effet, la société Google LLC avait mis

[1939] BESSUGES-MEUSY, R., « CMP : un passeur de consentement », *Expertises*, févr. 2021, p. 59.
[1940] Déc. n° MED 2018-042, 30 oct. 2018 mettant en demeure la société X, *JO* 09 nov. 2018.
[1941] ElementAI et Nesta, *Fiducies de données, un nouvel outil pour la gouvernance des données*, https://hello.elementai.com/rs/024-OAQ-547/images/Fiducies_de_Donnees_FR_201914.pdf
[1942] Voir *supra*, n°512 et s.
[1943] HULIN, A. -S., « Introduction à la fiducie québécoise de données », *Laboratoire de cyberjustice*, blog, nov. 2019
[1944] RGPD, art. 83, pt. 5.

en place un système de bouton précoché concernant l'utilisation des données pour les publicités personnalisées. La CNIL a sanctionné la société pour manquement aux droits des personnes concernées, notamment pour ne pas avoir respecté l'obligation d'obtenir un consentement spécifique et univoque, dans une délibération du 21 janvier 2019[1945]. La CNIL a prononcé, en outre, une sanction pécuniaire à hauteur de 50 millions d'euros. La société Google LLC a demandé l'annulation de cette délibération et le 19 juin 2020, le Conseil d'État a validé la décision de la CNIL.

II. Les écueils du recueil du consentement

753- En réalité, le recours au consentement « *profite essentiellement au responsable du traitement qui, le plus souvent, n'aurait pas pu mettre en œuvre le traitement de données sur le fondement d'une autre base juridique* »[1946]. Aussi, il faut faire le constat aujourd'hui que « *le consentement donné aux plateformes est rarement aussi explicite et spécifique que les règles l'exigent ; pas plus qu'il n'est préalable et suffisamment informé* »[1947]. Ce constat peut s'expliquer notamment en raison du fait que les conditions de recueil du consentement dans le respect du RGPD s'avèrent particulièrement difficiles (**A**). L'utilisation du consentement comme base légale comporte donc certains risques (**B**).

A. Les difficultés liées au recueil du consentement

754- Selon le G29, « *l'adjectif "libre" implique un choix et un contrôle réel pour les personnes concernées* »[1948]. Aussi, il convient d'abord d'envisager l'écueil du consentement libre (**1**), pour ensuite analyser l'incompatibilité du consentement libre et du contrat (**2**).

1. L'écueil d'un consentement libre

755- **Choix du consentement dans une relation déséquilibrée.** Pour que le consentement soit libre, il ne faut pas que le responsable de traitement soit dans un rapport de force avec la personne

[1945] CNIL, Formation restreinte, n° SAN-2019-001, 21 janv. 2019.
[1946] DOUVILLE, T., *Droit des données à caractère personnel : Droit de l'Union européenne, droit français*, Gualino, 2020, n°179.
[1947] HATZOPOULOS, V., « Vers un cadre de la régulation des plateformes ? », *RIDE*, 2019/3, p. 399.
[1948] G29, *Lignes directrices sur le consentement, op. cit.*, p. 6.

concernée. Il est donc exigé que la personne concernée puisse « *véritablement* » être « *en mesure d'exercer un choix* »[1949]. Il ne doit pas y avoir de « *risque de tromperie, d'intimation, de coercition ou de conséquences négatives importantes si elle ne donne pas son consentement* »[1950]. Ainsi, « *le consentement ne sera pas libre lorsque tout élément de contrainte, de pression ou d'incapacité d'exercer un véritable choix sera présent* »[1951].

756.- Principe de conditionnalité. Pour être libre, le consentement ne doit pas porter sur des données nécessaires à l'exécution d'un contrat ou d'une prestation de services[1952]. Autrement dit, lorsque la collecte des données conditionne l'exécution d'un contrat ou d'une prestation de services, leur traitement ne peut pas reposer sur la base du consentement.

757.- Nécessité de détailler le consentement. Le choix des finalités de traitement des données à caractère personnel, pour les personnes concernées, doit être totalement libre[1953]. Cette obligation est liée au caractère spécifique du consentement. Si la personne n'a pas la possibilité de choisir les finalités du traitement, alors son consentement est limité.

758.- Absence de préjudice. La personne concernée doit pouvoir librement faire le choix de consentir ou non au traitement de ses données à caractère personnel. Ce qui implique que le refus de la personne physique ne doit pas engendrer, pour elle, de préjudice, par exemple avec des frais, ou encore par « *la tromperie, l'intimidation, la coercition ou toute conséquence négative importante si la personne concernée refuse de donner son consentement* »[1954]. Par conséquent, le responsable de traitement doit pouvoir prouver que la personne concernée peut librement retirer son consentement sans subir de préjudice.

[1949] *Ibid.*, p. 8.
[1950] *Ibid.*
[1951] *Ibid.*
[1952] RGPD, art. 7 : « *Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat* » ; RGPD, cons. 43 : « […] *le consentement est présumé ne pas avoir été donné librement si un consentement distinct ne peut pas être donné à différentes opérations de traitement des données à caractère personnel bien que cela soit approprié dans le cas d'espèce, ou si l'exécution d'un contrat, y compris la prestation d'un service, est subordonnée au consentement malgré que celui-ci ne soit pas nécessaire à une telle exécution* ».
[1953] RGPD, cons. 32 : « *Le consentement donné devrait valoir pour toutes les activités de traitement ayant la ou les mêmes finalités. Lorsque le traitement a plusieurs finalités, le consentement devrait être donné pour l'ensemble d'entre elles* ».
[1954] G29, *Lignes directrices sur le consentement, op. cit*., p. 12.

2. L'incompatibilité du consentement libre et du contrat

759- **Les conséquences de l'incompatibilité entre consentement libre et contrat.** De toute évidence, il est difficile pour les acteurs du numérique de mettre en œuvre une obtention du consentement totalement libre au sens du RGPD. En effet, la collecte et l'usage des données ont souvent, voire toujours, pour finalité l'exécution d'un contrat ou d'une prestation de services. Or, le G29 conclut que « *ces deux bases juridiques du traitement de données à caractère personnel, à savoir le consentement et le contrat, ne peuvent pas être fusionnées et amalgamées* »[1955]. À cette fin, le G29 préconise de rechercher « *le champ d'application du contrat et les données qui seraient nécessaires à l'exécution dudit contrat* »[1956]. Le traitement des données doit avoir un lien direct et objectif avec la finalité d'exécution du contrat. Ce lien empêche de faire reposer le traitement sur la base légale du consentement. Le consentement et le contrat ne peuvent, donc, être couplés. Si le traitement des données repose sur un contrat ou une licence d'exploitation, le responsable de traitement ne peut pas se servir du recueil du consentement pour justifier son traitement. L'utilisation du consentement comme base juridique ne sera pas dans ce cas adéquate[1957]. Le contrôleur européen de la protection des données a eu l'occasion d'affirmer à ce sujet, « *qu'il n'est [...] pas toujours simple de déterminer ce qui constitue un consentement authentique, non équivoque. Certains responsables du traitement exploitent cette incertitude en recourant à des méthodes qui excluent toute possibilité de donner un consentement véritable, non équivoque* »[1958]. De même, selon le G29 « *la complexité des pratiques de collecte des données, des modèles commerciaux, des relations entre fournisseurs et des applications technologiques dépasse, bien souvent, la capacité ou la volonté d'une personne de décider, par un choix actif, de contrôler l'utilisation et le partage d'informations* »[1959].

760- **Le consentement actif dans les contrats.** Le juge a également eu l'occasion de se prononcer sur « *l'interprétation de l'exigence de consentement actif dans les clauses contractuelles* »[1960].

[1955] *Ibid.*, p. 9.
[1956] *Ibid.*
[1957] G29, *avis 15/2011 sur la définition du consentement,* 13 juill. 2011, WP 187, p. 11.
[1958] Contrôleur européen de la protection des données sur la communication de la Commission, avis « Une approche globale de la protection des données à caractère personnel dans l'Union européenne », 14 janv. 2011 : *JOUE* C-181, 22 juin 2011, p. 11.
[1959] G29 et Groupe de travail « Police et justice », *L'avenir de la protection de la vie privée*, Contribution conjointe à la consultation de la Commission européenne sur le cadre juridique du droit fondamental à la protection des données à caractère personnel, 1er déc. 2009, WP 168, p. 19.
[1960] BERTRAND, B., « Perfectibilité de la protection des données personnelles », *op. cit.*

Dans l'arrêt *Orange România* du 11 novembre 2020[1961], la Cour de justice de l'Union européenne devait en effet s'interroger sur l'existence d'un consentement actif de la personne concernée au traitement de ses données à caractère personnel lors de la conclusion d'un contrat contenant une case précochée. Dans les faits, la personne avait signé un contrat relatif à la fourniture de services de télécommunication qui contenait une clause selon laquelle elle avait été informée et avait consenti à la collecte, ainsi qu'à la conservation d'une copie de son titre d'identité à des fins d'identification. Les juges ont interprété les faits au regard du considérant 32 du RGPD qui interdit les cases précochées et en fait une application aux contrats écrits. Ainsi, lorsqu'un contrat contient une case précochée informant la personne concernée de son consentement pour la collecte de ses données à caractère personnel, il y a un inversement par la mise en place d'un refus actif au lieu d'un consentement actif. La société Orange ne respectait donc pas les règles du RGPD.

Deux autres hypothèses permettent de douter de l'existence d'un consentement actif lorsque la personne concernée signe un contrat comprenant une clause selon laquelle elle consent à la collecte de ses données. D'abord, la personne concernée doit toujours être informée au préalable des conséquences de son refus pour le traitement de ses données, il ne doit donc pas y avoir d'ambiguïté sur ces conséquences[1962]. Ainsi, la personne concernée doit toujours donner son consentement de manière informée[1963]. Elle doit, également, être informée du fait qu'elle peut « *conclure le contrat sans être tenue de consentir au traitement de ses données à caractère personnel* »[1964]. Enfin, le responsable de traitement ne doit pas exiger des modalités de refus supplémentaires qui auraient pour effet d'affecter le choix de la personne concernée[1965]. Les difficultés de recueil d'un consentement libre conduisent certains auteurs à estimer que le consentement ne peut jamais véritablement être libre et éclairé[1966].

761- **Impossibilité de recueillir un consentement libre dans les contrats de l'agriculture numérique**. De toute évidence s'agissant du traitement des données générées ou issues des exploitations agricoles, il sera extrêmement difficile, voire impossible, d'obtenir un consentement libre des agriculteurs. Les entreprises qui collectent les données des exploitations agricoles sont en règle générale dans un rapport de force avec les agriculteurs, qui sont eux bien

[1961] CJUE, 11 nov. 2020, aff. C -§ 1/19, *Orange România*
[1962] *Ibid*.
[1963] À propos des cookies, arrêt *Planet 49*, CJUE, 1er oct. 2019, aff. C-673/ 17, *Planet 49*, *D.* 2019, 1884.
[1964] DOUVILLE, T., « Consentement à un traitement de données à caractère personnel et contrat : nouveaux apports de la Cour de justice », obs. ss. CJUE, 11 nov. 2020, aff. C-61/ 19, *Dalloz IP/IT*, 2021, p. 290.
[1965] BERTRAND, B., « Perfectibilité de la protection des données personnelles », *op. cit*.
[1966] DESTREGUIL, M., « Plaidoyer en faveur d'une approche propriétariste des données personnelles », *RJPF*, n° 3, 1er mars 2019.

souvent limités dans le choix de leurs cocontractants. Les données collectées par des objets connectés ou saisies par l'agriculteur dans les logiciels de gestion sont donc utilisées pour l'exécution de prestations de services. Par conséquent, l'éventuel retrait du consentement de l'exploitant agricole sur le traitement de ses données aurait pour effet de stopper le service ou l'exécution du contrat. La nature déséquilibrée des contrats de l'agriculture numérique limite donc fortement le recueil d'un consentement libre qui peut, au contraire, engendrer des risques pour l'agriculteur.

B. Les risques de l'utilisation du consentement comme base légale

762- En cas de non-respect des règles de validité du consentement, le responsable de traitement risque de voir sa responsabilité engagée (**1**). En outre, il existe également des risques pour la personne concernée (**2**).

1. Les risques pour le responsable de traitement

763- En dehors d'une relation contractuelle équilibrée, le caractère libre du consentement recueilli peut être remis en cause et le recueil du consentement peut être invalidé. Or, l'absence de consentement de la personne concernée ou dans le cas d'un consentement invalide, le responsable de traitement engage sa responsabilité. Pour rappel, la CNIL a sanctionné très lourdement — plus de 50 millions d'euros — la société Google LLC en raison d'un consentement insuffisamment éclairé, spécifique et univoque[1967]. C'est dire à quel point le juge apporte une attention particulière à la validité du consentement.

2. Les risques pour la personne concernée

764- **Dévoiement.** Afin d'éviter les écueils d'un consentement libre, éclairé et univoque et pour parvenir aux traitements des données à caractère personnel qui les intéressent, il arrive bien souvent que les responsables de traitement essaient de se soustraire à leurs contraintes en passant par des chemins détournés. Pour se faire, il arrive que les responsables de traitement légitiment des traitements initialement impossibles. Pour cela, ils font reposer le traitement des

[1967] CNIL, dél. formation restreinte, prononçant une sanction pécuniaire à l'encontre de la société *Google LLC* n° SAN, 2019-001, 21 janv. 2019.

données à caractère personnel sur une autre base légale. Ils dépassent dans ce cas le cadre de l'intérêt général ou de la nécessité contractuelle afin d'éviter d'avoir recours au consentement de la personne concernée. De cette manière, ils « *légitiment des traitements initialement impossibles* »[1968] et retirent à la personne concernée son choix dans le traitement de ses données.

765- ***Consent fatigue*.** Le recours au consentement comme base légale comporte un risque pour les personnes concernées dû à l'émergence d'un nouveau phénomène, le *Consent fatigue*[1969]. Ce phénomène suppose que par facilité, ignorance ou incompréhension, les personnes concernées acceptent ou refusent d'un bloc tout traitement de leurs données sans même lire les conditions du traitement. Un tel comportement démontre encore une fois les difficultés de l'obtention d'un consentement éclairé, libre et univoque.

766- **Contraintes.** Il existe un risque de contrainte pour les personnes concernées. En effet, par crainte de « *[l'] exclusion d'un service internet ou parce qu'au contraire, il pourrait bénéficier d'avantages commerciaux* »[1970], les utilisateurs sont, bien souvent, dans une situation de dépendance aux « *outils technologiques et numériques* » telle qu'ils sont contraints de consentir au traitement de leurs données à caractère personnel. Dans le secteur de l'agriculture numérique, Mme C. Béguin Faynel[1971] rappelle à ce titre que les agriculteurs sont souvent dépendants économiquement de leur prestataire, ce qui s'apparente à de la contrainte. Il se peut donc que les agriculteurs consentent au traitement de leurs données à caractère personnel à des fins qui ne leur conviennent pas ou qui pourraient finalement leur porter préjudice. Par conséquent, les difficultés liées au recueil d'un consentement libre, éclairé, univoque et spécifique peuvent rendre cet outil inefficace et risqué pour les entreprises qui l'utilisent.

§2. *L'anonymisation, une solution risquée pour le traitement des données personnelles des agriculteurs*

767- Le *Privacy by design* « *consiste à intégrer la protection des données personnelles dès la conception des outils de collecte, de traitement et d'exploitation des données et à maintenir sa prise en compte tout au long de la vie du projet* »[1972]. Ainsi, les données collectées par les objets

[1968] DESTREGUIL, M., « Plaidoyer en faveur d'une approche propriétarise des données personnelles », *op. cit.*
[1969]https://www.lemonde.fr/idees/article/2020/03/15/le-rgpd-offre-paradoxalement-une-immense-opportunite-de-collecte-pour-les-publicitaires-et-autres-societes-de-services-marketing_6033132_3232.html
[1970] *Ibid.*
[1971] BEGUIN-FAYNEL, C., « La problématique de l'appropriation des données agricoles », *op. cit.*
[1972] ZOLYNSKI, C., « Le sens des normes *by design* », *Les objets connectés*, Actes de colloque, 2018, p. 134.

connectés doivent répondre aux normes *by design*[1973], être protégées dès lors qu'elles sont collectées et tout au long de leur vie. Parmi les mesures évoquées par le RGPD afin de répondre à cette obligation, l'anonymisation des données à caractère personnel est un outil précieux. En effet, le considérant 26 du RGPD distingue deux types de données, celles qui sont anonymes et celles qui sont anonymisées. Les premières sont définies comme « *les informations ne concernant pas une personne physique identifiée ou identifiable* », alors que les secondes sont des « *données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable* ». Dès lors que les données répondent à ces conditions, elles sortent du champ d'application du RGPD et de la LIL. Il est donc nécessaire d'étudier les solutions techniques d'anonymisation qui permettent aux acteurs de l'agriculture numérique d'exploiter des données initialement personnelles sans obtenir le consentement de la personne concernée (**I)**. Néanmoins, bien que le G29 se soit emparé de la question[1974] des techniques d'anonymisation, celles-ci présentent un écueil important. Les responsables de traitement doivent porter une attention particulière sur les techniques utilisées afin d'éviter la qualification de données pseudonymisées. Dans le cas d'une pseudonymisation des données, les responsables de traitement courraient le risque de faire entrer de nouveau ces données dans la catégorie des données à caractère personnel soumise au RGPD (**II**).

I. Les solutions techniques d'anonymisation

768. L'anonymisation est un outil efficace pour l'exploitation des données à caractère personnel, à condition, toutefois, qu'elle réponde aux conditions particulièrement strictes du RGPD (**A**). Dans un tel cas, elle pourra produire ses effets (**B**).

A. Les conditions de l'anonymisation

769. Le G29 s'est intéressé à la question des techniques d'anonymisation et a fourni une définition conceptuelle de la notion d'anonymisation : « *pour rendre des données anonymes, il faut en retirer suffisamment d'éléments pour que la personne concernée ne puisse plus être identifiée. Plus précisément, les données doivent être traitées de façon à ne plus pouvoir être utilisées pour identifier une personne physique en recourant à "l'ensemble des moyens susceptibles*

[1973] *Ibid*., pp. 131 et s.
[1974] G29, *avis 05/2014 sur les techniques d'anonymisation*, WP216, 10 avr. 2014.

d'être raisonnablement mis en œuvre", soit par le responsable du traitement, soit par un tiers. Un facteur important est que le traitement doit être irréversible »[1975]. Deux conditions de l'anonymisation se dégagent de cette définition. Tout d'abord, l'anonymisation des données à caractère personnel doit rendre non identifiable la personne concernée (**1)**, ensuite, l'anonymisation doit être irréversible (**2**).

1. La non-identification des données anonymes ou anonymisées

770- La première condition impose que l'anonymisation des données ait pour effet de ne plus identifier la personne concernée. Ainsi, peu importe la technique d'anonymisation mise en œuvre, il est nécessaire que « *les données ne permettent pas d'identifier la personne concernée par "l'ensemble" des moyens "susceptibles" d'être "raisonnablement" employés* »[1976].

2. Le caractère irréversible de l'anonymisation

771- Non réidentification de la personne concernée. Le G29 précise que « *le résultat de l'anonymisation, en tant que technique appliquée aux données à caractère personnel, devrait être, dans l'état actuel de la technologie, aussi permanent qu'un effacement, c'est-à-dire qu'il devrait rendre impossible tout traitement de données à caractère personnel* »[1977]. Le résultat de l'anonymisation doit être « *aussi permanent qu'un effacement* »[1978]. Par conséquent, il doit être totalement impossible de revenir en arrière et de réidentifier la personne concernée initialement par les données. L'ensemble des moyens « raisonnablement » susceptibles d'être utilisés ne doivent pas permettre la réversibilité de l'anonymisation et la réidentification de la personne concernée.

772- Les critères de l'irréversibilité de l'anonymisation. Le G29 a fixé trois critères pour connaître de la fiabilité des techniques d'anonymisation et des bonnes pratiques[1979]. D'abord, concernant les critères de fiabilité, la méthode choisie doit répondre à trois questions qui sont celles de savoir s'il est toujours possible d'isoler un individu, s'il est toujours possible de relier entre eux les enregistrements relatifs à un individu et si l'on peut déduire des informations concernant un individu. La CNIL s'appuie, également, sur ces critères pour conditionner

[1975] *Ibid*, p. 6.
[1976] *Ibid*.
[1977] *Ibid*.
[1978] G29, *avis 05/2014 sur les techniques d'anonymisation, op. cit*., p. 6.
[1979] *Ibid*., p. 27.

l'utilisation du responsable de traitement d'un jeu de données anonymisées : « *le responsable de traitement doit réaliser une analyse permettant de démontrer que ses processus d'anonymisation respectent les trois critères définis par l'avis n°05/2014* ». À défaut du respect de ces conditions, le responsable de traitement doit mener une étude des risques de réidentification, ainsi qu'une réévaluation régulière de ces risques[1980]. La CNIL s'appuie donc sur la bonne pratique d'anonymisation développée par le G29[1981]. En substance, « *l'identification doit être impossible pour le responsable de traitement ou pour toute autre personne* »[1982].

B. Les effets de l'anonymisation

773- L'anonymisation des données produit plusieurs effets. En premier lieu, la réglementation sur le RGPD cesse de s'appliquer (**1**). En second lieu, les données anonymisées entrent dans la catégorie des données à caractère non personnel (**2**).

1. L'exclusion des données anonymisées du RGPD

774- Le paquet européen sur la protection des données ne s'applique pas aux données anonymes ou anonymisées[1983]. Selon le considérant 26 du RGPD « *le présent règlement ne s'applique […], pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche* ». Par conséquent, les données anonymisées sont exclues de la protection du RGPD.

[1980] CNIL, Dél. n°2020-034 du 19 mars 2020 portant décision unique et autorisant la société Carte blanche partenaires à mettre en œuvre des traitements automatisés à des fins de recherche, d'étude et d'évaluation nécessitant un accès aux données nationales du programme de médicalisation des systèmes d'information (PMSI) (Saisine n°918404) ; Dél. n°2020-023 du 6 février 2020 portant décision unique et autorisant la société Pierre Karam Conseil santé à mettre en œuvre des traitements automatisés à des fins de recherche, d'étude et d'évaluation nécessitant un accès aux données nationales du programme de médicalisation des systèmes d'information (PMSI) (Saisine n°918249 v1).

[1981] G29, *avis 05/2014 sur les techniques d'anonymisation, op. cit,* p. 27 : « *Le responsable de traitement doit identifier les nouveaux risques et réévaluer régulièrement les risques résiduels ; Examiner si les contrôles des risques identifiés sont suffisants et les ajuster en conséquence ; Surveiller et contrôler les risques* ».

[1982] LESAULNIER, F., « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT*, 2016/12, p. 573.

[1983] *Ibid.*

2. La requalification en données à caractère non personnel

775- Les données anonymes ou anonymisées entrent dans la catégorie des données à caractère non personnel et seront alors soumises aux règlements qui leur sont applicables. Pour l'heure, les entreprises détentrices de données sur les exploitations agricoles peuvent traiter et réutiliser librement les données anonymes ou anonymisées sans faire reposer le traitement sur une quelconque base légale. Ces données ne sont plus identifiantes et ne font courir aucun risque de porter atteinte aux personnes concernées, les acteurs peuvent exploiter et partager librement leur « *gisement* » de données[1984] dans les mêmes conditions que les données à caractère non personnel. Aussi, elles entrent dans le champ d'application du Règlement n°2018/1807 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne[1985]. L'objet de ce règlement vise « *à assurer le libre flux de données autres que les données à caractère personnel au sein de l'Union* ». Les données anonymes ou anonymisées peuvent également être conservées « *au-delà de leur durée de conservation* »[1986]. Néanmoins, ces règles devraient bientôt changer en ce qui concerne les données à caractère non personnel avec la consécration du règlement sur les données proposé le 23 février 2022[1987]. Il faudra, alors, se conformer aux obligations en matière d'accès, d'utilisation et de partage des données à caractère non personnel lors de l'exploitation des données anonymisées.

II. Les difficultés de mise en œuvre des techniques d'anonymisation

776- Le CEPD (ex-G29) expose différentes techniques d'anonymisation sans, toutefois, être exhaustif. Cependant, à la lecture de la jurisprudence, il apparaît que la fiabilité des techniques d'anonymisation s'avère très difficile à démontrer. C'est pourquoi il convient d'envisager, dans un premier temps, les contraintes des méthodes d'anonymisation (**A**). Pour, dans un second temps, étudier l'efficacité, somme toute, relative des techniques d'anonymisation (**B**).

[1984] https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles
[1985] *JOUE* L 303/59 du 28 nov. 2018.
[1986] *Ibid.*
[1987] Voir *supra*, n°590 et s.

A. Les contraintes des méthodes d'anonymisation

777- D'une part, les techniques d'anonymisation sont complexes à mettre en œuvre dans le cadre du RGPD pour les responsables de traitement (**1**), d'autre part, les données anonymisées ont moins d'utilité (**2**).

1. Des techniques d'anonymisation complexes

778- **Définition des techniques d'anonymisation.** Le G29 a publié un avis sur les techniques d'anonymisation le 10 avril 2014[1988]. Il définit l'anonymisation comme « *une technique appliquée aux données à caractère personnel afin d'empêcher irréversiblement leur identification. L'hypothèse de départ est donc que les données à caractère personnel doivent avoir été collectées et traitées dans le respect de la législation applicable en matière de conservation des données sous une forme identifiable* ». Il précise également que l'anonymisation des données constitue un « *traitement ultérieur* » au sens du RGPD. Par conséquent, ce traitement ultérieur « *doit satisfaire au critère de compatibilité conformément aux lignes directrices proposées par le groupe de travail "Article 29" dans son avis 03/2013 sur la limitation des finalités*[1989] ».

779- **Techniques d'anonymisation.** Le choix de la technique d'anonymisation est laissé librement aux responsables de traitement. En effet, le RGPD ne fournit pas d'exemples de techniques d'anonymisation. La place est libre pour toutes les méthodes envisageables du moment que leur résultat est le même : les données doivent être totalement anonymisées. Pour combler cet espace vide, le G29 expose, dans son avis de 2014, de manière non limitative, des méthodes pouvant être utilisées comme processus d'anonymisation. Il s'agit des techniques de randomisation et de généralisation. Ce ne sont que des propositions puisque la CNIL a eu l'occasion de retenir que les avis du CEPD, ex-G29 (dont elle fait partie) n'étaient pas contraignants[1990], ils ne relèvent que du droit souple.

D'abord, la randomisation consiste « *à altérer la véracité des données personnelles contenues dans la masse* » en ajoutant du bruit ou en permutant des données. Il devient alors particulièrement difficile de retrouver une personne lorsque les données sont modifiées.

[1988] G29, *avis sur les techniques d'anonymisation*, WP 216, 10 avr. 2014.
[1989] *Ibid.* ; *id.*, *avis 03/2013 sur la limitation des finalités*, WP 203, 2 avr. 2013.
[1990] PERRAY, R. et UZAN-NAULIN, J., « Existe-t-il encore des données non personnelles ? », *Dalloz IP/IT*, 2017, p. 286.

Ensuite, la généralisation consiste à utiliser les techniques k anonymat ou l diversité. K anonymat permet « *de regrouper les personnes en catégories ordonnées par intervalles* ». l diversité « *prescrit l'indication de chaque groupe de personnes anonymes d'autant de facteurs que d'attributs utiles* ». Les acteurs sont donc libres d'utiliser les méthodes d'anonymisation de leur choix à condition de respecter les conditions d'irréversibilité et de non-identification des personnes concernées. Or, au vu de l'évolution des technologies toujours plus performantes, il est relativement difficile de répondre totalement à ces conditions.

Un exemple de hachage de données dans le secteur de la santé peut être développé. Il s'agit d'un dispositif cryptologique de fonction d'occultation d'identifiant nominatif (FOIN) élaboré en 1996 par la Caisse Nationale de l'Assurance Maladie des Travailleurs Salariés (CNAMTS). Ce dispositif permet de mettre en œuvre de manière fiable et sécurisée « *une version pseudonymisée des résumés de sortie hospitalière issus du programme de médicalisation des systèmes d'information (PMSI)* »[1991]. L'objectif est de suivre la prise en charge d'un patient au moyen d'un numéro d'identification anonyme. Pour cela le processus d'anonymisation doit être irréversible, robuste et sécurisé. Ce processus passe alors par la cryptographie afin d'éviter les risques de réidentification. Néanmoins, il a été soulevé en 2008 par l'ANSSI et en 2014 par la CNAMTS que l'algorithme sur lequel repose le dispositif FOIN serait rapidement obsolète et ne resterait, par conséquent, fiable que durant une période limitée[1992].

2. Le paradoxe de l'anonymisation des données personnelles

780- **Limites de l'anonymisation.** Avec le temps, les méthodes ont évolué, se sont affinées, afin de garantir le respect à la vie privée[1993] et la non-identification des personnes concernées. Néanmoins, un paradoxe est né de cela puisqu'en contrepartie d'une bonne anonymisation les données perdent en utilité. En effet, plus les données sont transformées pour assurer leur anonymisation, moins elles sont utiles pour les usages futurs.

781- **Des solutions au paradoxe limitées.** Aujourd'hui, de nouvelles méthodes s'appuient sur l'anticipation selon l'objectif de l'usage des données lorsqu'il est connu au préalable[1994].

[1991] TROUESSIN, G., « Données de santé : anonymat et risque de ré-identification », Dossiers Solidarité et santé, n°64, juill. 2015, p. 96.
[1992] https://www.silicon.fr/donnees-sante-protegees-indesirable-sha-1-146672.html.
[1993] ZOLYNSKI, C., « Le sens des normes *by design* », *op. cit.*
[1994] *Ibid.*

Cependant, l'usage qui va être fait des données après leur anonymisation n'est pas toujours connu. Il est donc difficile d'anticiper tous les usages pour assurer une anonymisation efficace.

Afin d'éviter les désagréments liés de l'anonymisation des données, le CNNum a fait des préconisations dans le cadre de *l'Open Data*, avec la mise en place d'une licence spécifique pour les données anonymisées[1995]. Ainsi, la licence devrait contenir des clauses obligatoires qui portent sur l'obligation d'informer les utilisateurs quant au « *fait que le jeu de données a fait l'objet d'une anonymisation* ». De plus, une clause devrait prévoir qu'il est interdit de procéder à « *des recoupements d'informations anonymisées ou toute autre pratique permettant de rendre ces données identifiantes* ». Enfin, le responsable de traitement devrait informer le réutilisateur sur le fait qu'il engage sa responsabilité dans le cas où il procèderait à des « *pratiques de croisement de données anonymisées* ».

782- **Constat d'échec.** Dans tous les cas, la technique n'a pas permis de découvrir de solutions efficaces en toutes circonstances[1996]. D'autant que l'évolution des techniques d'anonymisation entraine dans son sillage les techniques de désanonymisation. L'évolution de l'informatique ne s'arrête pas à l'anonymisation des données, elle évolue également pour son corollaire.

B. L'efficacité relative des méthodes d'anonymisation

783- Les risques de réidentification que font courir les techniques d'anonymisation (**1**) soulèvent la question de savoir si l'utilisation de l'anonymisation comme outil pour l'exploitation des données ne devrait pas être abandonnée (**2**).

1. Les risques de réidentification

784- **Réidentification.** Les scientifiques ont pointé du doigt les possibilités de réidentification grâce aux moyens technologiques et au *Big Data* permettant aujourd'hui de faire des croisements de données et de parvenir à l'identification d'une personne. C'est ce que révèle notamment une étude menée par l'Université Catholique de Louvain et l'*Imperial College* de Londres publiée dans Nature le 23 juillet 2019, dans laquelle les chercheurs ont développé un algorithme de *Machine learning* afin de réidentifier les personnes concernées. Le résultat est sans appel, l'algorithme a permis de réidentifier 83 % des Américains à partir de trois critères seulement,

[1995] CNNum, *Ambition numérique*, *op. cit.*, p. 141.
[1996] CASTETS-RENARD, C. et GANDON, N., « *Open Data* des données de la recherche publique : entre réformes législatives et retour d'expérience sur un guide pratique à destination des chercheurs », *Légicom*, 2016, p. 67.

et 99,98 % avec quinze critères[1997]. Aussi, de manière unanime, les auteurs concluent à la difficulté d'assurer l'irréversibilité des techniques d'anonymisation[1998]. Le CEPD a lui-même considéré que « *le résultat de l'anonymisation […] devrait être, dans l'état actuel de la technologie, aussi permanent qu'un effacement, c'est-à-dire qu'il devrait rendre impossible tout traitement de données à caractère personnel* »[1999]. Or, au vu de la difficulté de mettre en œuvre l'anonymisation des données, c'est à se demander si seul l'effacement ne permettrait pas de garantir l'impossibilité de tout traitement de données à caractère personnel. En effet, trois risques de réidentification ont été identifiés par le CEPD, ex-G29. D'abord, l'individualisation « *correspond à la possibilité d'isoler une partie ou la totalité des enregistrements identifiant un individu dans l'ensemble de données* ». Ensuite, la corrélation « *consiste dans la capacité de relier [entre eux], au moins, deux enregistrements se rapportant à la même personne concernée ou à un groupe de personnes concernées (soit dans la même base de données, soit dans deux bases de données différentes)* ». Enfin, l'inférence, « *est la possibilité de déduire, avec un degré de probabilité élevé, la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs* ». En réalité, « *tout dépend de la solidité de l'anonymisation* »[2000]. Mais, comme le relève un auteur, cette solidité n'est pas inhérente à la méthode d'anonymisation, elle dépend à la fois de « *l'habilité de l'attaquant éventuel et du caractère raisonnable des moyens préventivement mobilisés pour que l'attaque échoue* »[2001].

785- **Requalification en données pseudonymisées.** Le risque de la réidentification des données à caractère personnel est la qualification des données anonymisées en données pseudonymisées. Une telle requalification a pour effet d'engager la responsabilité du responsable de traitement et de l'attaquant. La « pseudonymisation » est définie comme « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires* ». Pour le garantir, le texte a posé des exigences opérationnelles strictes. Il requiert, d'abord, « *que ces informations supplémentaires soient conservées séparément* », selon la méthode de codification, notamment utilisée en matière d'essais cliniques[2002]. Ensuite, les informations doivent être « *soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère*

[1997] https://usbeketrica.com/fr/article/donnees-personnelles-etude-enterre-anonymat

[1998] *Ibid.* ; DESTREGUIL, M., « Plaidoyer en faveur d'une approche propriétarise des données personnelles », *op. cit.*

[1999] G29, *avis 05/2014 sur les techniques d'anonymisation*, *op. cit.*, p. 6.

[2000] VIANGALLI, F., « Des données à la responsabilité : de l'anonymisation à l'attaque par ré-identification », *RLDI*, n°173, 1e août 2020.

[2001] *Ibid.*

[2002] G29, *avis n°4/2007 sur le concept de données à caractère personnel*, *op. cit.*, pp. 20 et 21.

personnel ne sont pas attribuées à une personne physique identifiée ou identifiable ». Toutefois, la pseudonymisation n'empêche pas l'application du RGPD à la différence de l'anonymisation des données.

2. Les restrictions des techniques d'anonymisation : la mort annoncée de l'anonymisation ?

786- **Techniques d'anonymisation invalidées.** À la lecture de la jurisprudence, les techniques d'anonymisation suffisamment efficaces pour rendre en tous points anonymes des données sont relativement difficiles à mettre en place. En effet, l'arrêt *JCDecaux*[2003] permet de constater la lecture particulièrement restrictive que fait le juge des « *moyens raisonnablement susceptibles d'être utilisés par le responsable de traitement ou par toute autre personne* ».

Dans cette affaire, la société JCDecaux avait déposé auprès de la CNIL une demande d'autorisation d'un traitement automatisé de données à caractère personnel qui consistait à traiter pendant quatre semaines des adresses MAC, identifiants réseaux des appareils mobiles ayant l'interface WIFI activée dans un rayon de 25 m des panneaux publicitaires et à calculer leur position géographique. La finalité de ce traitement devait être une méthodologie d'estimation quantitative des flux de piétons sur la dalle de La Défense ainsi que des axes de déplacements effectués dans ce périmètre. Afin de respecter l'obligation d'anonymisation des données, la société JCDecaux avait présenté des techniques d'anonymisation. D'abord, elle souhaitait tronquer les adresses MAC de leur dernier demi-octet, pour ensuite les compléter par une suite de caractères en application de la technique dite « salage », afin de mettre en œuvre une méthode dite de « hachage à clé », en transformant une donnée. La société avançait également que ces opérations rendaient négligeable le risque de réidentification et que, de toute façon, la collecte des données avait pour seul objectif d'améliorer la valorisation des panneaux publicitaires, l'identification des personnes concernées étant sans intérêt pour elle. Cette collecte avait en outre vocation à être limitée dans le temps puisqu'il s'agissait d'une expérimentation de quatre semaines. La CNIL a cependant refusé de donner l'autorisation de mettre en œuvre ce traitement automatisé de données au motif notamment que les techniques d'anonymisation avancées par la société JCDecaux n'étaient pas suffisamment efficaces pour empêcher la réidentification des personnes concernées. La société JCDecaux a alors demandé l'annulation de cette décision pour excès de pouvoir. Dans un arrêt du 8 février 2017, les 10e et 9e chambres réunies du Conseil d'État ont validé le raisonnement de la CNIL en retenant que

[2003] CE, 10ème - 9ème chambres réunies, 08 févr. 2017, 393714, rec.

les techniques d'anonymisation ne sont pas compatibles avec une anonymisation des informations recueillies parce que le gestionnaire du traitement peut identifier les personnes concernées et le traitement permet de compter le nombre de terminaux mobiles et le nombre de passages sur la dalle de La Défense, ce qui permettait par conséquent de déterminer les comportements des personnes concernées. Les juges retiennent alors que la donnée doit être rendue anonyme à la fois pour les tiers et pour le responsable de traitement[2004]. De même, les procédés évoqués de « hachage » et de « salage » n'empêchent pas le responsable de traitement *« de procéder à l'identification des personnes concernées et n'interdisent ni de corréler des enregistrements relatifs à un même individu, ni d'inférer des informations le concernant* ». Par conséquent, le Conseil d'État n'y voit alors qu'une mesure de sécurité, certes efficace, mais pas de nature à garantir une anonymisation au sens strict, c'est-à-dire, parfaitement irréversible qui empêcherait l'application du RGPD.

787. **Techniques d'anonymisation validées.** La CNIL a toutefois dans le passé validé des techniques d'anonymisation. C'était le cas notamment dans une délibération du 9 mai 2017[2005] pour un traitement qui portait là encore sur les adresses MAC des appareils mobiles, collectées à l'aide de boitiers de détection spécifiés et fabriqués par la société demanderesse. Le procédé consistait en l'anonymisation des données dans les cinq minutes suivant leur collecte directement dans le boitier et se basait sur une méthode d'agglomération des informations individuelles qui seules ne seraient pas utiles. Cette agglomération était réalisée dans deux microcontrôleurs embarqués dans les boitiers et fonctionnant de façon disjointe et asynchrone. En plus de cela, des procédés cryptographiques successifs étaient mis en œuvre et en particulier des techniques de hachage utilisant des sels renouvelés tous les quinze jours (soit pour chaque campagne de mesure). Enfin, les données étaient envoyées chaque soir aux serveurs de la société demanderesse au moyen de réseaux de communication chiffrés utilisant le protocole HTTPS et assurant l'authentification de la source et de la destination. La Commission a fait des observations sur ces techniques d'anonymisation et a considéré que des mesures de protection étaient mises en œuvre à la fois en matière de logiciel et de manière physique. En effet, le logiciel ne permettait pas d'accéder aux adresses MAC des personnes concernées, les données étaient conservées dans la mémoire vive des boitiers (en cas de coupure d'alimentation, les

[2004] « *… ne peut être regardée comme rendue anonyme que lorsque l'identification de la personne concernée, directement ou indirectement, devient impossible que ce soit par le responsable du traitement ou par un tiers* ».
[2005] CNIL, dél. n°2017-145 du 09 mai 2017 autorisant la société Retency à mettre en œuvre à titre expérimental un traitement automatisé de données à caractère personnel ayant pour finalité la mesure d'audience et de fréquentation de dispositifs publicitaires au sein de la gare SNCF de Dijon (demande d'autorisation n°2020915).

données étaient automatiquement effacées) et un procédé d'effacement avait été mis en place en cas d'ouverture du boitier.

Récemment encore, la CNIL a validé une méthode d'anonymisation des données de santé par avatar portée par la société WeData[2006] et expérimentée au CHU de Nantes.

Comme le soulèvent certains auteurs, « *les cas dans lesquels une technique pourra être considérée comme une véritable anonymisation sera pour le moins extrêmement rare. D'autant plus, compte tenu de l'exigence de réévaluer régulièrement les risques résiduels, examiner si les contrôles des risques identifiés sont suffisants et les ajuster en conséquence* »[2007].

788- **La quasi-impossibilité d'anonymiser des données de l'exploitation agricole**. Au vu de ces différents exemples, ce n'est qu'au coût d'une mise en œuvre particulièrement drastique des techniques d'anonymisation que la CNIL accorde son aval. L'anonymisation des données personnelles n'est donc pas à la portée de tous, elle nécessite des moyens techniques, financiers et opérationnels conséquents afin d'obtenir l'accord de la CNIL. Par conséquent, certains auteurs considèrent que l'anonymisation n'est jamais tout à fait irréversible et appellent à une modification du règlement afin de supprimer cette possibilité.

789- **Conclusion de la section.** Le RGPD permet aux responsables de traitement de traiter des données à caractère personnel à des fins autres que celles expressément prévues par le Règlement, soit en demandant le consentement de la personne concernée, soit en anonymisant les données. Néanmoins, ces solutions doivent être maniées avec prudence puisqu'un consentement non valable ou un risque de réidentification auraient pour effet d'engager la responsabilité du responsable de traitement.

790- **Conclusion du chapitre.** Comme toute personne physique, l'agriculteur bénéficie également de la protection des données à caractère personnel pour les données issues de son exploitation permettant de l'identifier dans son individualité. C'est pourquoi les entreprises de l'*AgTech* doivent porter une attention accrue aux données des exploitations afin de déterminer celles qui permettent d'identifier l'agriculteur en tant que personne physique. En présence de telles données, ces entreprises devront se soumettre aux obligations du RGPD lors de leur traitement.

[2006] https://www.usine-digitale.fr/article/la-cnil-approuve-wedata-pour-l-anonymisation-des-donnees-de-sante.N1024644

[2007] VIVANT, M., WARUSFEL, B., MALLET-POUJOL, N. et COSTES, L., *Le Lamy droit du numérique, (Guide)* n°3921.

791- **Conclusion du titre.** Les nombreuses données collectées sur les exploitations agricoles renferment des informations précieuses à la fois pour l'agriculteur lui-même et pour les entreprises de l'agriculture numérique. Cependant, certaines données à caractère non personnel devraient faire l'objet d'un contrôle de l'usage par l'agriculteur dès lors qu'elles ne portent pas sur des informations d'intérêt public ou général et qu'elles n'ont pas fait l'objet d'un enrichissement substantiel. Cette solution est envisagée pour les données industrielles non personnelles par le Règlement sur les données proposé par la Commission européenne le 23 février 2022. Celui-ci devrait donc permettre de renforcer les droits des agriculteurs sur les données brutes non personnelles qu'ils génèrent lors de leurs activités, de la même manière que le RGPD a renforcé les droits des agriculteurs, personnes physiques, sur les données personnelles qu'ils fournissent ou qui sont issues de leur exploitation.

792- **Conclusion de la partie.** Afin de renforcer les droits des agriculteurs, les replacer au centre de l'économie des données agricoles et les protéger de certains comportements prédateurs des entreprises de l'agriculture numérique, reconnaître un droit de contrôle de l'usage en leur faveur semble tout indiqué. En effet, un tel droit leur permettrait, par exemple, de choisir les utilisations possibles de leurs données ou les personnes à qui ils souhaitent les partager. Dans ce sens, la future réglementation sur les données présentée le 23 février 2022 devrait permettre, en grande partie d'atteindre ces objectifs. Un tel droit de contrôle de l'usage sur les données à caractère non personnel aurait également le mérite d'harmoniser, dans une certaine mesure, le régime de ces données avec celui des données à caractère personnel. Toutefois, le législateur devrait toujours garder à l'esprit la nécessité d'assurer la circulation des données en recherchant un équilibre entre ces différentes injonctions parfois contradictoires afin d'éviter une sclérose des activités numériques dans le secteur agricole.

Conclusion

793- Ce travail de recherche a eu pour objectif d'étudier les conséquences juridiques de l'évolution du secteur agricole vers le numérique quant à l'exploitation des données. Le monde agricole essentiellement attaché au travail de la terre est aujourd'hui en pleine mutation. La valeur des connaissances des agriculteurs se déplace sur celle de la détention et de l'utilisation des données. Les rapports de force et les pouvoirs de chacun évoluent en raison de la détention des données des exploitants agricoles par les entreprises positionnées sur ce nouveau marché. Si, avant les évolutions technologiques, les agriculteurs avaient la pleine maîtrise de leur activité sur leur exploitation, de nos jours l'omniprésence des objets connectés et des services numériques dans les champs et les fermes réduit leur isolement, mais peut aussi les rendre captifs des concepteurs de matériels et des fournisseurs de services. Aussi, l'étude du droit des données agricoles a exigé l'analyse de chacune des réglementations qui leur étaient applicables. Ce travail s'est révélé délicat à plusieurs égards. En effet, les données agricoles répondent à des injonctions différentes, voire contradictoires, et parfois de manière cumulative. Un *patchwork* de droits forme ainsi un halo juridique autour de ces données qui complique la matière. Néanmoins, si dans les années 1990 l'objectif était essentiellement de protéger l'investissement[2008] et donc les entreprises qui détenaient les données, aujourd'hui les ambitions politiques tendent plutôt vers plus d'accessibilité et une meilleure circulation de ces données dans l'espace européen[2009] afin notamment de susciter l'innovation et la créativité. Mais cette libération des données vise également à les rendre plus accessibles pour le co-contractant des entreprises de l'*AgTech* afin également de leur permettre de contrôler l'usage des données qu'ils génèrent. Les personnes impliquées dans l'exploitation des données agricoles devaient donc être identifiées dans le but de mieux cerner les rôles de chacun, à savoir qui détient les données, qui les génèrent, qui les utilisent, etc.

794- Aussi, l'ambition du législateur est apparue au cours de ce travail de recherche comme étant de « délivrer » les données en général, et les données agricoles en particulier, afin de les rendre plus accessibles, d'une part, et de rétablir les rapports de force dans les contrats, d'autre part (**I**). Néanmoins, il faut garder en vue que de rendre effectif le droit des données agricoles ne doit pas en contrepartie scléroser le marché de l'agriculture numérique (**II**).

[2008] Dir. n°96/9/CE, du 11 mars 1996, concernant la protection juridique des bases de données

[2009] Commission européenne, *Une stratégie européenne pour les données*, 19 févr. 2020, COM(2020) 66 final.

I. L'ambition de la « délivrance » des données agricoles

795. Au cours de cette recherche, un premier axe concernant la « délivrance » des données agricoles sur le marché à l'égard de tous est apparu afin de les rendre plus accessibles et d'encourager leur partage. Le second axe soulevé portait sur la maîtrise des données qui a pour objectif de rééquilibrer les pouvoirs des parties sur les données agricoles dans les relations contractuelles.

796. **Une accessibilité renforcée aux données publiques.** Il a été étudié que les données agricoles peuvent être soumises à la politique d'ouverture des données publiques, qui organise l'accès et la diffusion des données, lorsqu'elles sont collectées ou produites au cours d'une mission de service public. Par exemple, les données géographiques et les données environnementales collectées ou produites au cours d'une mission de service public doivent, à ce titre, être diffusées. Cette libération des données tend vers la création d'un État-plateforme. Dans cette perspective, le secteur agricole a ainsi créé la plateforme API-AGRO[2010] afin de favoriser et d'encourager le partage des données de l'agriculture numérique.

797. **Une accessibilité renforcée des données de la recherche scientifique.** Les données produites à des fins de recherche scientifique sont également soumises à une obligation de diffusion dans le cadre d'une mission de partage et de diffusion des connaissances scientifiques. Par conséquent, les données agricoles collectées par les chercheurs à des fins de recherche scientifique doivent également être diffusées et être largement accessibles[2011].

Ainsi, ces développements ont permis d'envisager les données agricoles qui devaient être diffusées dans l'intérêt public ou pour l'enrichissement des savoirs. Mais ce raisonnement est facilité dès lors que tant l'Administration que les instituts et autres organismes de recherche sont soumis par la loi à l'obligation de diffusion des données qu'ils détiennent. La question a été plus délicate toutefois s'agissant de l'accès aux données agricoles privées.

798. **Les perspectives d'ouverture de certaines données privées.** La question de l'ouverture des données faisant l'objet d'une réservation privative a sollicité, dans un premier temps, la recherche de la définition de la notion de données privées. Pourtant ni la loi ni la doctrine n'ont encore donné de définition à cette notion, puisqu'elle recouvre des réalités bien trop différentes pour toutes les cantonner dans une seule acception[2012]. Or, ces données, bien que d'origine privée, peuvent avoir un intérêt pour le public en général, mais aussi pour les consommateurs

[2010] Voir *supra*, n°673.
[2011] Voir *supra*, n°59 et s.
[2012] Voir *supra*, n°135.

ou toute autre personne de la société civile. En effet, celles contenant des informations environnementales ou encore celles qui ont trait à la santé humaine peuvent revêtir le caractère de données d'intérêt général. L'ouverture de ces données n'est pas encore effective et repose encore sur un système d'intermédiation avec la personne publique avant toute diffusion ce qui rend leur accessibilité limitée. Cet écueil fait l'objet de critiques par la doctrine qui plébiscite une ouverture des informations en raison de leur objet et non plus du caractère privé ou public de la personne qui les détient[2013].

Les données d'intérêt général ne sont pas les seules dans le viseur du législateur, les données conférant un avantage concurrentiel sont également soumises à une politique d'ouverture. L'objectif est ainsi de libérer le marché et de limiter les atteintes au libre jeu de la concurrence. Néanmoins, le marché de l'agriculture numérique apparaît comme un secteur dynamique pour lequel l'abus de position dominante est difficile à établir ainsi que l'éventuelle atteinte au libre jeu de la concurrence par un acteur du secteur en particulier. De plus, les évolutions technologiques permettent à chaque acteur de collecter les données dont il a besoin afin de développer ses propres services. Il apparaît donc que les enjeux concurrentiels se situent plutôt sur la variété des services proposés et leur qualité plutôt que sur la détention des jeux de données agricoles en elle-même. Le manque d'interopérabilité des services pourrait toutefois limiter la collaboration avec les plus petits acteurs dont l'utilisation des services nécessite l'appariement avec les outils et les solutions informatiques de leurs concurrents.

799. **L'exception de fouilles de textes et de données.** Un autre élément permet de constater cette libération des données, il s'agit de l'exception de fouille de textes et de données qui repose sur deux composantes. La première permet aux chercheurs d'accéder au contenu des bases de données à des fins de recherche scientifique[2014], tandis que la seconde, intégrée en droit français par l'ordonnance du 24 mai 2021[2015], intéresse toute personne qui le souhaite à condition toutefois d'avoir souscrit un abonnement ou en tout cas d'avoir accès aux données de manière licite. Dans le deuxième cas, le producteur de la base peut néanmoins décider de refuser la fouille de textes et de données dans la licence d'utilisation qu'il propose. Par conséquent, bien que cette exception au droit des bases de données reste limitée pour l'objectif d'ouverture des

[2013] EPSTEIN, A.-S., « La compatibilité du droit d'accès aux informations environnementales de source privée avec la protection du secret des affaires : Prélude à la consécration d'un droit d'accès aux données d'intérêt général de source privée », *RJE*, 2020/HS20 n° Spécial, pp. 137 à 149 ; ROCHFELD, J., CORNU, M. et MARTIN, G., J., ss. dir., L'*échelle de communalité, Propositions de réforme pour intégrer les biens communs en droit*, Rapport final de recherche, n°17 à 34, avr. 2021.

[2014] Voir *supra*, n°264.

[2015] Ord. n°2021-1518 du 24 nov. 2021 complétant la transposition de la directive 2019/790 du Parlement européen et du Conseil du 17 avril 2019 sur le droit d'auteur et les droits voisins dans le marché unique numérique et modifiant les directives 96/9/CE et 2001/29/CE : *JORF* n°0274 du 25 nov. 2021.

données, il demeure que son existence démontre une nouvelle fois la volonté du législateur d'ouvrir les données au plus grand nombre.

800- **La liberté de réutilisation des informations publiques produites par l'Administration.** Pour terminer, la délivrance des données passe également par leur possible réutilisation. Les informations publiques font en effet l'objet d'un droit de réutilisation que la directive *Public Sector Information* du 20 juin 2021 devrait renforcer[2016]. Aussi, les données contenues dans les bases de données produites par l'Administration sont librement réutilisables (ex. données de référence). De plus, le principe de gratuité, irriguant la liberté de réutilisation des informations publiques et interdisant les redevances allant au-delà de la part substantielle des coûts liés à l'accomplissement de leur mission de service public, tend une nouvelle fois vers une libération des données. La circulaire n°6224/SG du Premier ministre du 27 avril 2021 confirme cette tendance puisqu'elle prévoit l'extinction des redevances de réutilisation d'ici 2023. À ce titre, Météo-France et l'Institut national de l'information géographique et forestière (IGN) sont aujourd'hui désormais contraints de rendre gratuite la réutilisation des données qu'ils produisent.

801- **La réservation des données.** La tendance naturelle du marché de l'agriculture numérique tend vers la réservation des données par les entreprises qui les détiennent. En effet, les fournisseurs de services et les fabricants de matériels peuvent accaparer de grands jeux de données lorsqu'elles en ont les moyens techniques et financiers. Le droit est particulièrement accommodant avec les comportements réservataires puisque le droit de la propriété intellectuelle offre une double protection aux bases de données qui répondent aux conditions soit du droit d'auteur, soit du droit *sui generis*. Mais dans le cas où la base de données ne répondrait pas à ces conditions, l'entreprise peut tout de même réserver l'accès aux données au moyen du contrat (clause de confidentialité, secret d'affaires)[2017] et de la technique (STAD)[2018]. Cette inclination pour la réservation peut s'avérer néfaste pour les agriculteurs puisqu'ils n'ont pas toujours l'accès à leurs données ni le contrôle de leur usage.

802- **Le contrôle de l'usage des données.** L'usage étant par nature une prérogative du droit de la propriété, les données, en elles-mêmes, ne peuvent faire l'objet d'un tel droit en raison de leur caractère non rival et reproductible. Aussi, ni le droit ni le contrat ne permettent à l'agriculteur d'obtenir de manière efficiente le contrôle de l'usage des données qu'il génère par son utilisation des objets connectés et des services liés. Les acteurs du numérique ont bien proposé

[2016] Voir *supra*, n°414.
[2017] Voir *supra*, n°304 et s.
[2018] Voir *supra*, n°376 et s.

un cadre pour leurs propres contrats afin de mieux partager la valeur des données agricoles, mais ce droit souple manque encore d'effectivité. En effet, bien que ces textes de *Soft Law* organisent, notamment, l'accès et le contrôle de l'usage des données que détiennent les entreprises de l'*AgTech* de manière favorable à l'agriculteur, ils peuvent toutefois à certaines reprises manquer de cohérence et de clarté, mais aussi et surtout d'effets dissuasifs. Dans les faits, tant la Charte Data-Agri que le Code de conduite de l'Union européenne relatif au partage des données par accord contractuel, sont encore trop peu appliqués et manquent d'efficacité. C'est pourquoi seule une réglementation impérative pourrait assurer un véritable contrôle de l'usage par l'exploitant agricole.

803- **Évolution législative.** C'est ainsi que la législation européenne se dirige aujourd'hui vers un assouplissement des règles de réservation et de contrôle par l'entreprise qui détient les données, puisque le futur règlement sur les données proposé en février 2022 par la Commission européenne devrait une nouvelle fois limiter le droit *sui generis*. En effet, l'article 35 de la proposition de règlement prévoit que les données industrielles c'est-à-dire celles qui sont obtenues ou générées par des objets connectés seront exclues de la protection du droit des bases de données. En outre, ce futur règlement envisage un régime spécifique en faveur des utilisateurs d'objets connectés qui leur permet d'accéder, d'utiliser et de partager avec des tiers les données qu'ils génèrent par leur utilisation. En sont néanmoins exclues les données ayant fait l'objet d'un « enrichissement significatif », ce qui permet de conserver l'intérêt de l'investissement des entreprises dans l'enrichissement des données agricoles. Par conséquent, les agriculteurs qui utilisent des objets connectés sur leur exploitation pourraient bénéficier de cette réglementation. Il serait alors nécessaire d'harmoniser le droit national applicable afin d'interdire toute forme de réservation de ces données que ce soit par le contrat ou par la technique. Il semble néanmoins que certaines spécificités de l'agriculture numérique ne sont pas prises en compte dans le texte. Aussi, à cette fin, il serait nécessaire que le texte soit affiné afin de prendre en considération le niveau de sensibilité de certaines données. Le régime applicable différerait ainsi selon qu'il s'agit de données « normales » d'exploitation, ne portant sur aucune information considérée comme sensible par l'agriculteur, ou bien de données sur lesquelles l'agriculteur souhaiterait conserver la maîtrise en raison des informations qu'elles contiennent (les techniques agricoles, par exemple). Un tel droit devrait permettre de prendre en compte de manière plus fine et granulaire les intérêts de chacun.

804- **Une pierre de plus à l'édifice de la stratégie européenne en matière de données.** La réglementation sur les données devrait rejoindre les textes déjà adoptés par le parlement

européen pour la construction d'une stratégie européenne en matière de données[2019]. Elle permettrait, dans une certaine mesure d'harmoniser le droit applicable aux données industrielles non personnelles sur celui des données à caractère personnel couvertes par le RGPD. En effet, les entreprises qui traitent des données personnelles des agriculteurs répondent déjà aux obligations des responsables de traitement. Toutefois, ces traitements demandent beaucoup de vigilance puisque le consentement de l'agriculteur et l'anonymisation des données s'avèrent dans les faits difficiles à obtenir. Les entreprises de l'agriculture numérique pourraient alors à ce titre engager leur responsabilité.

II. Vers un droit des données agricoles effectif et le maintien d'un marché dynamique

805.- Afin de rendre plus effectif le contrôle de l'usage des données, certains auteurs préconisent de reconnaître la patrimonialité des données à caractère personnel et de rémunérer les personnes en échange de l'utilisation de leurs données. Cette option n'a pas été développée au cours de cette recherche puisqu'il semble qu'en raison du caractère non-rival et reproductible des données et des difficultés de les évaluer en argent il serait difficile de mettre en place un tel système. La contrepartie de l'échange des données semble résulter plutôt de la fourniture d'un service ou d'un matériel que d'une somme d'argent.

806.- De plus, le monde agricole est aujourd'hui fragilisé par le numérique puisque les données peuvent être la cible de pirates informatiques. Aussi, bien qu'il ait été rappelé que les entreprises avaient des obligations de sécurisation des données, la Cybersécurité n'a pas pu être approfondie et mériterait des développements plus conséquents.

807.- Également, le contrôle de l'usage sur les données de l'exploitant agricole, co-contractant générateur de données, doit se cantonner aux seules données qu'il génère. Aussi, les entreprises de l'agriculture numérique doivent conserver la maîtrise des données qu'ils enrichissent de manière significative. Afin de mieux encadrer les données agricoles, il serait donc opportun de définir exactement ce qui est entendu par « enrichissement significatif ». L'objectif étant que les entreprises ne donnent pas elles-mêmes leur propre définition de l'enrichissement pour éviter que toute sorte de travail sur les données puisse être considéré comme tel. Ainsi, le droit de contrôle de l'usage pourrait devenir plus effectif.

[2019] Voir *supra*, n°34.

808- Afin de maintenir et favoriser le dynamisme du marché des données agricoles, un équilibre doit être trouvé entre les différents impératifs. Il s'agit en effet d'assurer à la fois la circulation, la réservation, le partage et la protection des données agricoles, le cas échéant. Les risques d'une sclérose du marché pourraient ainsi venir de l'existence d'un trop grand nombre de réglementations à la fois de textes impératifs et de textes négociés. Il semble alors essentiel de clarifier et simplifier la réglementation applicable aux droits des données agricoles.

809- L'objectif est donc d'obtenir une meilleure effectivité de la protection des agriculteurs et un meilleur partage des données sur le marché dans lequel les intérêts de chacun seraient respectés et la valeur des données partagée de manière plus équitable. Plusieurs options pouvaient être envisagées. La première consistait en une libéralisation du marché afin de laisser les acteurs s'autoréguler. Il semble que cette option laisserait néanmoins trop la place aux comportements prédateurs sur les données, ce qui créerait des tensions et des crispations pour les nouveaux entrants sur le marché. Au contraire, la deuxième option aurait pu consister en la création d'un régime protectionniste afin de contrôler l'accès et l'usage des données dans le but de protéger à la fois, la circulation de l'information, les données des agriculteurs et l'investissement. Néanmoins, il semble qu'un régime trop protectionniste pourrait également avoir pour effet de scléroser le marché en encourageant les entreprises à contourner la loi pour conserver leur compétitivité. Par conséquent, il semble que la solution se situe entre les deux options. Il s'agit donc de renforcer les pouvoirs de l'agriculteur sur les données qu'il génère tout en favorisant la circulation des données entre les différents acteurs. C'est l'option que semble avoir choisie le législateur européen à travers sa Proposition de règlement sur les données du 23 février 2022 et le Règlement sur la gouvernance des données du 30 mai 2022.

810- En outre, il sera nécessaire dans le futur de s'assurer que cette réglementation n'aura pas d'effets indésirables de blocage de l'économie de l'agriculture du numérique et donc de l'innovation afin de maintenir la compétitivité des entreprises françaises et européennes sur le marché international. En effet, la concurrence de mastodontes venant d'États, tels que la Chine ou les États-Unis moins regardants sur le droit des données, et en particulier sur les données personnelles, pourrait avoir de lourdes conséquences sur l'extension du marché de l'agriculture numérique français et européen.

Bibliographie

I. OUVRAGES

A. OUVRAGES JURIDIQUES

1. Traités et manuels

a. Droit privé

Droit de la propriété intellectuelle

BINCTIN N., *Droit de la propriété intellectuelle : droit d'auteur, brevet, droits voisins, marque, dessins et modèles,* LGDJ, 7e éd., 2022.

BERNAULT C., LUCAS A., et LUCAS-SCHLOETTER A., *Traité de la propriété littéraire et artistique,* LexisNexis, 5e éd., 2017.

BRUGUIERE J.-M., MALLET-POUJOL N. et ROBIN A., ss. dir., (équipe ERCIM) *Propriété intellectuelle et droit commun,* Université Paul Cézanne Aix-Marseille III, Presses Universitaires d'Aix-Marseille, 11/2007.

CLEMENT-FONTAINE M., *L'œuvre libre,* préf. Vivant M., Larcier, 2014.

GRYNBAUM L., LE GOFFIC C. et MORLET-HAÏDARA L., *Droit des activités numériques,* Dalloz, 1e éd., 2014.

MATTATIA F., *Droit d'auteur et propriété intellectuelle dans le numérique*, Eyrolles, 2e éd., 2019.

ROBIN A. et CHATRY S., *Introduction à la propriété intellectuelle*, 3e éd., Bruylant, 2021.

VIVANT M., ss. dir., *Grands Arrêts de la propriété intellectuelle,* Dalloz, 3e éd., 2020.

VIVANT M. et BRUGUIERE J.-M., *Droit d'auteur et droits voisins*, Dalloz, 4e éd., 2019.

Droit du numérique

CATALA P.,

- *Les transformations du droit par l'informatique, Émergence du droit de l'informatique,* éd. Des Parques, 1983.
- *Le droit à l'épreuve du numérique,* Jus Ex Machina, PUF, 1998.

CHATRY S. et GOBERT T., *Numérique : Nouveaux droits, nouveaux usages,* Mare & Martin, 2017.

GAUDRAT P. et SARDAIN F., *Traité de droit civil du numérique*, t.1 Droit des biens, Larcier, sept. 2015.

QUEMENER M., *Le droit face à la disruption numérique. Adaptation des droits classiques, Émergence de nouveaux droits*, Gualino, 2018.

LUCAS A., *Le droit de l'informatique*, PUF, 1987.

LUCAS A., DEVEZE J. et FRAYSSINET J., *Le droit de l'informatique*, 2e éd., PUF, 2001.

VIVANT M., WARUSFEL B., MALLET-POUJOL N. et COSTES L., *Le Lamy droit du numérique,* 2021.

Droit civil/des biens

ATIAS CH., *Droit civil, Les biens,* 11e éd., Litec, 2011.

BAUDRY-LACANTANERIE G., *Traité théorique et pratique de droit civil, Les biens*, Paris, 1896.

BERLIOZ P., *La notion de bien*, LGDJ, préf. Aynés L., 2007.

CARBONNIER J.,

- *Droit civil. Les biens, les obligations*, t.3, 2e éd., PUF, Paris, 2017.
- *Droit civil. Les personnes*, t.1, 20e éd., PUF, 2017.

CHARDEAUX M.-A., *Les choses communes*, LGDJ, 2006.

PIEDELIEVRE A., *Le matériel et l'immatériel, Essai d'approche de la notion de bien*, Mélanges M. Juglart, LGDJ, 1986.

PLANIOL M. et RIPERT G.,

- *Traité élémentaire de droit civil,* 1e éd., t. 1, LGDJ, 1939.

PORTALIS F. et PORTALIS J.-E.-M., *Discours et rapports sur le Code civil*, PUC, 06/2010.

REBOUL-MAUPIN N., *Droit des biens*, 5e éd., Dalloz, 2014.

ROCHFELD J., *Les grandes notions du droit privé*, PUF, 2011.

STIRN B., *Les libertés en question*, LGDJ, 8e éd., 2013.

TERRE F. et STIMLER H., *Droit civil, Les biens,* 10e éd., Dalloz, 2018.

ZENATI-CASTAING F. et **REVET Th.,**

- *Les biens*, 2e éd., refondue, PUF, 1997.
- *Les biens*, 3e éd., PUF, 2008.

Droit des contrats

LE TOURNEAU P., *Contrats informatiques et électroniques*, Dalloz référence, 9e éd., 2016.

Droit commercial

COHEN A., *Traité théorique et pratique des fonds de commerce,* vol. 1, rec. S., 1937.

b. Droit public

AUBY J.-B., BON P. et TERNEYRE P., *Droit administratif des biens*, Dalloz, Précis, 8e éd., 2020.

AUBY J.-B. et DUCOS-ADER R., *Droit de l'information*, Dalloz, 1982.

BRUGUIERE J.-M., *Les données publiques et le droit,* Paris, Litec, 2002.

CHEVALLIER J., *Le service public*, Que sais-je ?, 2018.

CORIOLAN S., *Responsabilité pénale des personnes publiques,* Rép. resp. puiss. Pub. D, 2020.

DUGUIT L., *Traité de droit constitutionnel* (t. 1 théorie générale de l'État), Fontemoing, 1911.

MOYSAN H., *Le droit de propriété des personnes publiques,* L.G.D.J, Bibl. de droit public, 2001.

TERESI L., *Droit de réutilisation et exploitation commerciale des données publiques,* Paris, La documentation française, CERIC, 2011.

c. Droit de la concurrence

DECOCQ A. et DECOCQ G., *Droit de la concurrence, droit interne et droit de l'Union européenne*, LGDJ, 7e éd., 2016.

MAINGUY D. et DEPINCE M., *Droit de la concurrence*, LexisNexis, 2e éd., 2015.

d. Droit des NTIC et des médias

BENGHOZI P.-J., BUREAU S., et MASSIT-FOLLEA F., *L'internet des objets, Quels enjeux pour l'Europe,* MSH, 2009.

BOURCIER D. et FILIPPI (De) P., ss. dir., *Open data & Big data, Nouveaux défis pour la vie privée*, mare & martin, 2016.

BOURGEOIS M., *Droit de la donnée, principes théoriques et approche pratique*, Lexis Nexis, 2017.

DOUVILLE T., *Droit des données à caractère personnel : Droit de l'Union européenne, droit français*, Gualino, 2020.

G'SELL F., ss. dir., *Le Big Data et le Droit*, Dalloz, 2020.

LEGEAIS D., *Blockchain et actifs numériques*, LexisNexis, 2e éd., 2019.

ROBIN A., *Droit des données de la recherche - Science ouverte, innovation, données publiques*, Larcier, 2022.

TERWANGNE (De) C. et ROSIER K., *Le règlement général sur la protection des données (RGPD/GDPR), analyse approfondie*, Larcier, 2018.

2. Dictionnaires & Lexiques

CABRILLAC R. et Alii., *Dictionnaire du vocabulaire juridique*, J.-Cl., 2002.

CORNU M., ORSI F. et ROCHFELD J., ss. dir., *Dictionnaire des biens communs*, PUF, 2017, 2e éd. mise à jour, 2021.

FERAL-SCHUHL C., *Cyberdroit, Le droit à l'épreuve de l'Internet*, Dalloz, 7e éd., 2018-2019.

GUILLIEN R. et VINCENT J., *Lexique des termes juridiques*, Dalloz, 16e éd., 2007.

CORNU G., *Vocabulaire juridique*, 12e éd., PUF, 2018.

CORNU M., ROCHFELD J. et ORSI F., ss. dir., *Dictionnaire des biens communs*, PUF, Quadrige, 08/2017.

B. OUVRAGES EN ECONOMIE/GESTION

ABIS S. et BRUN M., ss. dir., *Le Démeter 2021, Produire et se nourrir : le défi quotidien d'un monde déboussolé*, IRIS éd., févr. 2021.

ABITEBOUL S et PEUGEOT V., *Terra Data. Qu'allons-nous faire des données numériques ?*, Cité des sciences et de l'Industrie, éd. Le Pommier, 2017.

AIGRAIN P., *Cause commune. L'information entre bien commun et propriété*, Fayard, 2005.

BABINET G.,

- *L'ère numérique, Un nouvel âge de l'humanité,* Le passeur, 2014.
- *Transformation digitale : L'avènement des plateformes. Histoire de licornes, de data et de nouveaux barbares…,* Le passeur, 2016.

BASDEVANT A. et MIGNARD J.-P., L'*empire des données, Essai sur la société, les algorithmes et la loi,* éd. Don Quichotte, 03/2018.

BENABOU V.-L. et ROCHFELD J., *À qui profite le clic ?,* éd. Odile Jacob, 2015.

BENAVENT C., *Plateformes : sites collaboratifs, marketplaces, reseaux sociaux… Comment ils influencent nos choix*, FYP, 2016.

CHIGNARD S. et BENYAYER L.-D., *Datanomics, Les nouveaux business models des données*, FYP éd., 2015.

COLIN N. et VERDIER H., *L'âge de la multitude. Entreprendre et gouverner après la révolution numérique*, Armand Colin, 2012.

CORIAT B., *Le retour des communs, la crise de l'idéologie propriétaire*, LLL, 2015.

CORIAT B., BANCEL J.-L., ALIX N. et SULTAN F., coo., *Vers une république des biens communs ?*, LLL, 2018.

DARDOT P. et LAVAL C., Commun. *Essai sur la révolution au XXe siècle*, Paris, La Découverte, 2014.

DELORT P., *Le Big data, Que sais-je ?*, PUF, 2018.

KITCHIN R., *The Data revolution, Big Data, Open Data, Data infrastructures and their consequences*, Sage, 2014.

LEGEAIS D., *Blockchain et actifs numériques*, LexisNexis, 2e éd., 2019.

LEVY M. et JOUYET J.-P., *L'économie de l'immatériel, la croissance de demain*, La documentation française, 2007.

MOUVEMENT UTOPIA, *Propriété et communs, Idées reçues et propositions*, préf. de Coriat B., éd. Utopia, 2017.

RIFKIN J., *L'âge de l'accès, La nouvelle culture du capitalisme*, La découverte, Poche, 2005.

VEDEL G., préf. RANGEON, F., *L'idéologie de l'intérêt général*, Economica, 1986 (dernière version 1999).

SERONIE J.-M., *Vers un big bang agricole ? Révolution numérique en agriculture*, Nouvelles pratiques, autonomie et créativité, France agricole, 2016.

ZITTRAIN J., *The future of the Internet, And How to Stop It*, Yale University Press & Penguin, UK, 2008.

II. THESES ET MEMOIRES

AUBY J.-B., *La notion de personne publique en droit administratif*, dir. Ducos-Ader R., Bordeaux, 1979.

BIGOT-DESTREGUIL M., *Le bien information*, ss. dir. Loiseau G., Paris 1, 2017.

BLANCHET P.-A., *La valorisation du patrimoine immatériel des personnes publiques*, ss. dir., S. Braconnier, Paris, 2018, publié éd. L'Harmettan, 2020.

BRUGUIERE J.-M., *La diffusion de l'information publique. Le service public face au marché de l'information,* ss. dir. Vivant M., Montpellier, 1995.

CHAMARD-HEIM C., *La distinction des biens publics et des biens privés : contribution à la définition de la notion de biens publics*, préf. Intermaier J., Dalloz, Nouv. bibl. de thèses, t.33, 2004.

CLEMENT-FONTAINE M., *Les œuvres libres*, ss. dir. Vivant M., Montpellier, Montpellier, 2006

LELOUP J.-M., Le journal, les journalistes et le droit d'auteur, thèse, 1960.

MARCHAND J., *Recherche sur le régime des actions et participations financières publiques*, préf. Rapp L., LGDJ, Bibl. de droit public, t. 219, 2014.

MALLET-POUJOL N., *La commercialisation des banques de données, contribution à une approche juridique des richesses informationnelles*, dir. Lamberterie I. (de), CNRS éd., 1992.

ROBIN A., *La copropriété intellectuelle*. Préface de Thierry Revêt. Presses Universitaires d'Auvergne, 2005.

SCHMALTZ B., *Les personnes publiques propriétaires*, préf. Sestier J.-F., Dalloz, Nouv. Bibl. de Thèse, 2016.

TARLET F., *Les biens publics mobiliers*, thèse, Lyon 3, préf. Caudal S., Nouv. Bibl. de Thèse, vol. 170, Dalloz, 2017.

ZENATI F., *Essai sur la nature juridique de la propriété : contribution à la théorie du droit subjectif*, ss. dir. Rubellin-Devichi J., Lyon III, 1981.

III. CONFERENCES, COMMUNICATIONS & ACTES DE COLLOQUES

ABITEBOUL S., « Science des données. De la logique du premier ordre à la Toile », Leçon inaugurale à la chaire informatique et sciences numériques du Collège de France, prononcée le jeudi 8 mars 2012.

BEGUIN-FAYNEL C., « La problématique de l'appropriation des données agricoles », Droit rural, n°479, janv. 2020, colloque 2, n°9.

BELLON-MAUREL V., « Le numérique est dans le pré », On n'arrête pas l'éco, France Inter, 29 févr. 2020.

BERTIER-LESTRADE (De) B., « La bonne foi dans la réforme française des contrats », in Le Gallou C. et Marmisse-d'Abbadie d'Arrast A., ss. dir., Le contrat dans tous ses États, Presses de l'Université Toulouse 1 Capitole, pp. 141-160.

BINCTIN N., « Données et secret des affaires », Colloque – Circulation des données et propriétés intellectuelles, *PI*, avr. 2020.

DOUVILLE Th., ss. coord., « Dossier - Le droit des données agricoles », Université de Caen, 29 sept. 2017.

GALLOUX J.-C., « Libres propos sur le droit d'accès aux données », colloque, circulation des données et propriétés intellectuelles, PI, juill. 2020, n°76, pp. 11 à 19.

JUILLET-REGIS H., « Quelle régulation pour les données agricoles ? », *Droit rural*, n°479, janv. 2020, colloque 5.

LAMBERTERIE (De) I., « Les ressources informationnelles en jouissance partagée : quels modèles propriétaires ? », *in Les modèles propriétaires*, Actes du colloque international organisé par le CECOJI, PUJP,10 et 11 déc. 2009, pp. 75 à 86.

LEBRETON-DERRIEN S., ss. dir., « Dossier - Agriculture numérique et droit », *Droit rural* n°479, janv. 2020, coll. 1

LE GALLOU C. et MARMISSE-D'ABBADIE D'ARRAST A., ss. dir., Le contrat dans tous ses États, Presses de l'Université Toulouse 1 Capitole.

LESSIG L., « Code and the commons », Keynote, Conference on Media Convergence, Fordham Law School New York, NY, February 9, 1999.

MAZEAUD P., « Qui se soucie de l'intérêt général ? », Comm. à l'Académie des sciences morales et politiques, Canal académie audio, 7 févr. 2011.

ROBIN A., « Le statut juridique ambivalent du fichier : de l'appropriation de la compilation à la réservation de l'information », in Edazzi F. et Mauclair S., ss. dir., Le fichier, Actes du colloque organisé à la Faculté de Droit d'Orléans, 26 & 27 novembre 2015, LGDJ, 2016, pp. 215 à 233.

ROCHFELD J., « Contre l'hypothèse de la qualification des données personnelles comme des biens », *Les biens numériques*, CEPRISCA, pp. 221 et s.

TERESI L., *La commercialisation des données publiques*, Thèse, dir. Chérot, J.-Y.,Aix-Marseille, 2007.

VIVANT M.,

- « L'investissement rien que l'investissement. À propos des arrêts de la Cour de Justice des communautés du 9 novembre 2004 », *RLDI*, 2005/3, p. 41.
- « Les clauses de secrets. Les principales clauses conclues par les professionnels », Colloque de l'IDA, *PUAM*, 1991.
- « Données personnelles et propriété intellectuelle », *PI*, n°75, avr. 2020.

ZOLYNSKI C., « Le sens des normes *by design* », *Les objets connectés*, actes de colloque, 2018, pp. 131 à 143.

IV. Publications

- A -

AILINCAI M., « *La soft law est-elle l'avenir des droits fondamentaux ?* », dossier : Le droit des libertés en question(s) – Colloque des 5 ans de la RDLF, *RDLF*, 2017, chron.

ALLEAUME C.,

- « Les exceptions en faveur de l'enseignement et de la recherche scientifique, Commentaire des articles, 3 et 5 de la directive », *CCÉ*, n°10, oct. 2019.
- « Á propos de la propriété des données agricoles… », *Droit rural*, n°469, dossier 2, janv. 2009.

ALLEAUME C. et MARTIN D., « La directive 2019/790 sur le droit d'auteur dans le marché numérique », *RJC*, juill./août 2019, num. 4.

ANCIAUX A. et FARCHY J., « Données personnelles et droit de propriété : quatre chantiers et un enterrement », t. XXIX : *RIDE*, 2015/3.

ARTIGUELONG M. et GUIBERT D., « Directive européenne "Secret d'affaires": une menace pour les libertés ! », *Légipresse*, 2015.

AUBIN-BROUTE R.-J., « Le contrat pour la maîtrise des données agricoles », *Droit rural*, n°479, janv. 2020, colloque 3.

AUBY J.-B.,

- « La commercialisation des données publiques », *Rep., RFDA*, 2002.
- « La réutilisation des données publiques », *AJDA*, 2011.
- « L'immatériel dans l'État », repère 6, *AJDA*, juin 2007.

AZZI T., « open data et propriété intellectuelle », *D.*, n°11, 2017.

- B -

BECET J.-M., « Communication des documents des collectivités territoriales au public : Régime général », folio n°12210, *Dalloz*, 2019-1.

BELLON-MAUREL V., BOURNIGAL J.-M. et LENAIN R., « L'équation technologique et numérique en agriculture », *Le Démeter*, 2019.

BELLON-MAUREL V. et HUYGHE C.,

- « avant-propos », *Sciences Eaux & territoires*, 2019/3.
- « L'innovation technologique dans l'agriculture », *Géoéconomie 80*, mai/juin 2016

BELLON-MAUREL V., NEVEU P., TERMIER A. et GARCIA F., « Le *Big Data* en agriculture », *Enjeux numériques, n°2, Annales des Mines*, juin 2018.

BELORGEY J.-M., « L'État entre transparence et secret », Le Seuil, *Pouvoirs*, n°97, 2001/2, pp. 25 à 32.

BENABOU V.-L.,

- « Essai de prospective juridique sur les modes de valorisation des données : fonds informationnel, droit à la portabilité et dividende de la donnée », G'Sell F., ss. dir., *Le Big Data et le Droit*, Dalloz, 2020.
- « L'extension du domaine de la donnée », *Légicom*, n°59, 2017/2, pp. 3 à 17.
- « Une carte topographique est une base de données en raison de sa valeur informationnelle », obs. ss CJUE, 29 oct. 2015, aff. C490/14, *Freistaat Bayern c/Verlag Esterbauer GmbH* – Qualification de l'arrêt : important, *Dalloz IP/IT*, 2016, p. 89.

BENHAMOU F., « L'*Open Access*, domaine des communs éditoriaux. Du modèle encastré au modèle émancipé », in Sultan F., ss. dir., *Vers une République des biens communs, LLL*, 2018, pp. 143 à 153.

BENKLER Y., « Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain », 74 *New York University Law Review* 354, 1999.

BERNAULT C.,

- « Base de données : à défaut de propriété intellectuelle, le recours au contrat », L'Essentiel, *Droit de la propriété intellectuelle*, n°03, p. 3, 2015.
- « Revues scientifiques et droit d'auteur : la rupture de l'open access », Hermés, *La Revue*, vol. 71, n°1, 2015, pp. 92 à 99

BERTHAULT D., « La licence ODbL bloque la réutilisation des données publiques », *JCP A*, n°2240, 16 oct. 2017.

BERTRAND B.,

- « La volonté de réguler les activités numériques », *RTD Eur*., 2021.
- « Le modèle européen de partage des données », *Europe* n°2, févr. 2021, ét.1.
- « Perfectibilité de la protection des données personnelles », *RTD Eur*., 2021

BESSUGES-MEUSY R., « CMP : un passeur de consentement », *Expertises*, févr. 2021.

BINCTIN N., « Le statut juridique des informations non appropriées », *Légicom*, 2013/1, pp. 29 à 40.

BLAIZOT-HAZARD C., « Données publiques et patrimoine immatériel des personnes publiques », Colloque – Circulation des données et propriétés intellectuelles, *PI*, avr. 2020.

BOIZARD M., « La valorisation des données numériques par la protection juridique des algorithmes », *Dalloz IP/IT*, 2018.

BOUGEARD A., « Les dispositions relatives à l'accès et au portage des données : code de conduite et bonnes pratiques », *Dalloz IP/IT*, 2020, n°7 et 8.

BOUL M., « Réflexions sur la notion de donnée publique », *RFAP*, n°167, 2018/3, pp. 471 à 478.

BOURCIER D., « Réflexion éthique sur le partage des données en science : entre communs scientifiques et open data », in Bourcier D. et Filippi (De) P., ss. dir., *Open data & Big data, Nouveaux défis pour la vie privée*, mare & martin, 2016, pp. 211 à 243.

BOURCIER D. et FILIPPI (De) P., « Transparence des algorithmes face à l'open data : Quel statut pour les données d'apprentissage ? », *RFAP*, 2018, pp. 525 à 538.

BOURGEOIS M. et MOINE M., « Internet des objets (IOT) : quand l'inerte s'anime », *Rev. pratique de la prospective et de l'innovation* n°2, Oct. 2019, dossier 15.

BOUVET T., « Détermination du détenteur légitime des droits sur un secret d'affaires », *Rev. Prop. Ind.*, 2018

BOYLE J., « The Second Enclosure Movement and the Construction of the Public Domain », *Law and Contemporary Problems*, vol. 66, n°1 & 2, 2003.

BRUGUIERE J.-M.,

- « L'exploitation de l'image des biens », *Légicom*, 2005/2 (n°34), pp. 13 à 34.
- « Intelligence artificielle et droit d'auteur : Sortir de la science-fiction des "machines/auteurs", entrer dans la réalité du droit des données », *CCE* n°6, juin 2020, ét. 11.
- « Le droit à l'interopérabilité », *CCE* n°2, févr. 2007, ét. 3.
- « Le patrimoine immatériel de l'État est-il l'objet d'une propriété publique ? », *CDST*, 2010

- C –

CAQUE S., « Réflexions juridiques autour de l'articulation entre l'ouverture des données publiques et la protection des données personnelles », in Bourcier D. et Filippi (De) P., ss. dir., *Open Data & Big Data, Nouveaux défis pour la vie privée*, mare & martin, 2016, pp. 195 à 210.

CAMUS A., « La propriété des données publiques », *RFDA*, 2018/3, n°167, pp. 479 à 490.

CARON C., « République numérique rime avec exceptions et limitations en droit d'auteur, Commentaires », *CCE*, nov. 2016.

CARRE S., « Libre circulation des données, propriété et droit à l'information (1) : à propos du règlement (UE) 2018/1807 du 14 novembre 2018 », *Dalloz IP/IT*, 2020.

CARRE S. et MACREZ F., « Les ambivalences du copyright européen dans la construction du marché unique numérique », *Europe* n°7, ét. 6, juill. 2020.

CASSAR B., « La gouvernance des données », *IP/IT*, 2022.

CASTETS-RENARD C.,

- « Marché unique numérique : la Commission européenne présente les premières mesures en droit d'auteur », *D.*, 2016.
- « La liberté contractuelle et la réservation de l'information des bases de données non protégées devant la CJUE », *RLDI*, n°113, 1er mars 2015.

CASTETS-RENARD C., NDIOR V. et RASS-MASSON L., « Le marché unique numérique : Quelles réalités matérielles et conceptuelles ? », *D.*, n°956, 2019.

CASTETS-RENARD C. et MARTY F., « Facilités essentielles (approche économique et juridique) », in Cornu M., Orsi F. et Rochfeld J., ss. dir., *Dictionnaire des biens communs,* PUF, Quadrige, 08/2017, p. 541.

CASTETS-RENARD C. et GANDON N., « Open Data des données de la recherche publique : entre réformes législatives et retour d'expérience sur un guide pratique à destination des chercheurs », *Légicom,* 2016.

CATALA P.,

- « La propriété de l'information », in Marty, G., ss. dir., *Mélanges offerts à P. Raynaud,* Paris, D.S., 1985.
- « Ébauche d'une théorie juridique de l'information », *RDD,* 1983.
- « La transformation du patrimoine dans le droit civil moderne », *RTD civ.*, n°185, 1966.

CHEVALLIER J.,

- « Essai sur la notion juridique de service public », *Publications de la faculté de droit d'Amiens*, n°7, 1976, pp. 136-161.
- « La place de l'établissement public en droit administratif français », *Publications de la faculté de droit d'Amiens*, 2011, pp. 5-76.
- « Vers l'État-plateforme ? », *RFAP*, n°167, 2018/3, pp. 627 à 637.
- « Le droit français et la question des données publiques », in Bourcier D. et Filippi (De) P., ss. dir., *Open data & Big data*, mare & martin, 2016, pp. 29 à 40.
- « Transformation numérique. Les nouveaux développements de l'État plateforme », *JCP G*, n°19, 11 nov. 2020, doctr. 611.
- « La régulation juridique en question », *Droit et société*, 2001/3.

CHERON A., « La réutilisation des données publiques : Bases de données et open data (1) », *AJCT*, 2011.

CHONE-GRIMALDI S., « Données agricoles et droit de la concurrence », *Droit rural* n°469, janv. 2019, dossier 3.

CLEMENT-FONTAINE M.,

- « De l'exclusion des idées (Propriété intellectuelle. Principes généraux) », in Vivant M., ss. dir., *GAPI*, préf. Ph. Jestaz, Dalloz, 2015.
- « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *Légicom*, 2017/2.
- « La plasticité de la notion de responsable de traitement », *Rev. Aff. Eur.*, 2018/1, pp. 35 à 42.
- « Communs numériques (approche juridique) », in Cornu M., Orsi F. et Rochfeld J., ss. dir., *Dictionnaire des biens communs,* PUF, Quadrige, 08/2017, pp. 311 à 314.

CLUZEL-METAYER L.,

- « Les limites de l'open data », *AJDA*, 2016.
- « La loi pour une république numérique : l'écosystème de la donnée saisi par le droit », *AJDA*, 2017.
- « La construction d'un service public de la donnée », *RFAP*, n°167, 2018/3, pp. 491 à 500.
- « L'ouverture des données publiques », in AFDA, ss. dir., *Le droit administratif au défi du numérique*, Dalloz, 2019.

CLUZEL METAYER L. et DEBAETS E., « Le droit de la protection des données personnelles, la loi du 20 juin 2018 », *RFDA*, 2018.

CORIAT B.,

- « Communs (approche économique) », in Cornu, M., Orsi, F. et Rochfeld, J., ss. dir., *Dictionnaire des biens communs*, PUF, 08/2017, pp. 299 à 322.
- « *Communs informationnels* », in Cornu, M., Orsi, F. et Rochfeld, J., ss. dir., *Dictionnaire des biens communs*, PUF, 08/2017, pp. 308 à 311.

COSTA D., « Mission de service public assurée par une personne privée : clarification ou codification ? », *AJDA*, 2007.

CRETOIS P., « La propriété repensée par l'accès », *RIDE*, 2014/3 t. XXVIII, pp. 319 à 334.

CRETOIS P. et ROZA S., « De l'intérêt général : introduction », Astérion, 17/2017.

CYTERMANN L., « Le partage des données, un enjeu d'intérêt général à l'ère de l'intelligence artificielle », *Rev. Aff. eur.*, 2018/1, pp. 65 à 72.

- D -

DANDERN B. et HAUSSMANN C., « Les *Data Rooms* : une pratique vue sous un angle théorique », *Droit et patrimoine*, n°175, 2018.

DARAGON E., « Étude sur le statut juridique de l'information », *D.*, 1998. Chron.

DAVID BEAUREGARD-BERTHIER (De) O., « Le patrimoine immatériel de l'État », *Bien public, Bien commun, Mélanges en l'honneur d'Etienne Fatôme*, Dalloz, 2011.

DELAUNAY B., « Nouvelles limitations à l'accès aux documents administratifs », *AJDA*, 2013.

DEMOLOMBE C., « Traité de la distinction des personnes et des biens », in Demolombe, C., *Cours de Code Napoléon*, t. IX, Paris, Durand, 1870.

DERCLAYE E., « Le marché européen des données. La directive des Bases de données est-elle toujours adaptée à l'ère de l'internet des objets ? », *PI*, juill. 2020, n°76, pp. 20 à 32.

DESBOIS H., « Le droit d'auteur en France », *RIDC*, vol. 31, n°2, 1978.

DESTREGUIL M., « Plaidoyer en faveur d'une approche propriétariste des données personnelles », *RJPF*, n°3, 1er mars 2019.

DOUTRELEPONT C., « Le nouveau droit exclusif du producteur de bases de données consacré par la directive européenne 96/9/C du 11 mars 1996 », *Mél. M. WAELBROECK, Bruylant*, 1999, pp. 903 à 920.

DOUVILLE T.,

- « Contrat et données agricoles », *Droit rural* n°469, janv. 2019, dossier 4.
- « Consentement à un traitement de données à caractère personnel et contrat : nouveaux apports de la Cour de justice », obs. ss. CJUE, 11 nov. 2020, aff. C-61/19, *Dalloz IP/IT*, 2021, p. 290

DREYFUS J.-D., « La valorisation par l'État de son patrimoine immatériel », *AJDA*, 2009, n°696.

- E -

EDELMAN B., « Les bases de données ou le triomphe des droits voisins », *D.*, 2000.

EPSTEIN A.-S., « La compatibilité du droit d'accès aux informations environnementales de source privée avec la protection du secret des affaires : Prélude à la consécration d'un droit d'accès aux données d'intérêt général de source privée », *RJE*, 2020/HS20 n° Spécial, pp. 137-149.

- F -

FAVRO K. et ZOLYNSKI C., « DSA, DMA : l'Europe encore au milieu du gué », *Dalloz IP/IT*, 2021.

FERRARI P., « Les droits des citoyens dans leurs relations entre les administrations, Commentaire générale de la loi n°2000-321 du 12 avril 2000 », *AJDA*, 2000.

FILIPPI (De) P. et DULONG DE ROSNAY M., « Le piratage informatique, un explorateur des courants juridiques du réseau », *Revue de Sciences humaines* Tracés, n°26, 2014.

FORT F.-X. et ROBIN A., « Remarques sur le régime de gestion de la propriété industrielle entre personnes publiques », *AJDA*, 2010.

FOUCART T., « La définition contestable de l'intérêt général par le Conseil d'État », art. Iref-Europe, Contrepoints, 10 oct. 2018.

FRISON-ROCHE M.-A., « Le droit de la régulation », *D.*, 2001, chron.

- G -

GALLOIS J., « La clause de confidentialité (ou de secret) », *CCC*, n°5, mai 2021, dossier n°12.

GALLOUX J.-C.,

- « Ébauche d'une définition juridique de l'information », *D.*,1994. Chron.
- « Droit sur les créations nouvelles », *RTD com.*, 2014.
- « La directive sur le secret des affaires », *RTD com.*, 2017.

GARINOT J.-M., « Secret des affaires : la loi ne chasse pas le contrat », *AJCA*, 2018.

GASSIN R., « La protection pénale d'une nouvelle "Universalité de fait" en droit français : Les systèmes de traitement automatisé de données », *ALD*, 1989, pp. 13 à 28, *in* Vivant M. et al, ss. dir., *Lamy droit du numérique*, 2019.

GOUNIN Y., « La réforme du droit d'accès aux documents administratifs », AJDA, 2000.

GUGLIELMI G., « *Open Data* et service public : les données publiques ouvertes sont-elles un service public ? », in Bourcier D. et Filippi (De) P., ss. dir., *Open Data* & *Big Data, Nouveaux défis pour la vie privée*, mare & martin, 2016, pp. 41 à 55.

GUICHARDAZ R. et PENIN J., « L'économie de la réutilisation des données (non personnelles) », Dalloz *IP/IT*, 2020.

GRUGER H., SOULIEZ M. et LEBRETON-DERRIEN S., « Pour une utilisation négociée et éthique des données agricoles : l'exemple de la Charte Data-agri », *Droit rural* n°479, janv. 2020, coll. 4.

- H -

HARDIN G., « The tragedy of commons », *Science*, 13 déc. 1968.

HARTMANN P. et alii, « Big data for big business? A taxonomy of Data-driven Business Models used by start-up firms », Working paper, *University of Cambrigde*, mars 2014.

HATZOPOULOS V., « Vers un cadre de la régulation des plateformes ? » *RIDE*, 2019/3.

HUGENHOLTZ, B., « Against "Data Property" », in Ullrich H., Drahos P. & Ghidini G. (Eds.), *Kritika : Essa*ys on Intellectual Property (Vol. 3, pp. 48-71), Elgar, 2018.

HULIN A.-S., « Introduction à la fiducie québecoise de données », *Laboratoire de cyberjustice*, blog, nov. 2019.

- J –

JOLY P.-B., « Recherches scientifiques et recherches industrielles »**,** *in Construire la recherche avec la société civile : les enjeux de la démarche d'intermédiation*, Cahiers de l'action n°55, juill. 2020.

- L -

LALLET A. et NGUYEN DUY P.,

- « Communication des documents administratifs », *Rép. cont. adm.*, n°231, juin 2019.
- « Diffusion et réutilisation des informations publiques : « Open Data » - données ouvertes », *Rép. IP/IT et comm*., Dalloz, sept. 2020.

LANNA M., « Données publiques et protection des données personnelles : Le cadre européen », ENA, *RFAP*, n°167, 2018/3, pp. 501 à 511.

LAPOUSTERLE J., « La directive (UE) 2016/943, du 8 juin 2016 sur la protection des secrets d'affaires : apports et perspectives de transposition », *Dalloz IP/IT*, n°493, 2016.

LASSERRE CAPDEVILLE J., « Nouvelle solution favorable au vol d'informations », obs. Cass. crim., 28 juin 2017, n°16-81.113, *AJ Pénal*, 2017, p. 448.

LATREILLE A.,

- « La fouille de textes et de données à l'épreuve de la propriété intellectuelle », *CDST*, 2017.
- « L'appropriation des photographies d'œuvres d'art », *D.*, p. 299, 2002.

LE CROSNIER H., « Communs de la connaissance », *in* CORNU, M., ORSI, F. et ROCHFELD, J., ss. dir., *Dictionnaire des biens communs*, PUF, 08/2017, pp. 302 à 305.

LEDGER M. et TOMBAL T., « Le droit à la portabilité dans les textes européens ; droits distincts ou mécanisme multi-facettes ? », *RDTI*, n°72, 2018, pp. 25 à 44.

LEGEAIS D., « Bienvenue aux actifs numériques », *RJC*, mars/avr. 2020.

LEONETTI R., « La protection de l'affectation au service public des biens incorporels », *AJDA*, 2009.

LESAULNIER F., « La définition des données à caractère personnel dans le règlement général relatif à la protection des données personnelles », *Dalloz IP/IT*, 2016/12**.**

LE STANC C., « Secret d'affaires – Chut ! », *Propr. industr*., n°6, juin 2016, repère 6.

LAMBERTYE-AUTRAND (De) M.-C., « Nature des biens », *eEssentiel*, 2017.

LENOIR N., « Le droit de la concurrence confrontée à l'économie du *Big Data* », *AJCA*, févr. 2016.

LIBCHABER R., « Le portefeuille de valeurs mobilières : bien unique ou pluralité de biens ? », *Defrénois*, 1997.

LOMBARD M., « La régulation par la donnée », in AFDA, ss. dir., *Le droit administratif au défi du numérique,* Dalloz, 2019.

LUCAS A. et SIRINELLI P., « L'originalité en droit d'auteur », *JCP*, 1993. I. 3681.

LUCAS DE LEYSSAC M.-P., « L'arrêt Bourquin, une double révolution : un vol d'information seule, une soustraction permettant d'appréhender des reproductions qui ne constitueraient pas des contrefaçons », *RSC*, n°3, juill. - sept. 1990, pp. 507 à 520.

- M -

MACREZ F. et DUFLOT F., « L'interopérabilité, principe incontournable des libertés numériques », *PI*, oct. 2017, n°65.

MAISL H.,

- « La diffusion des données publiques ou le service public face au marché de l'information », *AJDA*, 1994.
- « Régime de la protection juridique des bases de données publiques », *AJDA*, 1997.

MAISON-ROUGE (De) O.,

- « La donnée : Enjeu cardinal de la cybersécurité. Définition, nature, classification et extraction », *Dalloz IP/IT*, 2018.
- « Le secret des affaires : Une protection juridique des données stratégiques », sur le site de Village de la justice, 2 août 2018.

MALAURIE-VIGNAL M., HEINTZ D. et LECOLE M., « Comment appréhender les abus et l'utilisation des données dans la relation d'une plateforme avec ses partenaires contractuels ? » *CCC*, n°12, déc. 2020.

MALLET-POUJOL N.,

- « La directive concernant la protection juridique des bases de données : la gageure de la protection privative », *DIT*, 1, 1996
- « Appropriation de l'information : l'éternelle chimère », *D.*, 1997.
- « La protection des bases de données : un péage pour l'accès aux informations génétiques ? », *RLDI*, 2013.
- « Biens informationnels (approche juridique) », in Cornu M., Orsi F. et Rochfeld J., ss. dir., *Dictionnaire des biens communs*, PUF, Quadrige, 08/2017, pp. 126 et s.

- « Protection des données personnelles et droit à l'information », *Légicom*, n°59, 2017/2, pp. 49 à 59.

MALWE C., « La valorisation du patrimoine immatériel de l'État », *AJDA*, n°4, avr. 2009.

MANCOSU G., « La transparence publique par l'ouverture des données personnelles ? Focus sur les systèmes juridiques italien et français », in Bourcier D. et Filippi (De) P., ss. dir., *Open data & Big data, Nouveaux défis pour la vie privée*, mare & martin, 2016.

MARQUET V., « Directive Secret des affaires : quand la liberté d'expression devient une exception, ou une vision européenne de la transparence », *Légipresse*, 2016.

MARTIAL-BRAZ N., « Les nouveaux droits des personnes concernées », Rev. *Aff. Eur*., 2018-1, pp. 7 à 17.

MARTIN N. et LE GAL C., « Droit des bases de données et parasitisme : un arrêt en demi-teinte de la cour d'appel de Paris », *RDLI*, 2006.

MARTINEZ R. et MARX B., « La longue marche de l'information publique, de la liberté d'accès aux documents administratifs à la réutilisation commerciale des informations publiques », *Documentaliste-Sciences de l'Information*, 2007/3, (Vol.44), pp. 218 à 217.

MARTY F., « Accès aux données, coopétition intra-plateforme et concurrence inter-plateformes numériques », *Revue d'économie industrielle*, 2020/1, n°169, pp. 221 à 246.

MATTATIA F. et YAICHE M., « Être propriétaire de ses données personnelles (1ère partie) : peut-on recourir aux régimes traditionnels de propriété ? », *RLDI*, 2015/114.

MERLAND G., « L'intérêt général dans la jurisprudence du Conseil constitutionnel », *LGDJ*, 2004, p. 2.

MICHAUX B.,

- « L'originalité en droit d'auteur, une notion davantage communautaire après l'arrêt Infopaq », *Auteurs & Média*, 5/2009, pp. 473 à 488.
- « La cour de justice favorise-t-elle l'appropriation des données par celui qui les a traitées ? », note ss CJUE, 2e ch., aff. n° C-490/14, 29 oct. 2015, *Auteurs & Media*, n°1, pp. 28 à 34.

MILCHIOR R. et FOURGOUX V., « Directive sur les secrets d'affaires : création d'un nouveau droit de propriété intellectuelle », *AJCA*, n°391, 2016.

MOUCHETTE J., « Haro sur les obligations de localisation des données non personnelles », *Dalloz IP/IT*, 2020.

MOURIER R., « *Open Data vs* droit de propriété intellectuelle », comm., ss. CE, 8 févr. 2017, nº 389806, Sté NotreFamille.com, Rec. CE, 27 février 2017, Actualité du droit, Lamy.

MOUSSERON J.-M. et VIVANT M., « Les mécanismes de réservation et leur dialectique : le "terrain" occupé par le droit », *JCP E*, n°11, 1988-1.

MORALES M., « La réutilisation des données publiques : le cas particulier de la culture », *RFDA*, 2018.

MULLER E., « La libre circulation des données et la directive concernant la réutilisation des données du secteur public », *Dalloz IP/IT*, 2020.

- N -

NETTER E.,

- « La portabilité, un droit à inventer », *Dalloz IP/IT*, n°352, 2020, 20 juin 2020.
- « À quoi sert le principe de transparence en droit des données personnelles ? », *Dalloz IP/IT*, n°611, 2020.

NOUCHER M. et GAUTREAU P., « Le libre accès rebat-il les cartes ? Nouvelles perspectives pour les données géographiques », *LCN*, 2013/1, Vol. 9, pp. 57 à 83.

- O -

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 », *RFDA*, n°6, 2015, p. 1157.

- P -

PADOVA Y., « Entre patrimonialité et injonction au partage la donnée écartelée (Partie I et II) », *RLDI*, n°155, 2019.

PASSA J.,

- « La limitation par contrat de l'exploitation d'un objet non protégé par un droit de propriété intellectuelle », *RDC*, n°02, 2015.
- « L'opposition en droit de la propriété intellectuelle », *LPA*, n°68, 2007.
- « La propriété de l'information : un malentendu ? », Communication au colloque « Renouveau du droit de propriété ? » organisé par l'Université Lyon 2 en octobre 2000, *Droit et patrimoine*, n°91, mars 2001, pp. 64 à 72.

PELLIGRINI F., « La portabilité des données et des services », *RFAP*, n°167, 2018/3, pp. 513-523.

PERINET-MARQUET H., « Regard sur les nouveaux biens », *JCP G*, n°44, 2010.

PERRAY R., « La loi "pour une république numérique" », *RLDI*, n°144, 1er janv. 2018.

PERRAY, R. et UZAN-NAULIN, J., « Existe-t-il encore des données non personnelles ? », *Dalloz IP/IT*, 2017.

PICARDAT S., « GAÏA-X : L'agriculture au cœur de la souveraineté numérique européenne », Abis, S. et Brun, M., ss. dir., *Le Démeter 2021, Produire et se nourrir : le défi quotidien d'un monde déboussolé*, IRIS éd., févr. 2021

PIGNATARI O. et COUSIN A., « L'originalité des logiciels », *Dalloz IP/IT* n°248, 2016.

PILCZER J.-S., « La notion de service public », *Informations sociales*, n°158, 2010/2, pp. 6 à 9.

PILLET G., « L'efficacité du droit français des contrats face aux géants de l'internet », *RTD com.*, 2018.

PISAN M., « IGN : la gratuité des données en question », *Expertises*, mai 2019.

PLANTIN J.-C. et VALENTIN J., « Données ouvertes et cartographie libre, autour du cas de Montpellier », *LCN*, 2013/1, vol. 9, pp. 85 à 107.

POLLAUD-DULIAN F., « Idées. Méthode intellectuelle. Choix arbitraires mais pas créatifs », *RTD Com*., 2006.

PUCHERAL P., RALLE A., ROCHELANDET F. et ZOLYNSKI C., « Le *Privacy by design* : une fausse bonne solution aux problèmes de protection des données personnelles soulevés par *l'Open Data* et les objets connectés », *Légicom*, 2016, p. 89.

PUËLL P., « Secret des affaires : Une mise en conformité nécessaire », *Expertises*, nov. 2020.

- R -

REY P., « L'approche économique des marchés "biface" », *RLC*, n°35, 1er avr. 2013.

ROBIN A.,

- « 3 questions — Gouvernance des données : l'ambition européenne de l'espace unique numérique », *JCP E*, n°8-09, 24 févr. 2022.
- Définition de 4 verbi (« valorisation », « open access », « open science », « communs scientifiques »), *Dictionnaire des biens communs*, ss. dir., Cornu M., Rochfeld J. et Orsi F., PUF, Quadrige, 08/2017.
- « Secret d'affaires et liberté d'expression : l'exercice d'équilibrisme de la directive », *RLDC*, 2016.
- « Les données scientifiques au prisme du dispositif *Open Data* » *CCE*, 2017, n°9, ét. 14, pp. 7 à 14.
- « Valorisation de la recherche scientifique, propriété intellectuelle, innovation », chr., *CDST*, 7/2017.
- « Agriculture numérique, données et droit : topographie juridique de l'"écosystème informationnel vert », *Sciences Eaux & Territoires*, 2019, pp. 38 à 41.
- « L'ouverture des données publiques scientifiques, de l'examen de la règle "*Open as possible, closed as necessary*" », *CCE*, n°9, sept. 2020, ét. 15.
- « Exploitation de l'innovation », *CDST*, 12/2021.

ROCHET J.-C. et TIROLE J.,

- « Two sided markets : An overview », *The Economics of Two-Sided Markets* 12 mars 2004.
- « Platform Competition in Two-sided Markets », *JEEA*, vol. 1, n°4, June 2003.

ROCHFELD J.,

- « Chose commune (approche juridique) », Cornu M., Orsi F. et Rochfeld J., ss. dir., *Dictionnaire des biens communs*, PUF, Quadrige, 08/2017, p. 184.
- « Entre propriété et accès : La résurgence du commun », in Bellivier F., ss. dir., *La Bioéquité*, Autrement, Frontières, 2009, pp. 69 à 87.
- « Penser autrement la propriété : la propriété s'oppose-t-elle aux "communs" ? », *RIDE*, 2014/3 (t. XXVIII), pp. 351 à 369.

ROUX C., « La propriété publique à l'épreuve des données publiques », in AFDA, ss. dir, *Le droit administratif au défi du numérique*, D.S., 2019, pp. 43 à 64.

ROZENFELD S., « Données personnelles : Un pas vers la monétisation des données », *Expertises*, nov. 2020.

- S -

SAINT-ARNAUD P., « L'informatisation de l'agriculture ouvre la porte à la cybercriminalité », *La Presse Canadienne*, L'actualité, 25 avr. 2021.

SAINT AUBIN T., « Les nouveaux enjeux juridiques des données (big data, web sémantique et linked data) Les droits de l'opérateur de données sur son patrimoine numérique informationnel », *RLDI*, 2015.

SCHULER M. et ZNATY B., « Quelle protection juridique pour l'algorithme ? », *in* INPI, *La propriété intellectuelle et la transformation numérique de l'économie*, 2015.

SINE M., HAEZEBROUCK T.-P. et EMONET E., « API-AGRO, Création d'une plateforme d'échange de données agricoles fédératrices d'acteurs publics et privés », *Innovations Agronomiques* n°71, 2019.

STASIAK F., « L'affaire K. vue avec un peu de recul », *RLDA*, n°97, 2014.

STORRER O., « Pour un droit commercial de l'exploitation des données à caractère personnel », *D.*, 2013.

- T -

TABAKA B., « De l'accès à la réutilisation : le nouveau régime applicable aux données publiques », *RLDI*, 2005.

TERESI L.,

- « L'open data et le droit de l'Union européenne (1) », *AJDA*, 2016.
- « Observations sur la directive n°2013/37/UE du 26 juin 2013 sur la réutilisation de l'information du secteur public », *JCP A*, n°7, 2039, n°21, 2014.

TERNEYRE P., « Les actifs immatériels des personnes publics », *RJEP*, ét. 16, 2013.

TESTU F.-X., « Responsabilité civile et propriété des idées en matière de brevets et de savoir-faire », *RCA*, n°5, mai 2017. Dossier 8.

TIMSIT G., « Les deux corps du droit : essai sur la notion de régulation », *RFAP*, 78, 1993.

TINIERE R., « L'apport de la Charte des droits fondamentaux à la protection des données personnelles dans l'Union européenne », *Rev. Aff. Eur.*, 2018/1.

TOMASSO L., LAUGA B. et PINET F., « Chaîne de confiance : des données partagées en transparence et en sécurité », *Perspective agricole*, 1er juin 2021, [en ligne].

TROUESSIN G., « Données de santé : anonymat et risque de ré-identification », Dossiers Solidarité et santé, n°64, juill. 2015, p. 96 [En ligne].

TRUCHET D., « Nouvelles récentes d'un illustre vieillard : Label de service public et statut de service public » *AJDA*, 1982.

- V –

VERDIER H. et MURCIANO C., « Les communs numériques, socle d'une nouvelle économie politique », *Esprit*, 2017/5 (mai), pp. 132 à 145.

VIANGALLI F., « Des données à la responsabilité : de l'anonymisation à l'attaque par ré-identification », *RLDI*, n°173, 1e août 2020.

VINGIANO-VIRICEL I., « Les obligations précontractuelles d'information lors de la vente d'un objet connecté [contrat de vente] », ét. 6, *CCC*, déc. 2019.

VIVANT M.,

- « An 2000 : l'information appropriée ? », *Mélanges offerts Jean-Jacques Burst*, Litec, 1997.
- « La privatisation de l'information par la propriété intellectuelle », *RIDE*, 2006/4 (t.XX, 4), pp. 361 à 388.
- « L'investissement, rien que l'investissement », *RLDI*, 2005/3.
- « Touche pas à mon filtre ! Droit de marque et liberté de création : de l'absolu et du relatif dans les droits de propriété intellectuelle », *JCP E.*, 1993, I.
- « À la recherche de la condition d'originalité », *GAPI*, Dalloz, 2e éd., 2020, comm. 44 à 46, p. 274 et s.
- « Données personnelles et propriété intellectuelle », *PI*, n°75, avr. 2020, pp. 58 à 67.
- « Le droit sui generis du producteur d'une base de données ne peut s'opposer à la réutilisation des données publiques », *RLDI*, n°137, 1e mai 2017

- W -

WAGNER M., « Le droit pénal spécial et les fonctions publiques : une illustration des affres de la pénalisation à outrance », *RSC*, 2011/1 (n°1), pp. 37 à 57.

WARUSFEL B., « La protection des bases de données en question : un autre débat sur la propriété intellectuelle européenne », *PI*, n°13, 2004.

WILKINSON M. D., DUMONTIER, M., AALBERSBERG IJ. J., APPLETON G., AXTON M., BAAK A., MONS B., "The FAIR Guiding Principles for scientific data management and stewardship". *Scientific Data* n°3, 2016. https://doi.org/10.1038/sdata.2016.18.

- X -

XIFARAS M., « Le copyleft et la théorie de la propriété », Association Multitudes, *Multitudes*, 2010/2, n°41, pp. 50 à 64.

- Y -

YOLKA P.,

- « Les meubles de l'administration », *AJDA*, 2007.

- « Les patrimoines publics à l'épreuve de la propriété intellectuelle », *AJDA*, prat. 1, 2012.
- « Open data : l'ouverture c'est l'aventure », *AJDA*, 2016.
- « Le droit de l'immatériel public », *AJDA*, 2017.

- Z -

ZOLYNSKI C.,

- « Un nouveau droit de propriété intellectuelle pour valoriser les données : le miroir aux alouettes ? », *Dalloz IP/IT*, 2018.
- « Quelle circulation des données non personnelles pour l'Union européenne ? », *Rev. Aff. Eur.*, 2018/1, pp. 73 à 78.
- « La loyauté des plateformes pensée par la loi pour une République numérique », *in* Chatry, S., et Gobert, T., ss. dir., *Numérique : Nouveaux droits, nouveaux usage*s, Mare & Martin, 2017, pp. 125 à 126.

ZOLYNSKI C. et LE ROY M., « La portabilité des données personnelles et non personnelles, ou comment penser une stratégie européenne de la donnée », *Légicom*, n°59, 2017/2, pp. 105 à 113.

V. FASCICULES, GUIDES & REPERTOIRES

AUBY J.-B., « Données publiques – Définitions. Principes. Orientation », fasc. 109-30, *JCP A.* 2018.

BERTRAND A., *Droit d'auteur*, *Dalloz action*, 2010.

CASEAU-ROCHE C., « La clause de confidentialité », *AJCA*, 2014.

CHATRY S., « Droit des producteurs de bases de données », *J.-Cl. Propr. litt. et art.,* fasc 1650, 2018.

COSTES L.,

- « Précisions de la CJCE sur la signification de l'investissement », *Le Lamy Droit du numérique* (Guide), 3354, 2019.
- « Intérêt et objet de cette protection », *Le Lamy Droit du numérique* (Guide), 3352, 2019.

LEPAGE A., « Un an de droit pénal des nouvelles technologies (oct. 2012 – oct. 2013) », *Dr. Pén.* 2013, chron. 11.

LIBCHABER R., « Répertoire de droit civil », *RTD Civ.*, 2016.

LUCAS A., « Propriété littéraire et artistique », fasc. 1650 : Droits des producteurs des bases de données (CPI, art. L.112-3 L.341-1 à L.343-7), *J-Cl Civil* Annexes, 3 nov. 2010, mis à jour 1er févr. 2018

MALLET-POUJOL N., « Droit des bases de données », J.-*Cl. Communication*, Fasc.

ROBACZEWSKI C., « Atteinte aux systèmes de traitement automatisé de données », J-*Cl. Pénal*, 19 févr. 2010.

ROBIN A.,

- « Les places de marché en ligne. Définitions et distinctions », *J-Cl com.*, fasc. 827, oct. 2019.
- « Les places de marché en ligne. Responsabilité », *J.Cl com.*, fasc. 827, oct. 2019.

VI. RAPPORTS, ETUDES & ENQUETES

ACTA, *L'accès aux données pour la recherche et l'innovation en agriculture*, Position des Instituts techniques agricoles, oct. 2016.

AILINCAI M., *Revue des droits et libertés fondamentaux - RDLF*, Centre de Recherches Juridiques de Grenoble, 2017, Le droit des libertés en question(s) - Colloque des 5 ans de la RDLF, RDLF 2017, pp.chron. n°20.

AN,

- *Les plateformes numériques, Rapport d'information n°3127,* 24 juin 2020.
- *Rapport n°3185, relatif au droit d'auteur et aux droits voisins dans la société de l'information*, 22 juin 2006.

APIE, *Le patrimoine immatériel public : une ressource pour moderniser et créer de la valeur, rapport d'activité*, 2018.

ARCEP, *Pour un numérique soutenable*, rapport d'étape, 15 déc. 2020.

AUT. CONC. ET BUNDESKARTELLAMT, *Droit de la concurrence et données*, Avis, 10 mai 2016.

AUT. CONC., *Rapport annuel 2012*, 20 mars 2013.

BOTHOREL E., Mission confiée par le Premier ministre, *Pour une politique publique de la donnée*, Rapport Bothorel, déc. 2020.

BOUCHOUX C., *Rapport d'information au nom de la mission commune d'information sur l'accès aux documents administratifs et aux données publiques*, Sénat, n°589, 5 juin 2014 (2 t.).

BOURNIGAL J.-M., HOULLIER F., LECOUVEY P. et PRINGUET P., *30 projets pour une agriculture compétitive et respectueuse de l'environnement*, #AgricultureInnovation2025, Propositions, oct. 2015.

CAPO-CANELLAS V., *Météo-France*, Rapport d'information n°840 fait au nom de la commission des finances, 22 sept. 2021.

CAPPELLO M. (Ed.), *Au*torégulation et corégulation dans la nouvelle directive SMAV, IRIS Spécial, Observatoire européen de l'audiovisuel, Strasbourg, 2019.

CCI, *Industrie du futur, Pratiques et attentes des entreprises françaises en matière de partage des données industrielles*, oct. 2021.

CDC, *Les données du ministère de l'agriculture et de l'alimentation : un potentiel à mieux explorer*, 2020.

CE,

- *Rapport public annuel*, 1995.
- *Réflexions sur l'intérêt général, Rapport public 1999*, EDCE n°50, La documentation française, 30 nov. 1998.

- Numérique et droits fondamentaux, Rapport pour l'année 2014.
- *Puissance publique et plateformes numériques : accompagner l'"ubérisation",* EDCE, 29 sept. 2017.

CECOJI, *Les modèles propriétaires,* Actes du colloque international**,** PUJP, 10 et 11 déc. 2009.

CNIL,

- *Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles*, 34e rapport d'activité, La documentation française, 2013.
- *Blockchain et RGPD : Quelles solutions pour un usage responsable en présence de données personnelles ?,* 24 sept. 2018, [en ligne].
- *Mort numérique ou éternité virtuelle : que deviennent vos données après la mort ?*, 31 oct. 2014.

CNNum,

- *Ambition numérique, Pour une politique française et européenne de la transition numérique,* Rapport remis au premier ministre, juin 2015.
- *La levée des obligations de localisation des données,* fiche, juill. 2017.
- *La libre circulation des données dans l'Union européenne*, avis, avr. 2017.
- *Synthèse de la consultation sur la régulation des contenus illicites, États généraux des nouvelles régulations numériques,* mai 2020.
- *La consécration d'un droit à la portabilité des données non personnelles*.

COMMISSION EUROPEENNE, *Consultation publique sur l'environnement réglementaire concernant les plateformes, les intermédiaires en ligne, les données et l'informatique en nuage, ainsi que l'économie collaborative*, 15 déc. 2015.

COLLIN P. et COLIN N., *Mission d'expertise sur la fiscalité de l'économie numérique*, Rapport, janv. 2013.

CSPLA,

- *Rapport de la mission sur la réforme européenne du droit sui generis des bases de données*, juill. 2022.
- *Mission sur la réforme européenne du droit des bases de données*, Note d'étape, avr. 2021.
- *Droit de la propriété littéraire et artistique, données et contenus numériques,* Rapport, sept. 2018.
- *Mission sur l'interopérabilité des services numériques,* Rapport établi par MOCHON, J.-P. et PETITDEMANGE, E., avr. 2017.

CYBERLEX et CECYE, *Code pénal et lutte contre la cybercriminalité : Proposition pour une efficacité juridique renforcée,* Rapport, 25 janv. 2017.

CYTERMANN L., Maître des requêtes au CE, *Rapport relatif aux données d'intérêt général*, Rapport d'étape CE / CGE / IGF, 2015.

DEDIEU L., *Rédiger et publier un Data paper dans une revue scientifique en 5 points*, Montpellier : CIRAD, 2014.

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*, n°48, (dossier vie privée), juin 2015.

FAURE-MUNTIAN V., *Rapport au Gouvernement, Les données géographiques souveraines,* juillet 2018.

GOUVERNEMENT VALLS II, *Stratégie numérique du gouvernement*, publié du 26 Août 2014 au 11 Février 2016, Dossier de presse du 18 juin 2015.

GORCE G. et 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 (2013-2014), 16 avril 2014.

JUTAND F., *Ouverture des données de transport*, Rapport remis au secrétaire d'État chargé des transports, de la Mer de la Pêche, mars 2015.

OECD,

- « A measurement roadmap for the future », in *Measuring the Digital Transformation: A roadmap for the future*, OECD Publishing, Paris, 2019.
- « Data-driven Innovation: Big Data for Growth and Well-Being », OECD Publishing, Paris, 2015.

ROCHFELD J., *La propriété dans la jurisprudence de la Cour de cassation*, La documentation française, ét. annuelle 2019.

ROCHFELD J., CORNU M. et MARTIN G., J., ss. dir., *L'échelle de communalité. Propositions de réforme pour intégrer les biens communs en droit*, Rapport final de recherche n°17-34, avr. 2021.

SOLEILHAVOUP M. et CRISAN M., *Enquête Pratiques culturales en grandes cultures et prairies 2017 – Principaux résultats* (version modifiée), actualisée le 24 juin 2020, https://agreste.agriculture.gouv.fr/agreste-web/disaron/Chd2009/detail/

THINK TANK GENERATION LIBRE, *Mes data sont à moi. Pour une patrimonialité des données personnelles.* Rapport, 2018.

THINK TANK RENAISSANCE NUMERIQUE,

- *Les défis de l'agriculture connectée dans une société numérique*, nov. 2015.
- *La valeur des données agricoles*, févr. 2018.

THYRAUD J., *Rapport n°3 fait au nom de la commission des lois***,** Doc. Sénat, 1987-88.

TOMASSO L., *Analyse juridique contractuelle des données de l'agriculture numérique*, Multipass, 29 nov. 2019.

VERDIER H., *La donnée comme infrastructure essentielle*, Rapport au premier ministre sur la donnée dans les administrations 2016-2017 de l'administrateur général des données, La documentation française, 2018.

VILLANI C., *Donner un sens à l'intelligence artificielle : Pour une stratégie nationale et européenne, Rapport AI for Humanity*, Mission confiée, par le Premier Ministre Philippe E., Mission parlementaire du 8 sept. 2017 au 8 mars 2018, publié en mars 2018.

WAINSTAIN J., « Partager les données pour réussir les transitions agricoles et alimentaires », in Abis, S. et Brun, M., ss. dir., *Le Démeter 2021, Produire et se nourrir : le défi quotidien d'un monde déboussolé*, IRIS éd., févr. 2021, pp. 191 - 206.

WARUSFEL B., « Numérisation de l'action publique et open data : une révolution face à ses limites », Colloque – Circulation des données et propriétés intellectuelles, *PI*, avr. 2020

VII. DOCUMENTATION NON JURIDIQUE

BIARD V., « partage de données agricoles, les applications montent en puissance en France », avr. 2022, https://www.larevuedudigital.com/partage-de-donnees-agricoles-les-premieres-applications-en-france/

BRUN F., « Quelles opportunités et craintes sur les échanges de données agricoles ? Point de vue des agriculteurs », Projet Multipass, 14 janv. 2019 ; https://numerique.acta.asso.fr/multipass-1-opportunites-craintes-data-agri/.

CHAPUIS J., « Agriculture et numérique : la technologie au service des agriculteurs ? », Un monde en docs, présenté par CHAPUIS J., émission diffusée sur Public Sénat, le 27 févr. 2021.

COCHELIN P., « La poule aux œufs d'or échappera-t-elle aux agriculteurs ? », *Terre-net média*, 15 mai 2018.

COPA COGECA, *Code de conduite de l'UE relatif au partage des données agricoles par accord contractuel*, 2018.

L'EFFET PAPILLON, « États-Unis : Les agro-hackeurs », *Documentaire*, 24 sept. 2017.

EUDES Y., « Les agriculteurs hackeurs du Nebraska », *in Le Monde*, https://www.lemonde.fr/pixels/visuel/2017/08/08/agro-hackeurs-du-nebraska_5170156_4408996.html.

FNSEA et JA, *Valoriser et sécuriser les données des exploitations agricoles dans les contrats, Charte Data-agri*, 2018.

LAUGA B., *Synthèse du projet MULTIPASS – faire émerger de nouveaux services dans une chaine de confiance*, mai 2021.

LEROUX C., *Standards et échanges de données dans le numérique Agricole*, sur le site Aspexit, https://www.aspexit.com/standards-et-echanges-de-donnees-dans-le-numerique-agricole/.

MAUREL L., « Données personnelles et recherche scientifique : quelles articulations dans le RGPD ? », 18 juill. 2018.

PAYSAN BRETON, « Le cyber-risque désormais présent dans le secteur agricole », Paysan Breton, *Hebdomadaire Technique Agricole*, 26 mars 2021.

VIII. WEBINAR/COURS EN LIGNE

FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, *Farm Data Management, Sharing and Services for Agriculture Development*, Unit 2. Data Sharing Principles, Lesson 2.2: Challenges for Smallholders in Data Value Chains, oct./nov. 2019.

GODAN, *Webinar: Farmers rights on data and ownership issues*, 18 sept. 2018.

Table de jurisprudence

I. Jurisprudence

A. Jurisprudence interne

1. Conseil constitutionnel

Cons. const., 12 juill. 1979, n°79-107 DC, *Ponts à péage* : Rec. p. 31 ; RJC, I, 73 ; FAVOREU, L., *Rec. de jur. constit*., 1959-1993, p. 73 ; *RDP*, 1979, 1691.

Cons. const., 26 juin 1986, décision n°86-207, DC, *Loi autorisant le Gouvernement à prendre diverses mesures d'ordre économique et social* : *JORF* du 27 juin 1986 ; Rec., p. 61 ; note RIVERO J., *AJDA 1986*. 575 ; chron. AVRIL P. et GICQUEL J., *Pouvoirs*, 1987, n°40, p. 178 ; chron. FAVOREAU L., *RD publ*. 1989. 399 ; FAVOREAU L. et PHILIP L., S. 1989. 659-682 ; note CHAMARD-HEIM C., *GDDAB* 2013. 644 ; note FAVOREAU L. et Philip L., *D.* 2009. 514 ; note GENEVOIS B., *Annuaire int. de just. const*., 1986, pp. 427 et 454 ; note GUYON Y., *RDS* 1986. p. 606 ; note AMADEI J.-P., *LPA*, 1995, p. 19.

Cons. const., 30 nov. 2012, déc. n°2012-285, QPC : chr., DISANT, M., *LGP*, 2013, n°97 à 99, pp. 21 à 22 ; doc., FRAPPIER, M., *RDP*, 2021, n°05, pp. 1239 à 1267 ; chr., MATHIEU, B., VERPEAUX, M. et MACAYA, A., *JCP G*, 2014, JCP G, n°12, pp. 567 à 574 ; chr., GICQUEL, J.-É, *LPA*, 2013, n°140, pp. 6 à 22.

Cons. const., déc. n°2019-823, QPC, 31 janv. 2020, *Union des industries de la protection des plantes* : Pan. DEBAETS E. et JACQUINOT, N., *D.S.*, 2021. 24 ; chron. VERPEAUX M., MACAYA A., *JCP G* 2021. 39 ; chron. VIDELIN J.-C., *JCP A*, 2021. 21 ; chron. FONBAUSTIER L., *Energie – Environnement – Infrastructures,* 2021, 4 ; pan. HOURSON S., *Rev. Du Centre Michel de l'Hospital,* 2021, 22 ; chron. PEGLION-ZIKA C.-M., *RLDC*, 2021, 190 ; Comm. TORRE-SCHAUB M., *AJFP*, 2020, 43 ; KAMAL-GIRARD M., *LGP*, 2020, 25; chron. ROBLOT-TROIZIER A., *RFDA*, 2020, 501; comm. ATTARD J., *LPA*, 2020, 10; note BRAMERET S., RLC, 2020, 26 ; chron., MARTINEZ J., *Concurrences*, 2020, 211 ; Pan., CLAVEL S., et JAULT-SESEKE F., *D.S.*, 2020, 951 ; MONTEILLET V., et LERAY G., *D.S.*, 2020, 1012 ; Ét. BILLET P., *JCP A*, 2020, 44 ; chron. AUDUBERT V., *RDH*. 2020. 14 ; note PARANCE B et MABILE S., *DS.* 2020. 20 ; SALLES S., *LGP*. *2*020. 24 ; Pan. REBOUL-MAUPIN N. et STRICKLER Y., *D.S.* 2020. 31 ; Pan. AVOUT L. BOLLE S. et FAMOUX É., *D.S.* 2020. 35.

2. Tribunal des conflits

T. confl., 6 nov. 1978, *Bernardi*, 02086 : Rec. 652 ; note MODERNE F., *RDSS* 1979. 91 ; chron. DUTHEILLET DE LAMOTHE O. et ROBINEAU Y., *AJDA* 1979, n°1, p. 22.

3. Juridictions judiciaires

a. Juridictions de première instance

TGI, Paris, 19 déc. 1968 : *D.*, 1969, somm. 118.

T. Com., Lyon, 30 juill. 1993 : note LATREILLE A., *LPA* 28 avr. 1995, p. 14 ; obs. VIVANT M. et LE STANC C., *JCP E* 996, I, 559 ; obs. KÉRÉVER A., *RIDA* 4/1994, p. 297.

TGI Nanterre, 18 mai 1994 : *Gaz. Pal*. 1997, 2, somm.

TGI Paris, 12e ch., 26 juin 1995 : note ALVAREZ, *LPA* 1996, n°27, p. 4.

TGI Paris, 13e ch., 25 févr. 2000 : JurisData n°2000-134655 ; *D.* 2000, p. 219.

TGI, Paris, 3ech., 5 sept. 2001, n°00/1796 : JurisData n°2001-161802 ; obs. MAFFRE-BAUGE A, *JCP G*, 2002, n°73 ; obs. COSTES L., *RLDA*, 2001, n°43, n°2735 ; obs. TELLIER-LONIEWSKI L., *Légipresse*, 2001, n°187, III, p. 219 ; note CARON Ch., *CCE*, 2002, n°2, comm. 16.

TGI Versailles, 18 déc. 2007, n°0511965021, *L. c/ Valéo* : CAPRIOLI É., *CCE*, 2008, comm. 62.

TGI Paris, 3e ch., 1re section, 6 oct. 2009, *Casalis c/Ville de Paris* : JurisData n°2009-020440, CARON C., *CCE* n°5, mai 2010, comm. 45.

TGI, Paris, 3e ch., 30 mars 2010 : obs. SIRINELLI P., *RIDA* 2/2015, p. 345 et p. 281 ; note LARRIEU, J., *Propr. industr*. 2010, comm. 75.

TGI, Paris, 3e ch., 13 avr. 2010 : note CARON C., *CCE*, 2010, comm. 84, 3e esp. ; obs. BERNAULT C., *LEPI* nov. 2010, p. 3.

TGI Clermont-Ferrand, ch. corr., 21 juin 2010 : VERON M., *Dr. pén*. 2010, comm. 116.

TGI Nîmes, 28 juin 2013, n°13/1677 : CAPRIOLI É., *CCE*, n°1, janv. 2014, comm. 11.

TGI, Paris, 13e ch. corr. 1, 28 sept. 2016.

T. com., Paris, 28 mars 2022, n°2018017655 : comm. BERLEMONT, J., *Actualités du droit*, , avr. 2022 ; comm., AUGAGNEUR, L.-M., *Actualités du droit*, mars 2022.

b. Cours d'appel

Douai, 7 oct. 1992 : JurisData n°1992-49432.

Paris, 1e ch., sect. conc., 18 mars 1993, *Sté du journal téléphoné*, n°92/1499 : note DRAGO R., *RJC*, 1993. 320 ; note COUSIN A, *Gaz. Pal*., 9 juill. 1993, p. 317.

Paris, 4e ch., 15 janv. 1997 : JurisData n°1997-022369 ; *Expertises* 1997, p. 193, note TELLIER-LONIEWSKI, L., *LGP*, n°18, p.p. 52 et 53.

Bordeaux, 1e ch., 29 avr. 1997, *Pradier c/Artphoto*.

Paris, déc. n°97-D-69, 23 sept. 1997, *SARL Héli-Inter Assistance* : BOCC, 1997.

Paris, 1re ch., 27 janv. 1998 *EDF c/ Société auxiliaire de chauffage et autres* : *BOCCRF* 1998 p. 54 ; note ADAM C. et BLAZY S., *AJDA* 1998 n°5 p. 435., *D. aff*. 1998, p. 326 ; *JCP E* 1998.

Paris, 4e ch., 8 oct. 1998, n°15 : note MECARY

Paris, 4e ch., 18 juin 1999 : *RIDA* 1/2000, p. 316 ; note CARON C., *CCE*, 1999, comm. 21, 3e esp.

Paris, 4e ch., B, 28 avr. 2000, *Midi minuit* c/ *Hesser* : JurisData n°117960.

Paris, 30 oct. 2002, *Kitetoa c/ Sté Tati* : *CCE*, 2003.

Riom, ch. Com., 14 mai 2003, *Rubie's France c/Msat* : note CARON C., *CCE*, déc. 2003, n°12, p. 27 § 117.

Paris, 4e ch., 18 juin 2003 : JurisData n°2003-223155 ; note CARON C., *CCE*, 2003, comm. 106, ; obs. SIRINELLI P., *D.* 2003, p. 2756.

Paris, 12 févr. 2004, SAEM : *BOCC* 4 mai 2004, prat. DOM J.-P. et BACCICHETTI E., *LPA*, n°126, pp. 5 à 21, 2005.

Versailles, 9e ch., 18 nov. 2004, *Rojo R… c/ Guy R…* : note COSTES L., *RLDI* 2005/2, n°50, p. 21.

Paris, 31 janv. 2006, n°2005/14782 : obs., SELINSKY V., *Lamy conc*., 2006, n°7, pp. 16 à 19.

Paris, 4e ch., 28 févr. 2007 : *RIDA* 2/2007, p. 315 ; obs. LUCAS, A., *PI*, 2007, p. 331.

Montpellier, 2e ch., 2 mars 2007, *Robert* c/*Amed* : JurisData n°342090.

Paris, 1ère ch., 30 sept. 2008 : JurisData n°2008-371143

Paris, 4e ch., 8 oct. 2008, n°07/14272 : n°15, p. 24, note MECARY.

Douai, ch. Corr., 21 oct. 2008 : *JurisData*, n°2008-374086.

Metz, 8 janv. 2009 : RG 06/03499.

Paris, 4e ch. B, 13 mars 2009 : JurisData n°2009-002638

Paris, 27 juin 2012 : obs. COSTES, L., *RLDI* 2012/85, n°2859.

Paris, pôle 5, ch. 12, 24 oct. 2012, n° RG : 11/00404, *Jérôme Kerviel c/ ministère public* : note MORTIER, R., *JCP E* 2012, 1702 ; note RONTCHEVSKY, N., *Bull. Joly Bourse* 2013, p. 87 ; obs. STASIAK, F., *RSC*, 2013, p. 381 ; note LASSERRE CAPDEVILLE J., *JCP G* 2012, 1371.

Paris, Pôle 5, 2e ch., 21 juin 2013, n°12/10106.

Paris, pôle 4, 10e ch., 5 févr. 2014 : note CAPRIOLI E., *CCE* 2014. comm. 40.

Montpellier, 3e ch. corr., 2 juin 2015 : JurisData n°2015-028856.

Paris, pôle 5, 27 oct. 2015 : obs. BRUGUIERE, J.-M., *PI*. 2016, p. 69,; note LARRIEU, *D.*, 2016, p. 2141.

Paris, pôle 5, ch. 14, 14 nov. 2017, M. *X. et Ministère public c/ UpToTen, M. Y, et autre*.

Versailles, 26 janv. 2018, RG, n°16-02894.

Rennes 1ère ch., 17 mars 2020, n°19/06749.

Paris, pôle 5-2, 19 juin 2020, n°19/02523 : JurisData n°2020-009513 ; obs. LE CAM S., *CEIPI* sept 2020 p. 2 ; obs. DALEAU J., *Dalloz IP/IT*, 2021, p. 96.

CA Paris, 2 févr. 2021, n°17/17688, *Le Bon coin*.

Rennes, 1re ch., 14 déc. 2021, n°20/03118.

c. Cour de cassation

Crim 8 janv. 1979, aff. *Logabax*, n°77-93038 : *Bull. crim.* n°13 ; note CORLAY P., *D.*, 1979, p. 509.

Civ. 1re, 6 mars 1979, n°76-15.367 : *Bull. civ.* I, n°82 ; obs. FRANÇON A., *RTD com.* 1979. 462.

Cass. ass. plén., 7 mars 1986, n°84-93.509 : note EDELMAN B., *D.* 1986. 406 ; obs. FRANÇON A., *RTD com*. 1986. 399 ; note MOUSSERON, J.-M., TEYSSIE, B. et VIVANT, M., *JCP* 1986. II. 20 631.

Crim., 9 mars 1987, pourvoi n°84.91-977 : *Bull. crim*. 1987, n°11 ; note DEVEZE J., *JCP* 1988. II. 20913.

Civ. 1ère, 21 déc. 1987, *Bureau de recherches géologiques et minières (BRGM)*, n°86-14167 : Bull. civ. 1987, I, n°348, p. 249 ; concl. CHARBONNIER L. et note PACTEAU B., *RFDA* 1988. 771 ; note RICHER L., *CJEG* 1988. 107 ; note VERON O., *Gaz. Pal.* 1988, II, 685 ; note NICOD B., *JCP* 1989, II, 21183 ; note PERROT R., *RTD civ.* 1989. 145 ; note YOLKA Ph., *GDDAB*, Dalloz, 2013, n°75, p. 663.

Crim., 12 janv. 1989, aff. *Bourquin*, n°87-82265 : *Bull. crim*. n°14 ; JurisData n°1989-700634 ; obs. BOUZAT, P., *RSC* 1990, p. 346 ; obs. LUCAS DE LEYSSAC, M.-P, *id.*, p. 507. ; obs. BOUZAT P., *RTD com.* 1990, p. 143; *Bull. crim*. 1989, n°14 ; obs. DEVEZE J., *DIT*. 1989, p. 34 ; obs. DOUCET, *Gaz. Pal.*, 14/15 juill. 1989, p. 23 ; *Expertises* 1989, p. 269.

Crim., 1er mars 1989, aff. *Antonioli,* n°88-82815 : *Bull. crim*. n°100 ; JurisData n°1989-001418 ; note HUET J., *D.* 1990, p. 330 ; obs. BOUZAT P., *RSC* 1990, p. 346 ; obs. LUCAS DE LEYSSAC, M.-P., *id.*, p. 507 ; obs. BOUZAT P., *RTD com.* 1990, p. 142. ; obs. HUET J., *D.* 1990, somm. p. 230 ; obs. VIVANT, M. et LUCAS, A., *JCP E* 1990, II, 15761 ; *Gaz. Pal.* 12 nov. 1989, n°306, jur. p. 18 ; JC*P G* 1989, n°21, IV, p. 186 ; *JCP E*, 1989, n°21, I, p. 141 ; *D.* 1990, n°37, p. 330.

Civ. 1ère, 2 mai 1989, 87-17.657, *Coprosa* : *Bull*. 1989 I n°180 p. 120 ; *RIDA* 1/1990, n°309 ; comm., POLLAUD-DULIAN, F., *Légipresse*, n°118, p. 1 à 17 ; note LUCAS A., *JCP G* 1990, II, 21392.

Civ. 1re, 7 nov. 2000, n°98-17.731 : *Bull.* 2000, n°283, p. 183 : note AUGUET Y., *D.* 2001, p. 2400 ; chron. SERRA Y., obs. PENNEAU J., obs. TOURNAFOND O. ; obs. MESTRES J. et FAGES B., *id.*, p. 130 ; note VIALLA F., *JCP* 2001.éd.GII.10452 ; obs. ROCHEFELD J., I.301, n°16 ; obs. LEVENEUR L., *Contrats, conc. consom*. 2001.18.

Crim., 14 nov. 2000, n°99-84.522 : *Bull. crim.* ; 2001. 1423, note de LAMY B. ; obs. OTTENHOF R., *RSC* 2001. 385 ; obs. REVET T., *RTD civ*. 2001. 912.

Crim., 9 sept. 2003, n°02-87.098 : note DELVOIE A., *Gaz. Pal.* 2004. Somm. 1338.

Com., 12 juill. 2005, n°04-12.388, NMPP/MLP : Bull. civ. 2005, IV, n°163 ; Note FRISON-ROCHE, M.-A., *RDA*, n°2006/2, 2006.

Crim. 6 sept. 2005 : note COSTES, L., *RLDI*, 2005/19, n°279, p. 18.

Civ. 1re, 29 nov. 2005, *Marie-Claire Album c/ Hamel*, n°04-12.721 : obs. DALEAU J., *D.* 2006, AJ p. 145, et note TRICOIRE A., *Jur*. p. 517 ; obs. CARON C., *CCE*. févr. 2006, n°18.

Crim., 14 mars 2006, n°05-83.423 : *Bull. crim.* N°69 ; *D.* 2006 ; *AJ pénal* 2006, p. 260.

Com., 20 févr. 2007, n°06-12.424 : obs. PHILLIPE, J. et JANSSENS T., *LGP*, 2007, n°166, pp. 37 et 38.

Crim., 4 mars 2008, n°07-84.002 : NP, note DETRAZ S., *D.* 2008. 2213 ; obs. VIVANT M. et MALLET-POUJOL N., *JCP E* 2009. 1674, nº 22 ; obs. BRUGUIERE J.-M. et HUET J., *CCE* 2008. Ét. 25 ; comm. DETRAZ S., *D.*, 2008, p. 2213 ; comm. FRANCILLON J., *Revue de science criminelle*, 2009, p. 131.

Civ. 1ère, 5 mars 2009, n°07-19.734, 07-19.735, aff. *Précom, Ouest France Multimédia c/ Direct annonces* : *Bull*. ; note POLLAUD-DULIAN F., *RTD com.*, 2009, n°4, pp. 724 à 727.

Civ. 1ère, 5 mars 2009, *News invest c/ PR Line* : Bull. civ. I, nº 46 ; note CARON C., *CCE* 2009, nº 5, comm. 43 ; obs. DALEAU J., *D.*, 2009, AJ, 948 ; *JCP G* 2009, IV, nº °1570 ; obs. BRUGUIERE J.-M., *PI*, 2009, nº 32, p. 275 ; chron. SIRINELLI P. *RIDA*, 2009, nº 221, p. 491 ; note RAMBAUD S., *RLDI* 2009/49 nº 1572 et *RLDI* 2009/49 nº 1594.

Crim., 27 oct. 2009, n°09-82.346 : *Bull. Crim.*, n°177 ; obs. DARSONVILLE A., *D.* 2010. 806 ; note LASSERRE CAPDEVILLE J. ; obs. ROYER G., *AJ pénal* 2010. 79 ; obs. FRANCILLON J., *id.*,

2010. 178 ; obs. BOULOC B., *RTD com.* 2010. 441 ; note LEPAGE A., *JCP* 2010, n°1-2, 19 ; note ARRIGO P. et BLIN D., *Gaz. Pal*. 2010. 1, jur p. 261.

Com., 23 mars 2010, n°08-20.427, n°08-21.768 : JurisData n°2010-002593 ; note CARON C., *CCE* 2010, comm. 83, 1re esp. ; *Expertises* 2010, p. 230 ; note BOUCHE N., *Propr. industr*. 2010, comm. 43 ; obs. BRUGUIÈRE J.-M., *PI* 2010, p. 856 ; obs. CASTETS-RENARD C., *RLDI* juill. 2010, n°62, 2030.

Crim., 27 avril 2011, n°10-86.233.

Cass. 1ère civ., 20 oct. 2011, n°10-21.251.

Crim**., 16 nov. 2011, n°10- 87.866 :** *Bull. crim.* 2011, n°233

Crim, 30 janv. 2013, n°11-89.224 : *Bull. crim*. 2013, n°33 **;** note VERON M., *Droit pénal*. 2013. 5 ; note DREYER E., *LGP. 2*013. 128-131 ; chron. BOURSIER M.-E., *LPA.* 2013. 125 ; chron. BOULOC B., *RTD com*. 2013. 3 ; chron. MARON A. ROBERT J.-H., VERON M., *JCP G*. 2013. 40 ; note LASSERRE CAPDEVILLE J., *AJDP. 2*013. 11 ; chron. HENON M., GOUPIL M., CARVLHO K et al., *JCP A.* 2013. 45 ; chron. ROUJOU DE BOUBEE G., GARE T., GOZZI, M.-H., MIRABAIL S. et POTSZKIN T., *D.S*., 2013. 41.

Civ. 1ère, 14 nov. 2013, n°12-20.687 : obs. SIRINELLI P., *D*. 2014. 2078.

Crim., 19 mars 2014, n°12-87.416.

Crim. 22 oct. 2014, pourvoi n°13-82.630 : JurisData n°2014-024941.

Cass. 1ère civ., 18 févr. 2015, n°13-26.036.

Crim., 20 mai 2015, n°14-81.336.

Civ. 1ère, 3 nov. 2016, n°15-22.595.

Crim., 22 mars 2017, pourvoi n°15-85.929 : *Bull. crim.* 2017, n°78.

Crim., 10 mai 2017 : *JurisData,* n°2017-008826.

Com., 21 juin 2017, pourvoi n°15-25.941, inédit.

Crim., 28 juin 2017, n°16-81.113 : BEAUSSONIE, G., *D*. 2017. 1885, DESGENS-PASSANAU, G., *Dalloz, IP/IT*, 2017. 663, ROUJOU DE BOUBEE, G., *D*. 2017. 2501 ; SAENKO, L., *RTD. com*. 2017. 713 ; MATSOUPOULOU, H., *RSC* 2017. 752.

Crim., 7 nov. 2017, n°16-84918.

Crim. 16 janv. 2018, *JurisData,* n°2018-000269.

Crim., 5 avr. 2018, pourvoi n°17-81.085 : *Bull. crim*. 2018, n°62.

Civ. 3e ch., 10 oct. 2019, n°16-21.177 : Juris-Data n°2019-017692 *Inédit* ; comm. MEILLER E., *Rev. droit rural*. 2020. 480 ; pan. ROUX J.-M. *Annales des loyers*. 2019. 12.

Civ. 1ère, 2 févr. 2022, n°20-16.040, *Association Red Pill*.

4. Juridictions administratives

a. Tribunaux administratifs

TA Poitiers, 31 janv. 2013 : obs. L. C., *RLDI* 2013/92, 3059 ; note BRUGUIERE, J.-M., *JCP A* 2013, 2442.

b. Cours administratives d'appel

CAA Nancy, 2 févr. 2009 : req. n°07NC00604, inédit ; Rec.

CAA Nancy, 3e ch., 19 mars 2009, n°07NC01327 : JurisData n°2009-005087.

CAA Bordeaux, 4e ch., 26 févr. 2015, *Notrefamille.com* c/ *Département de la Vienne* : obs. BRUGUIERE J.-M., *PI* 2015, p. 209.

c. Conseil d'État

CE, 1er févr. 1901, *Descroix et autres boulangers de Poitiers* : concl. ROMIEU J., *S.*, 1991. 17 ; note HAURIOU M., *RGD* 2014. 15150.

CE, 29 mars 1901, *Casanova*, req. n°94580 : Rec. p. 33 ; comm. FAURE B., *AJDA* 2001. 136 ; note HAURIOU M., *RGD*. 2013. 3.

CE, sec., 30 mai 1930, *Chambre syndicale du commerce en détail de Nevers*, req. n°06781 : Rec. p. 583 ; concl. JOSSE ; note ALIBERT R. ; avis GUYOMAR M. et COLLIN P., *AJDA*, 2000. 12 ; comm. TREPPOZ A., *AJDA*. 2001. 7 ; comm. LOMBARD M., *RJEP*. 2011. 683 ; comm. TOUZEIL-DIVINA M., *JCP A*. 2020. 15 ;

CE, ass., 31 juill. 1942, *Monpeurt*, n°71398 : Rec. p. 239 ; concl. SEGALAT, note P.C. *D.* 1942. 138 ;. Concl. LAROQUE P., *JCP* 1942. II. 2046 ; note BONNARD *RD publ.* 1943.57, concl. ; concl. S. 1942.3.37 ; CASSIN R. et WALINE M., *GAJA*. 2017. 304.

CE, 28 juin 1946, *Morand*, n°73774 : rec. 183 ; note P.M. S. 1947.

CE, sect., 18 juin 1963, *Narcy*, req. n°43834 : Rec. p. 401 ; obs. WALINE M., *RD publ*. 1963. 1186 ; obs. de LAUBADERE A., *AJDA* 1964, p. 91.

CE, avis, 21 nov. 1972, *Ofrateme*, pourvoi n°309721 : comm. KUPERFILS G., *GACE*, 2e éd., Dalloz, 2002, p. 105 ; comm. YOLKA Ph., *GDDAB*, Dalloz, 2e éd., 2015.

CE Sect. 13 oct. 1978, *ADASEA du Rhône* : Lebon 368 ; RD publ. 1979.899, note ROBERT, J., p. 908 et s., concl. GALABERT, *D.* 1979.249, note AMSELEK, P., et WALINE, J., *AJDA* 1979. II. 35, *ibid.* I. 22, chron. DUTHEILLET DE LAMOTHE ET ROBINEAU.

CE, 20 juill. 1990, *Ville de Melun et association « Melun-culture-loisirs » c/Vivien et autres* : rec. 220 ; concl. POCHARD. *AJDA* 1990. 820 ; note FATOME *JCP* 1991. II. 21663.

CE 17 févr. 1992, *Sté Textron* : *Lebon* 66, *AJDA* 1992.450 ; note PENNEAU A., *D.* 1992, Jur. p. 519.

CE, 20 nov. 1995, *Borel*, req. n°147026 : Rec. 795, *Gaz. Pal.* 1996, Pan. *Dr. Adm*. p. 84.

CE ass., 10 juill. 1996, *Sté Direct mail promotion*, n°168702, 168734, 169631, 169951 : *Rec*. 277 ; concl. DENIS-LINTON M., *RFDA* 1997. 115 ; note MAISL H., *AJDA* 1997, 189.

CE, 29 juill. 2002, *Sté Cégédim*, pourvoi n°200886 : *Rec*. p. 280 ; note NICINSKI S., *AJDA* 2002, p. 1072 ; obs. GONZALEZ G., *Dr. adm*. 2002, p. 901 ; note BAZEX M. et BLAZY S., *Dr. adm*. 2002, 13 ; note et comm. BRUGUIERE J.-M., *JCP E* 2003. 149 ; concl. MAUGÜE C., *AJDA* 2004, veille p. 166 ; note SCHMIDT-SZALEWSKI J., *PI*, 2004. 28 ; note LUCAS A., *PI* 2003. 57 ; MALAURIE-VIGNAL M., *CCC*. 2003. 12 ; chron. BOITEAU C., *JCP* 2002. 2278 ; LATREILLE A., *Dr. et patr*. 2007. 28 ; note BOISSE (de) H., *Expertises*, 2003. 23 ; HOURSON S., RGD. 2008. 1.

CE, 26 févr. 2003, *Société protectrice des animaux*, n°212943 : *Rec*. 787 ; note COSTA D., *AJDA*. 2003. 1488 ; concl. GOULARD *BJCL*. 2003. 361.

CE, sec. cont., 22 févr. 2007, *Association du Personnel relevant des Établissements pour Inadaptés (APREI)*, n°264541 : Rec. p. 92 ; concl. VEROT. Chron. LENICA et BOUCHER, *AJDA* 2007. 793 ; note GUGLIELMI et KOUBI, *JCP A* 2007. 2145 ; note BOITEAU, *RFDA* 2007. 803.

CE, sect., 06 avr. 2007, *Commune d'Aix-en Provence*, n°284736 : Rec. 155 ; chron. LENICA F. et BOUCHER J., *AJDA*. 2007. 1020 ; note BAZEX M. et BLAZY S., *AJDA*, 2007. 35 ; note ROUAULT M.-C. *RLCT*. 2007. 26 ; chron. PLESSIX B., *JCP G*. 2007. 21; MARAIS B., KOVAR J.-P., et RODRIGUES S., *Concurrences*. 2007. 163 ; note BRUNET P., *Rev. des contrats*. 2007. 867 ; concl. SENERS F., *RJEP*. 2007. 273 ; comm. KARPENSCHIF M., *JCP G*. 2007. 31 ; comm. GLATT, J.-M., *LPA*. 2007. 13 ; note TOUZEIL-DIVINA M., *LGP*. 2007. 4 ; chron. ORSONI G., *RTD com*. 2007. 694 ; note COURNIL C. et RENEAUD F., *JCP E* 2009. 37.

CE, 5 oct. 2007, *Société UGC-Ciné-Cité*, n°298773 : Rec., p. 418 : concl. CASAS D., *BJCP* 2007, n°55, p. 483 ; note ECKERT G., *CMP*, 2007, n°11, p. 27 ; note LINDITCH F., *JCP A* 2007, n°56, p. 38 ; note DREYFUS J.-D., *AJDA* 2007, n°41, p. 2260 ; chron. PLESSIX B., *JCP* n°50, p. 19 ; note GLATT J.-M., *LPA*, 2007, n°252, p. 19 ; note MONDOU Ch., *RLCT*, 2008, n°31, p. 26 ; note CLAMOUR G., *RLC*, 2008, n°14, p. 57 ; note MILLET F.-X., *Gaz. Pal.* 2008, n°48-50, p. 12 ; note MOREAU D., *RJEP*, 2008, n°652, p. 27 ; note COURNIL Ch. et RENEAUD F., *JCP E* 2009, n°11, p. 37 ; ét. VIEL M.-Th, *RGCT*, 2010, n°47, p. 163.

CE 5 mai 2008, *Thiébaux*, req. n°294645 : Rec., inédit ; *JCP Adm*. 2008. 2182, note DARCY, G., *AJDA* 2008. 1735, *JCP N* 2001. 547 ; *Gaz. Pal.* 3-4 oct. 2001, p. 22.

CE, 25 juill. 2008, *Commissariat à l'énergie atomique (CEA)*, n°280163 : *Rec*, p. 751 ; obs. AÏT-EL-KADI. AJDA. 2008. 1521.

CE, 10e et 9e ch. réunies, 10 mars 2010, *Commune de Sète,* n°303814 : Rec. 70 ; note PELLISSIER G., *JCP A*. 2010 n°16 p. 23 ; note MELLERAY F., *AJDA*. 2010, n°5 p. 25 ; GLASER E., *RLCT*. 2010 n°58 p. 18 ; obs. DUBREIL *JCP A*. 2010. 221.

CE, 2 mars 2011, déc. n°345288, *Sté Manirys*.

CE, 10ème et 9ème ch. Réunies, 17 avr. 2013, *Ministre du travail, de l'emploi et de la santé c/ Cabinet de la Taille*, req. n°344924 : *Rec*. ; comm. DELAUNAY B., *AJDA*. 2013 n°33 p. 1920.

CE, 17 avril 2013, *La Poste c/ M. Bigi*, n°342372, t. pp. 601-602 : comm. KOUBI G., *JCP A*. 2013 n°28 p. 25 ; note DELAUNAY B., *AJDA*. 2013 n°°33 p. 1920.

CE, 8e et 3e ch., 15 févr. 2016, *Société cathédrale d'Images*, n°384228 : note SCHMITT R., *Lexbase* éd. pub. 2016. 407 ; note EXKERT G., *CMP*. 2016 n°4 p. 45 ; comm. BRENET F., *AJDA*. 2016. n°5 p. 34 ; comm. PAULIAT H., *JCP A*. 2016 n°25 p. 37 ; chron. LLORENS F. et SOLER-COUTEAUX P., *CMP* 2017 n°3 p. 11.

CE, 8 févr. 2017, n°389806, *Sté Notrefamille.com* : Rec ; *AJDA* 2017. 318 ; obs. LARRIEU J., LE STANC C. et TREFIGNY P., *D*. 2017. 2390, ; obs. DREYFUS J.-D. *AJCT* 2017. 350 ; obs. LAMBOT, *JCP Adm*. 2015, 2239.

CE, 10ème - 9ème chambres réunies, 08 févr. 2017, n°393714 : rec. ; *AJDA* 2017. 325 ; obs. PERRAY R. et UZAN-NAULIN J., *Dalloz IP/IT*, 2017 p. 286.

CE, 10ème et 9ème ch. réunies, 21 avr. 2017, *Régie autonome des transports parisiens*, n°395952 : *Rec*. ; concl. CREPEY E., *AJDA* 2017. 1206 ; comm. VIROT-LANDAIS A., *JCP A*. 2017 n°27 p. 15 ; note CHIFFLOT N., *Procédures* 2017 n°10 p. 27.

CE, 6e et 1e ch. réunies, 12 juill. 2017 : n°397403, rec. ; chr., ROUSSEL S., *LGP*, 2017, n°44, p. 34 et 35 ; chr., LOMBARD, F., *RTD com*., 2017, n°4, pp. 859 à 861.

CE, 10e et 9e ch. Réunies, 8 nov. 2017, *Association spirituelle de l'Église de scientologie Celebrity centre*, n°375704 : note DELAUNAY, *AJDA* 2013. 1920 ; note COSTES L., *RLDI*. 2017 n°143 p. 30 ; note ROUSSEL S., *LGP*. 2017 n°44 p. 32 ; note CHIFFLOT N., *Procédures*. 2018 n°1 p. 37 ; note CARON C., *CCC* 2018 n°2 p. 34 ; comm. EVEILLARD G., *AJDA* 2018 n°3 p. 29 ; chron. EVEILLARD G., *JCP G* 2018 n°13 p. 621 ; note BRUGUIERE J.-M, *PI*. 2018 n°67 p. 38 ; chron. ROUAULT M.-Ch., *LPA*. 2018 n°81 p. 9 ; comm. BINCTIN N., FOULQUIER N., KALFLECHE G. et SORBARA J.-G., *PI*. 2018 n°68 p. 82 ; chron. MORAND-DEVILLER J., POULET F. et BOURDON P., *LPA* 2018 n°143 p. 12 ; note PETELIN T., *JCP E*. 2019 n°6 p. 40.

CE, 2ème et 7éme ch. réunies, 16 févr. 2018, *Union des transports publics et ferroviaires (Arafer)*, req n°403508 : *Rec*. ; AJDA 2018 371 comm. MARCIOT H. et HULOT Q., *RLC*. 2018 n°71 p. 7 ; chron. GUILLAUME E., *Concurrences* 2018 n°2 p. 175.

B. Juridictions européennes

1. TPIUE (ex-TPICE)

TPICE, 18 sept. 1996, n° T-353/94, *Postbank* : chron. BLAISE, J.-B. et IDOT, L., *RTD eur.* 1997. 459.

TPICE, 15 sept. 1998, aff. T-374/94, T-375/94 et 388/94, *European Night services ltd et a. c/commission* : Rec. II. 3141 ; note IDOT L., *Eur*. 1998 n°11 p. 17 ; note POILLOT-PERUZZETTO S., *CCC*. 1998 n°12 p. 14 ; note *LPA* 2000 n°27 p. 14 ; chron. CHABRIER H., COULON E., LORIOT G. et TRUCHOT L., *RMCUE* 2000 n°436 p. 179 ; BLAISE J.-B et IDOT L., RTD *Eur*. 1999 n°29.

TPICE, 25 mars 1999, aff. T-102/96, *Gencor Ltd/Comm*. CE : Rec. II. p. 753 ; note PRIETO C., 2005, *JDI* 2005 n°2 p. 446 ; chron. PILCZER J.-S., *Cah. Dr. eur*. 2014 n°3 p. 597 ; IDOT L., *Eur*. 1999, p. 7.

TPICE 6 juill. 2000, aff. T-62/98, *Volkswagen AG c/Comm. CE* : comm. IDOT L., *Rev. Eur*. 2000 n°10 p. 21 ; chron. VALLERY A. et LOUIS F., *Cah. Dr. eur*. 2000 n°5-6 p. 719 ; note POILLOT-PERUZZETTO S., *CCC* 2000 n°12 p. 15 ; chron. KRAMER P., *LGP* 2000 n°357 p. 50; note PIRETO C., *JDI* (Clunet) 2001 n°2 p. 656 ; chron. SUDRE F., *RTDH* 2001 n°47 p. 797 ; chron. BLAISE J.-B. et IDOT L., *RTDE* 2002 n°3 p. 555 ; comm. VALIGNY C., *RLC* 2005 n°5 p. 139.

TPICE, 22 déc. 2004, aff. T-201/04, *Microsoft* : Rec. 2004 II-04463 ; note BENABOU V.-L., PI, 2005 n°14, p. 89.

TPICE, 22 févr. 2005, n° T-383/03, *Hynix Semiconductor* c/Conseil : Rec. p. II-621.

TPIUE, 17 sept. 2007, aff. T-201/04, *Microsoft* : obs. CHEVRIER E., *AJ*. 2007 p. 2303 **;** EDITO ROME F., *Eur*. 2007 p. 2521 ; obs. POLLAUD-DULIAN F., *RTD com.* 2007 p. 715 ; Prat. ROBIN C. et SELINSKY V., *RLC* 2008 n°14 p. 26 ; note GUNTHER J.-P *RLC* 2008 n°14 p. 169 ; note BENABOU V.-L., *PI* 2008 n°26 p. 122 ; note CHALTIEL F., BERR C., FRANCQ S. et PRIETO C., *Journal du droit international* 2008 n°2 p. 632 ; note PHILIPPE J. et JANSSENS T., *LGP* 2008 n°9 p. 17 ; LUBY M. et POILLOT-PERUZZETTO S., *JCP G* 2008 n°5 p. 20 ; note SCHMIDT-SZALEWSKI J., *PI* 2008 n°3 p. 41 ; note BEHAR-TOUCHAIS M., *CCC* 2008 n°3 p. 8 ; note DECOCQ G., *JCP E* 2008 n°10 p. 18 ; FOUQUET T., SLADIC J. et VANHAM É, *Eur*. 2008 n°148 p. 114 ; act. SELINSKY V., *RLC* 2008 n°15 p. 131 ; chron. PRIETO C., *RDC* 2008 n°3 p. 811; chron. LUBY M. et POILLOT-PERUZZETTO S., *JCP G* 2008 n°27 p. 28; pan. FERRIER D., *D.S*. 2008 n°31 p. 2193; comm. CARDON M., *RLC* 2008 n°17 p. 142; comm. Art J.-Y., *RLC* 2008 n°17 p. 173; comm. NOURISSAT C., *RLC* 2008 n°17 p. 176; obs. FERRIER D., *D*. 2008 p. 2193 ; chron. SARDAIN F., *JCP E* 2009 n°5 p. 28; chron. BACCICHETTI E. et BONNET Ph., *JCP E* 2009 n°46 p. 18.

TPI, 7 juill. 2011, *Gregorio Valero Jordana* c/ *Commission* : T-161/04

2. CJUE (ex-CJCE)

CJCE, 14 juill. 1972, aff. C-48/ 69, *Imperial Chemical Industries* : Rec. CJCE, p. 619.

CJCE, 13 févr. 1979, aff. 85/76, *Hoffmann-La Roche & Co. AG c/ Comm.* CE : Rec. 461.

CJUE, 28 janv. 1986, aff. 161/84, 61984J0161, *Pronuptia de Paris GmbH c/ Pronuptia de Paris Irmgard Schillgalis* : coll., CELAYA M., *Lamy Droit des affaires*, 2012, pp. 40-44.

CJCE, 6 avr. 1995, aff. jointes C-241/91 et C-242/91, *Magill* : *Rec*. p. I-743 ; obs. BONET G., *RTD eur.* 1995 p. 835 ; note BENABOU V.-L., *PI* 2002 n°3 p. 117 ; chron. POLLAUD-DULIAN F., *RTD com.* 2004 n°3 p. 491 ; Prat. HAUTBOURG S. et QUESSON S., *DJF* n°56 p. 64 ; chron. BONET G., RTD eur. 2004 n°4 p. 690 ; obs. LEVEQUE F., *concurrences* 2004 n°1 p. 16 ; note SARDAIN F., *JCP E* 2004 n°49 p. 1927 ; obs. GYSELEN L., *concurrences* 2005 n°2 p. 24 ; comm. VIVANT M., MALLET-POUJOL N. et BRUGUIERE J.-M., *JCP E* 2006 n°23 p. 1002 ; Ét. GRYNFOGEL C., JCP E 2008 n°47 p. 42 ; chron. SARDAIN F., *JCP E* 2009 n°5 p. 28.

CJCE 14 nov. 1996, *Tetra Pak c/ Commission*, aff. C-333/94 P : Rec. I. 5951 : note S., Y., *Gaz. Pal*., 1998, 184. p. 38 : comm. KORAH V., *ECLR* 1997, n°3 pp. 98 à 192**.**

CJUE, 26 nov. 1998, aff. C-7/97, *Bronner GmbH & Co KG c/ Mediaprint Zeitung* : *Rec.* I. 7791 ; obs. POILLOT-PERUZZETTO S., *RTD com* 1999 p. 798 ; chron., BLAISE J.-B et IDOT L., *RTD eur.* 1999 p. 271 ; note *Journal du droit international* 1999 n°2 p. 593 ; comm. BERGMAN M., *ECLR* 2000 n°2 p. 59 ; prat. HAUTBOURG S. et QUESSON S., *Décideurs Juridiques et Financiers* 2004 n°56 p. 64 ; pan. CHAGNY M., *Journal du droit international* 2019 n°1 p. 550 ; note BORSCO D., *CCC* 2021 n°5 p. 42.

CJUE, 29 avr. 2004, aff. C-418/01, *IMS Health GmbH & co. OHG* : *Rec.* p. I-5039 ; obs. KAMINA P., *PI*, 2004, n°6, p. 29 ; note IDOT L., *Eur.* 2004, n°6, p. 27 ; comm. CARON C., *CCC*, 2004, n°6, p. 28 ; Pan. BOULET PATIN A.-L., *Lexbase Hebdo*, 2004, n°126 ; note BENABOU V.-L., *PI*, 2004, n°12, p. 821 ; note BONET G., *RTD eur*., 2004, p. 691 ; Prat. HAUTBOURG S. et QUESSON S., *DJF*, 2004, n°56, p. 64 ; ét. PEYRE J., *RLC*, 2004, n°1, p. 26 ; chron., ARHEL P., *LPA*, 2004, n°143, p. 17 ; note SARDAIN F., 2004, *D.*S., n°32, p. 2366 ; pan. RESPAUD J.-L., *Cah. Dr. entr*., 2004, n°4, p. 39 ; comm. PEYRE J., *RLC*, 2004, n°1, p. 26 ; note POILLOT-PERUZZETTO S., *CCC*, 2004, p. 19 ; chron. SARDAIN F., *JCP E*, 2004, n°49, p. 1927 ; ét. SARDAIN F., *D.*, 2004, n°32, p. 2366 ; Prat. HAUTBOURG S. et QUESSION S., *DJF*, 20056, n°61, p. 94 ; comm. SCHMIDT-SZALEWSKI J., *PI*, 2005, n°3, p. 36 ; pan. CORDIER-FERON L., *LGP*, n°135, p. 34 ; obs. LEMARCHAND, *Expertises*, 2002, n°258, p. 139.

CJCE, 9 nov. 2004, aff. n°C-444/02, *Fixtures Marketing Ltd c/ Organismos Prognostikon agonon podosfairou AE (OPAP)* : Rec. *CJCE* 2004, I, p. 10590 ; *Propr. industr*. 2005, comm. 7, 3e esp., note KAMINA, P. et 22, 1er arrêt, note DERCLAYE, E., pt. 29 ; comm., TELLIER-LONIEWSKI, L., et MAURIELLO, P., *LGP*, 2005, n°201, pp. 9 à 11.

CJCE, 9 nov. 2004, aff. n°C-203/02, *The British Horseracing Board Ltd e.a. c/ William Hill Organization Ltd* : comm., TELLIER-LONIEWSKI, L., et MAURIELLO, P., *LGP*, 2005, n°201, pp. 9 à 11.

CJCE, 9 nov. 2004, aff. n° C-338/02, *Fixtures Marketing Ltd* c/ *Svenska Spel AB* : comm., TELLIER-LONIEWSKI, L., et MAURIELLO, P., *LGP*, 2005, n°201, pp. 9 à 11.

CJCE, 9 oct. 2008, aff. C-304/07, *Directmedia Publishing GmbH c/ Albert-Ludwigs-Universität Freiburg* : note CARON, C., *CCE*, 2009, nº 3, comm. 24 ; *Légipresse* 2008, nº 256, I, p. 149 ; note BENABOU, V.-L., *PI* 2009, nº 30, p. 77 ; chron. SIRINELLI, P., *RIDA* 2009, nº 219, p. 297.

CJCE, 16 déc. 2008, aff. C-524/06, *Heinz-Huber* c/ *Bundersrepublik Deutcshland* : comm. Kauff-Gazin, Eur., févr. 2009.

CJCE, 5 mars 2009, aff. C-545/07, *aff. Apis-Hristovich c/ Lakorda AD* : obs. SIRINELLI, P., *RIDA* 3/2009, p. 415 et p. 389 ; note CARON, C., *CCE* 2009, comm. 44 ; note LARRIEU, J., *Propr. industr*. 2009, comm. 48 ; *RLDI* avr. 2009, 1571 ; obs. SARDAIN, F., *JCP E* 2010, 1070, n°10 ; obs. BENABOU, V.-L., *PI* 2009, p. 383.

CJUE, 16 juill. 2009, aff. C-5/08, *Infopaq International A/S contre Danske Dagblades Forening* : note SARDAIN, F., *JCP E*, n°30 à 33, pp. 30 à 31 ;note MICHAUX B., *Auteurs & Média*, n°5, pp. 473 à 488 ; note VELARDOCCHIO D., *Droit et Patrimoine*, n°185, pp. 106 à 107 ; note POLLIAUD-DULIAN F., *RTD com*., n°4, pp. 715 à 717 ; note MARINO L., *Revue des aff. Eur*., n°2, pp. 361 à 365.

CJUE, 29 juin 2010, aff. C-28/ 08 P, *Commission* c/ *Bavarian Lager* : Rec. II. 4523 ; note DEROBUGNY D., *JDI*, n°2011-2, pp. 494 à 496.

CJUE, 9 nov. 2010 *Volker und Markus Schecke GbR et Hartmut Eifert c/ Land Hessen*, Aff. jointes C-92/09 et C-93/09 : chron. POTTEAU A., *RTD eur*. 2011. 375.

CJUE, 1er mars 2012, aff. C-604/10, *Football Dataco Ltd et autres c/Yahoo ! UK Ltd* : note 447, note VELARDOCCHIO D., *Droit et Patrimoine*, n°228, p. 64 ; note BENABOU V.-L., *PI*, n°46, pp. 88 à 92 ; note MARINO L., *LGP*, n°214 à 215, p. 11 à 12 ; note IDOT, L., *Europe*, n°5, pp. 45 à 46, 2012.

CJUE, 1er mars 2012, aff. C-173/11 *Football Dataco* : *RLDI* 2012/87, nº 2710, obs. Costes L., *JCP E* 2012, aff. 161, *JCP E* 2012, nº 1489, § 4, obs. VIVANT M., MALLET-POUJOL N. et BRUGUIERE J.-M., *D*. 2012, act. p. 735, *D.* 2012, 2838, obs. SIRINELLI P., *PI*. 2012, nº 45, p. 421, obs. BENABOU V.-L., *RIDA* 2012, nº 232, p. 487, obs. SIRINELLI P., *CCE* 2012, comm. 47, note CARON C., *Propr. indust*. 2012, comm. 75, note LARRIEU L., pt 19 ; voir comm. VARET E., *in RLDI* 2012/87, nº 2933.

CJUE, 2 mai 2012, aff. C-406/10, *SAS Institute c/World Programming* : *D*. 2012. 1186 ; note MARINO L., *Gaz. Pal*. 2012, 214-215 p. 12 à 13 ; note LOLJEEH R., *Lamy Dr. des aff*., 2012, n°73, pp. 68 à 69 ; note POLLAUD-DULIAN F., *RTD com.* 2012, n°3, pp. 536 à 540.

CJUE, 3e ch., 30 mai 2013, aff. C-342/ 12, *Worten* : LHERNOULD J.-P., TISSANDIER H., GARDIN A. et LAFUMA E., *RJS*, 2013, n°11, pp. 651 à 658 ; DUPONT-LASALLE J., *Europe*, 2013, n°7, p. 20.

CJUE, 13 mai 2014, aff. C-131/ 12, *Google Spain SL, Google Inc. c/ Agencia Española de Protección de Datos (AEPD), Mario Costeja González* : note HARDY B., *RTD E*, 2014 n°4, pp. 879 à 897 ; note KROPF J., *American Journal of international law*, 2014 n°108-3, pp. 502 à 509 ;

CJUE, 17 juillet 2014, aff. jtes C-141/12 et C-372/12 : chron., PLATON S., *Droit adm*., n2015, n°8, pp. 17-26.

CJUE, 15 janv. 2015, n° C-30/14, *Ryanair Ltd* c/ *PR Aviation BV* : *JurisData* n°2015-002578 ; obs. SIRINELLI, P., *RIDA*, 2015/2, p. 319 et p. 301 ; obs. LAMBRECHT, M., *Auteurs et medias*, 2015, p. 181 ; obs. BERNAULT, C., *PI*, 2015, n°55, p. 211 ; obs. CASTETS-RENARD, C., *RLDI*, mars 2015, n°3685 ; note LARRIEU, J., *Pr. Industr*., 2015, comm. 71.

CJUE, 29 oct. 2015, aff. C-490/14, *Freistaat Bayern c/ Verlag Esterbauer GmbH* : obs. BERNAULT, C., *LEPI*, 2016, n°25 ; obs. BERNAULT, C., *PI* 2016, n°58, p. 68 ; obs. BENABOU, V.-L., *Dalloz IP/IT*, 2016, p. 89 ; obs. POLLAUD-DULIAN, F., *RTD com*., 2016, p. 125 ; obs. FAVRE, C. et ZOLLINGER, A., *JCP E*, 2016, 1481, n°9.

CJUE, 19 oct. 2016, aff. C-582/14, *Patrick Breyer c/ Bundesrepublic Deutschland* : *D*. 2016. 2215 ; obs. PERONNE G. et DAOUD E., *Dalloz IP/IT*, 2017. 120 ; note METALLINOS N., *CCE* 2016, n°12, comm. 104; note GAZIN F., *Europe* 2016, n°12, comm. 444.

CJUE, 5e ch., 23 nov. 2016, aff. C-442/14, *Bayer CropScience SA-NV, Stichling De Bijenstichling* c/*College Voor de Toeliating van guasbeschermingsmiddelen en biociden* : JurisData n°2016-027449 ; obs. EMMANOUILIDOU, *RJ envir*. 2017.179 ; note JAMAY, *EEI* 2017, n°23 ; note THEVENOT, *Dr. envir*. 2017. 67 ; obs. CAZET S., *Europe* 2017, n°2.

CJUE, 5e ch., 23 nov. 2016, aff. C-673/13, P., *comm*. c/*Stichling Greenpeace Nederland et PAN Europe* : *RJ envir*. 2017.180, obs. EMMANOUILIDOU ; *EEI* 2017, no 23, note JAMAY; *Dr. envir*. 2017. 67, note THEVENOT.

CJUE 9 mars 2017, aff. C-398/15, *Camera di Commercio, industria, Artigianato e Agricoltura di Lecce c/ Salvatore Manni* : obs. LECOURT A., *RTD com*. 2017. 379 ; note REYGROBELLET, *Rev. sociétés* 2018. 79 ; obs. LECOURT B., *ibid*. 2017. 318 ; *RJDA* 2017, n°406 ; obs. METALLINOS, *CCE* 2017, no 66 ; obs. COSTES, *RLDI* avr. 2017. 33 ; note PAUTROT, *Légipresse* 2017. 494.

CJUE, 20 déc. 2017, aff. C-434/16, *Peter Nowak* c/ *Data Protection Commissioner* : chron. BONNEVILLE P., BROUSSY E., CASSAGNABERE H. et GÄNSER C., *AJDA* 2018. 329 ; obs. FAUVARQUE-COSSON B. et MAXWELL W., *D*. 2018. 1033.

CJUE, 29 juill. 2019, aff. n°C-40/17, *Fashion ID GmbH & Co.KG* c/ *Verbraucherzentrale NRW eV, Facebook Ireland Ltd* et autre : obs. LARRIEU J., LE STANC C. et TREFIGNY P., *D*. 2019. 1604 ; *D*. 2019. 2266 ; obs. DOUVILLE T., *Dalloz IP/IT* 2020. 126 ; *Légipresse* 2019. 448 ; obs. DROUARD E. et BEAUFOUR J., *Légipresse* 2019. 613 ; obs. BENOIT-ROHMER F., RTD *eur*. 2020. 319.

CJUE, 1er oct. 2019, aff. C-673/17, *Planet 49* : note PEYROU S., Eur., 2020, n°1, pp ; 210 à 219. D. 2019, 1884 ; entretien SAURON, *D*. 2019. 2128 ; obs. Crichton, *Dalloz IP/IT* 2019. 586 ; ét. THIERACHE et GAUTRON Légipresse 2019. 694 ; ét. PERRAY et ADDA, *CCE* 2020. 13.

CJUE, 11 nov. 2020, aff. C -1/19, *Orange România* : comm. COSTES L., *RLDI* 2020 n°176, p. 29 : comm., SIMON D., *Europe*, 2021, n°1, p. 14 ; chron. BERTRAND B., *RTDE*, n°1, pp. 143-145 ; chron., CALANDRI L., *JCP A*, 2021, n°21, pp. 24 à 25 ; SAURON J.-L., LONG M., PARAVANO L., *JCP A*, 2021, n°3, pp. 13 à 20 ; GAYREL C., *Journal de droit européen*, n°275, pp. 29 à 35.

CJUE, Trib., 10 nov. 2021, aff. T. 612/17, *Google LLC, Alphabet, Inc c/ Comm. UE (Google shopping)* : comm. MASMI-DAZI F., *D.* act., 2021 ; comm. BERLEMONT J., *ADD*, 2021 ; RONZANO A., *Concurrences*, 2022 n°1.

3. Commission européenne

Commission européenne, 19 févr. 2008, aff. M. 4726, aff. *Thompson corporation/Reuters Group*, SG-Greffe(2008) D/200711 : comm. GIRGENSON I. et BURE (de) F., *RLC* 2008 n°17 p. 13**.**

Commission européenne, déc., 11 mars 2008, aff. COMP/M.4731, *Google c/ DoubleClick*, C(2008) 927 final : note PHILIPPE J. et TRABUCCHI M., *LGP* 2010 n°281 p. 10 ; comm. BURE F., LAPREVOTE F.-C et DUPREY J.-S, *RLC* 2008 n°16 p. 11.

Commission européenne, 14 mai 2008, aff. COMP/M.4854, *TomTom c/Tele Atlas*, C(2008) 1859 : comm. LAPREVOTE F.-C., BURE (de) F. et PAROCHE E. *RLC* 2009 n°18 p. 15.

Commission européenne, 18 févr. 2010, aff. COMP/M.5727, *Microsoft c/ Yahoo! Search business*, C(2010) 1077 : comm. HULL D. et THEOPHILE D., *Concurrences* 2010 n°3 p. 121; note BURE (de) F., *RLC* 2010 n°24 p. 12 ; note PHILIPPE J. et TRABUCCHI M., *LGP* 2010 n°281 p. 10.

Commission européenne, 4 sept. 2012, aff. COMP/M.6314, *Telefonica/Vodafone/Everything EveryWhere*, C(2012) 6063 final : note BILLARD O., *Concurrences* 2013 n°2 p. 111.

Commission européenne, 25 juin 2014, aff. COMP/M.7137, *EDF c/ Dalkia en France*, C**(2014) 4438 final.**

Commission européenne, 3 oct. 2014 aff. COMP/M.7217, *Facebook/Whatsapp*, C(2014) 7239 final : note VERNEY C., *RLC*, 2015, n°42, p. 24.

4. Cour européenne des droits de l'Homme

CEDH., Cour (pleinière), 26 juin 1986, aff. *Van Marle et autres c/ Pays-Bas*, n°8543/79 et autres : note TAVERNIER P., *JDI*, n°1987-3, pp. 785 à 787.

CEDH, 5 janv. 2000, *Beyeler c/ Italie*, n°33202/96 : note RUDOLF B., *American Journal of international law*, 2000, n°94-4, pp. 736 à 740 ; note LECHEVALLIER V., *Europe*, 2002, n°8, p. 35 ; BALLIF G., *LPA* 2001, n°103, pp. 15 à 22 ; TAVERNIER P., *JDI* 1993, n°2, pp. 579 à 580.

CEDH, 30 juin 2009, n°32772/02, *Verein gegen Tierfabriken Schweiz* c/ *Suisse [GC]* : obs. SUDRE, *JCP* 2008, I., 110, n°1.

CEDH, 22 avr. 2013, n°48876/08, *Animal Defenders International* c/ *Royaume-Uni [GC]* : obs. LAVRIC S., Dalloz actualité, 29 avr. 2013 ; chron. BURGORGUE-LARSEN L., AJDA 2013. 1794, AJDA/CHRON/2013/0468 ; Légipresse 2013. 402.

CEDH, 16 juill. 2014, *aliae et autres c/ Bosnie-Herzégovine, Croatie, Serbie, Slovénie et l'ex-République yougoslave de Macédoine*, n°60642/08.

CEDH., 16 nov. 2018, aff., *Könyv-Tar KFT et autres c/ Hongrie* : req. n°21623/13.

Index

A

Abus de confiance 367 et s
Abus de position dominante 200, 283
Accès aux données agricoles privées 107
  Mise en oeuvre 151 et s
Accessibilité 43 et s
Acquisitions 195
Altruisme en matière de données 491
Anonymisation 767 et s
  Conditions 769 et s
  Effets 773 et s
  Mise en oeuvre 776 et s
  Privacy by design 767
  Risques de réidentification 784 et s

B

Bien public
  Notion 52 et s
Biens
  Appropriation 505 et s
  Caractères du droit de propriété 506 et s
  Catégorie 508 et s
  Exclusion des données 512 et s

C

CASD 475 et s
Choses immatérielles 520 et s
  Originalité 524 et s
Clause abusive 653 et s
Clause d'exclusivité 471
  Efficacité 472
Clause de confidentialité 339 et s
Clause de responsabilité 473
Co-contractant générateur de la donnée
  Notion 611 et s
Collecte 84 et s
  - à des fins de recherche 461 et s
  Données privées 138 et s
  Réseaux d'observation 462
Communs scientifiques 62
Concentrations 196 et s
Consentement 740 et s
  Effets 748 et s
  Limites 753 et s
  Notion 742 et s
  Recueil du consentement 741 et s
  Risques de l'utilisation comme base légale 762
Contrôle de l'usage 501 et s
  Clause de propriété 578 et s
  Contours du droit 606 et s
  Contractualisation 54 et s, 634 et s
    Inefficicence 577 et s
    Limites 566 et s
    Principe 545 et s
  Contrôle de l'équilibre contractuel 581 et s
  Débiteur de l'obligation 615
  Données à caractère non personnel 590 et s
  Données enrichies
    Exclusion 621 et s
  Fondements 592 et s
  Maîtrise des données 617 et s
  Mise en oeuvre 660 et s
  Objet du droit 616 et s
  Obligations des détenteurs de données 636 et s
  - Par l'exploitant agricole 588 et s
  Principe 591 et s
  Renforcement des droits des utilisateurs 646 et s
  Tiers de confiance 474 et s
  Titulaire du droit 608 et s
Création originale
  Données traitées ou analysées 523

D

Déséquilibre contractuel

Contrôle 651 et s
Déséquilibre significatif
Contrôle 320 et s
Devoir d'information précontractuel 637 et s
Devoir de loyauté 317 et s
Dividende de la donnée 626
Donnée publique
Notion 48 et s
Données
Caractères 513 et s
Création de forme 519 et s
Originalité 526 et s
Propriété intellectuelle 518 et s
Valeur 515 et s
Données à caractère personnel 170 et s
Caractérisation de la personne physique 698 et s
Clauses contractuelles obligatoires 728
Distinction de vie privée 691 et s
Droit d'accès 171 et s
Exclusion nuancée de la personne morale 705 et s
Maîtrise de l'usage 682
Mise en oeuvre de la protection 711 et s
Notion 684 et s
Objet de la protection 683 et s
Obligation de sécurité 338 et s
Principe de licéité 713 et s
Régime 680
Responsabilité 719 et s
Responsable de traitement
Notion 720
Traitement 714 et s
Données agricoles privées 133 et s
Définition 134 et s
Origine 139 et s
Données agricoles publiques
Catégorie 49 et s
Données concurrentielles 179 et s
Données confidentielles 84 et s
Données d'exploitation
Contrôle de l'usage 502 et s
Droit de propriété
Absence 504 et s
Données d’intérêt général 50, 141 et s
Absence de définition 142
Accès 153 et s
Données de forte valeur 146 et s
Données de référence 104 et s
Données enrichies
Définition 622
Données environnementales 166 et s
Données industrielles 619
Données phytosanitaires 159 et s
Données privées
Absence de régime d'ouverture 449 et s
Accès limité 458 et s
Contrôle de l'accès 447 et s
Données privées en raison d’un besoin exceptionnel 149
Données saisies 620
Données scientifiques
Qualification 60
Régime 61 et s
Données sensibles d'exploitation 628 et s
Droit à la portabilité
Contenu 734 et s
Mise en oeuvre 736 et s
Droit à la réutilisation 415 et s
Droit d’accès 42 et s, 92 et s, 132 et s
Contenu 98 et s
Limites 112 et s
Droit de la concurrence 280 et s
Droit des bases de données 218 et s
Création de forme, 155
Droit d’auteur 220 et s
Droit sui generis 239 et s
Contenu 252 et s
Exceptions 258 et s
Investissement 241 et s
Licences d’utilisation
Contenu 292 et s
Oeuvre de compilation, 155
Droit des données à caractère personnel Voir Droit à la portabilité
Anonymisation Voir Anonymisation
Consentement Voir Consentement

Outil d'autodétermination informationnel 730 et s
Portabilité 733 et s
Solutions de traitement 739 et s
Droit souple 552 et s
Charte Data-Agri 558 et s
Code de conduite de l'Union européenne relatif au partage des données agricoles par accord contractuel 562 et s
Gestion des consentements 555 et s

E

Économie des contrats de l'agriculture numérique 466 et s
Enrichissement significatif 624
Entente concurrentielle
Caractérisation 494 et s
Définition 493
Établissements publics 80
État-plateforme 107 et s
Exception de TDM 463

F

Facilités essentielles 208 et s
Fichier numérique 525
Fouille de texte et de données 264 et s
Fusions 194

G

Générateur de la donnée 169 et s
Notion 614
Gestion des consentements Voir Consentement

I

Informations
Appropriation 511
Informations publiques 420 et s
Définition 421
Documents administratifs 421 et s
Notions
Limites 424 et s
Initiatives citoyennes 65
Instituts techniques agricoles 81
Interdiction de diffusion 127 et s
Interopérabilité 664 et s
Contenu 668 et s
Évolutions réglementaires 675 et s
Mise en oeuvre 671 et s
Standards ouverts 672 et s

L

Législation sur les marchés numériques 496 et s
Liberté contractuelle
Contenu 311 et s
Limites 315 et s
Principe 305 et s
Libre réutilisation
Périmètre 419 et s
Principe 410
Licence d'utilisation
Contrôle de l'accès 465 et s
Informations publiques 436 et s
Licences homologuées 438
Licences types 437
Réutilisation 431 et s

M

Marché en cause
Définition 182 et s
identification 181 et s
Marchés bifaces 281 et s
Marchés connexes 189
Marchés multifaces 188
Métadonnées 620
Modèles alternatifs de régulation 547 et s

O

Originalité
Notion 227 et s

P

Partage des données
- Définition 488
- Proposition de réglement sur les données 641 et s
- Solutions envisageables 498

Partage des données agricoles 479 et s
- Constat d'échec 482 et s
- Écosystème 298
- Organisation 481
- Régulation 485 et s

Patrimoine immatériel de l'État 54

Photographies 527

Plateformes
- Comportements déloyaux 492

Portage 529 et s
- Contenu 532 et s
- Interopérabilité 336, 536
- Limites 538 et s
- Mise en oeuvre 535 et s
- Principe 531 et s
- Principe de transparence contractuelle 536
- Titulaire du droit 534

Pouvoir de marché 185 et s

Prestataires d'intermédiation de données 490

Proposition de Règlement sur les données 84

Protection du droit d'auteur
- Contenu 232 et s

R

Réglement sur la gouvernance des données 486 et s
- Contenu 488 et s
- Objectifs 487

Réglement sur la libre circulation des données à caractère non personnel 451 et s

Règles contractuelles par défaut 656 et s

Réseau des chambres d'agriculture 82

Réservation contractuelle 304 et s

Réservation d'informations confidentielles 329 et s

Réservation de l'accès 303 et s

Réservation des données agricoles 217 et s

Réutilisation
- Conditions 430 et s
- Contrôle 439 et s
- Limite 428 et s
- Principe 426 et s
- Principe de gratuité 434 et s

Réutilisation des données agricoles privées
- Régulation 477 et s

S

Savoir-faire 528

Secret des affaires 346 et s

Secrets 114 et s
- Protection 332 et s

Sécurisation des données
- Responsabilité 399 et s

Service public
- Construction 102 et s
- Notion 69 et s

STAD (Système de traitement automatisé de données) 376 et s
- Caractères 390 et s
- Notion 385 et s
- Régime 383 et s
- Répression 377 et s, 393 et s

T

Théorie des infrastructures essentielles 206 et s

U

Usage
- Contrôle de l'accès par le contrat 469 et s
- Maîtrise de l'usage 407 et s

Utilisateur
- Notion 609 et s

Utilisateur légitime 284 et s

V

Vie privée 121 et s

Vol de données 371 et s

Plan analytique

Remerciements **2**

Sommaire **3**

Liste des principales abréviations **4**

Introduction **9**

I. L'avènement des données dans l'agriculture numérique 11

A. Le numérique : le nouveau moteur de l'agriculture 11

1. L'aubaine du numérique pour répondre aux défis de l'agriculture 12

2. Les points de vigilance du développement du numérique pour les défis de l'agriculture 14

B. Les données : le carburant de l'agriculture numérique 15

1. Les difficultés d'appréhension de la notion de donnée 15

2. La circonscription de la recherche aux données agricoles 21

C. Les personnes gravitant autour des données agricoles 22

1. La notion de détenteur de données 22

2. La notion d'utilisateur de données 23

3. Les notions de producteur et de collecteur de données 24

II. L'appréhension laborieuse du cadre juridique des données agricoles 24

A. L'évolution empirique de la législation sur les données agricoles 25

1. L'appréhension de la donnée par le droit français 25

2. La volonté de créer un marché européen des données 29

B. Les effets du puzzle du droit des données 31

1. Les injonctions législatives sur les données 31

2. La part d'autorégulation sur l'exploitation des données agricoles 32

III. L'élaboration d'un cadre adapté aux données agricoles 32

Partie I. L'accessibilité des données agricoles **37**

Titre I. L'accès aux données agricoles : l'émergence d'un droit d'accès pour l'agriculteur **38**

Chapitre 1. L'accessibilité des données agricoles publiques 39

Section 1. La notion de données agricoles publiques 39

§1. La qualification des données agricoles publiques 39

I. La caractérisation des données publiques 39

A. La définition de données publiques 39

1. La spécificité des « données publiques » 40

2. L'étendue de la catégorie des données publiques 41
B. La nature juridique des données publiques 43
1. La notion de bien public 43
2. L'exclusion des données publiques de la catégorie des biens publics 45
II. La détermination des données agricoles publiques 49
A. Les données produites dans le cadre de missions de service public 49
1. Les données produites à des fins de statistiques 49
2. Les données produites à des fins d'information 50
B. Les données produites à des fins de recherche scientifique 52
1. La notion de données de la recherche scientifique 52
2. Le régime spécial des données de la recherche scientifique 53
3. Les initiatives citoyennes et participatives 58
§2. L'origine des données agricoles publiques 59
I. La production de données agricoles publiques dans le cadre d'une mission de service public 59
A. La notion de service public 59
1. La définition du service public 59
2. La caractérisation du service public 60
B. Les personnes en charge d'une mission de service public dans le secteur agricole 64
1. Les personnes publiques du secteur agricole 64
2. Les personnes privées en charge d'une mission de service public 68
II. La collecte de données agricoles privées dans le cadre d'une mission de service public 70
A. La mise à disposition obligatoire des données agricoles privées 71
1. La mise à disposition obligatoire des données agricoles privées à des fins de contrôle 71
2. La mise à disposition des données agricoles privées à des fins de statistiques publiques 72
B. L'accès limité des données agricoles privées 72
Section 2. La mise en œuvre de l'ouverture des données agricoles publiques 73
§1. Le principe du droit d'accès aux données agricoles publiques 74
I. Le droit d'accès 74
A. La construction du droit d'accès aux données publiques 74
1. La théorie du droit d'accès 74
2. La reconnaissance du droit d'accès 75
B. La mise en œuvre du droit d'accès 76
1. Le contenu du droit d'accès 76
2. Les conditions de l'accès 77
II. La construction d'un service public d'ouverture de la donnée 79
A. Les effets de la création d'un service public de la donnée 79
1. Les enjeux de la reconnaissance d'une mission de service public de la donnée 79

2. Les conséquences de la création d'un service public de la donnée sur le régime de l'ouverture des données publiques 80
B. Le prélude de l'État-plateforme 81
1. La mutation du service public 81
2. La notion d'État-plateforme 82
§2. Les limites du droit d'accès aux données agricoles publiques 83
I. Les exceptions à la communication des données 83
A. Les données non communicables en raison d'un secret 83
1. Les données non communicables au public 84
2. Les données non communicables aux tiers 84
B. L'exception du droit de propriété intellectuelle sur les données agricoles publiques 86
1. Le droit de propriété intellectuelle détenu par les tiers 86
2. L'inopposabilité des droits de propriété intellectuelle détenus par les administrations 88
II. La privatisation des données 91
A. La protection de la vie privée 91
1. Le jeu d'équilibriste entre deux régimes initialement opposés 91
2. La primauté de la protection des données personnelles et de la vie privée sur l'ouverture des données publiques 92
B. L'obstacle à la diffusion des données publiques 94
1. L'interdiction de diffusion 94
2. Les conditions d'accès limitées 95
Chapitre 2. L'accessibilité des données agricoles privées 97
Section 1. L'objet du droit d'accès : les données faisant l'objet d'une réservation privative 97
§1. La qualification des données agricoles privées 97
I. La définition des données agricoles privées 98
A. L'absence de définition des données privées 98
B. Le concept de données privées 98
II. La provenance des données agricoles privées 99
A. La collecte et la production des données par les sociétés de l'agriculture numérique 99
B. L'origine des données agricoles privées 101
§2. L'hétérogénéité des données agricoles privées 102
I. Les données d'intérêt général 102
A. L'absence de définition des données d'intérêt général 102
B. L'étendue de la catégorie des données d'intérêt général 104
II. La création de nouvelles catégories de données par le législateur européen 104
A. La future catégorie des données de forte valeur 104
1. La définition des ensembles de données de forte valeur 105
2. Les conditions d'ouverture des ensembles de données à forte valeur 105

B. La proposition de mise à disposition des données privées en raison d'un besoin exceptionnel 106
Section 2. La mise en œuvre de l'ouverture de l'accès aux données agricoles privées 107
§1. La reconnaissance de l'accès aux données privées selon leur objet 107
I. L'accès aux données d'intérêt général : une future consécration légale ? 108
A. La création d'un régime d'ouverture des données privées d'intérêt général 108
1. Les tentatives échouées de création d'un régime d'ouverture des données d'intérêt général 108
2. L'opportunité de la création d'un régime d'ouverture des données d'intérêt général 110
B. L'exemple de l'ouverture des données phytosanitaires 112
1. La mise à disposition des données phytosanitaires pour la réalisation d'une mission de service public 113
2. La reconnaissance de l'ouverture des données phytosanitaires pour l'intérêt général ou commun 117
II. La consécration du droit d'accès du générateur de la donnée 122
A. L'accès entériné aux données à caractère personnel de l'agriculteur 122
1. Le principe du droit d'accès aux données à caractère personnel 123
2. Les limites du droit d'accès aux données à caractère personnel 123
B. La consécration du droit d'accès de principe aux données non personnelles du générateur de données 124
1. Le fondement du droit d'accès 124
2. Les contours du principe légal de l'accès 128
§2. L'éventuelle consécration de l'accès aux données selon leur intérêt concurrentiel 129
I. L'accès aux données agricoles : le nouvel enjeu du droit de la concurrence 130
A. L'identification du marché en cause 130
1. La définition du marché en cause 131
2. La détention des données comme source de pouvoir de marché 132
B. La répression des atteintes à l'accès aux données sur le marché des données agricoles 137
1. Les comportements anticoncurrentiels quant à l'accès aux données 137
2. Les sanctions des atteintes à la concurrence 144
II. La théorie des infrastructures essentielles au soutien des politiques de partage 145
A. La régulation du marché en cause par le droit d'accès aux données essentielles 145
1. Les données comme facilités essentielles 145
2. La reconnaissance jurisprudentielle des données comme facilités essentielles 147
B. Les limites de la théorie des facilités essentielles appliquée aux données agricoles 148
1. Le caractère non rival des données agricoles 149
2. L'impact du développement de nouvelles technologies 149

Titre II. La réservation privative des données agricoles : l'organisation de l'exclusivité par les entreprises 152

Chapitre 1. La réservation de l'accès aux données agricoles protégées 153

Section 1. Le principe de la protection duale des bases de données 153

§1. La protection des bases de données originales par le droit d'auteur 154

I. Les conditions de la protection des bases de données par le droit d'auteur 154

A. Création de forme: la base de données 154

1. La notion d'œuvre de compilation 154

2. La base de données 155

B. Création originale : originalité de la structure de la base 156

1. La notion d'originalité 156

2. L'appréciation de l'originalité sur la base 157

II. Le contenu de la protection du droit d'auteur 160

A. L'étendue du droit d'auteur 161

1. Les droits patrimoniaux 161

2. Les droits moraux 162

B. Les exceptions spécifiques du droit d'auteur 162

1. L'exception de copie privée 162

2. L'exception relative à l'accès aux bases de données 163

§2. La protection des bases de données agricoles par le droit sui generis 163

I. Les bénéficiaires du droit *sui generis* 164

A. Condition d'application du droit *sui generis* : l'investissement 164

1. L'objet du droit sui generis : le contournement de la condition d'originalité 165

2. La notion d'investissement 166

B. La caractérisation de l'investissement substantiel 166

1. L'existence d'un investissement 167

2. L'existence d'un investissement substantiel 172

II. Le contenu du droit *sui generis* 173

A. Les droits du producteur sur la base de données 173

1. Les interdictions d'extraction ou de réutilisation 173

2. L'étendue de l'extraction ou de la réutilisation 176

B. Les exceptions au droit *sui generis* 179

1. L'extraction ou la réutilisation d'une partie non substantielle 179

2. L'extraction à des fins privées 180

3. La consultation par des personnes handicapées 180

4. La consultation à des fins pédagogique ou de recherche 181

5. La fouille de textes et de données 182

Section 2. Les effets sur l'organisation de l'accès aux bases de données protégées 185

§1. L'indisponibilité relative des données pour les tiers 186
I. Le principe de la réservation du contenu de la base pour le titulaire des droits 187
A. La réservation des données incluses dans les bases 187
1. L'évolution législative sur la réservation du contenu de la base de données 187
2. L'appropriation indirecte des données 188
B. Les effets d'appropriation des bases de données 188
1. La maîtrise monopolistique des bases de données étendue aux données elles-mêmes 189
2. Le maintien de l'absence de droit de propriété sur les données 189
II. Les limites externes à la réservation des bases de données 190
A. La future consécration de l'exclusion des données industrielles de la protection par le droit *sui generis* 191
1. L'ouverture de l'accès pour les utilisateurs d'objets connectés 191
2. L'ouverture de l'accès pour les tiers 191
B. L'impact du droit de la concurrence sur la réservation des bases de données 192
1. Les marchés bifaces dans l'agriculture numérique 192
2. La caractérisation de l'abus de position dominante sur le marché biface 194
§2. La pleine disponibilité des données pour l'utilisateur légitime 197
I. L'accès licite aux bases de données protégées 197
A. L'organisation de l'accès aux bases de données protégées 197
1. L'obtention de l'accès pour l'utilisateur légitime 197
2. La mise à disposition de la base de données 198
B. Les modalités de l'accès aux bases de données de l'agriculture numérique 199
II. Le contenu des licences d'utilisation 199
A. Les droits de l'utilisateur légitime 200
1. Le contenu des droits de l'utilisateur légitime 200
2. Les limites aux droits de l'utilisateur légitime 200
B. Les obligations du producteur sur la base de données 201
1. Une obligation prétorienne 201
2. Le contenu de l'obligation d'interdire l'utilisation de la base 201
Chapitre 2. La réservation de l'accès aux données agricoles non protégées 204
Section 1. La réservation contractuelle de l'accès aux données agricoles 204
§1. Le contenu du principe de la liberté contractuelle appliqué aux contrats de l'agriculture numérique 205
I. Le principe de la liberté contractuelle appliqué aux contrats de l'agriculture numérique 205
A. Le principe de la liberté contractuelle sur les bases de données non protégées 205
1. L'affaire Ryanair c/PR Aviation 206
2. Le bénéfice de la liberté contractuelle sur l'accès aux bases de données 207

B. Les effets de la liberté contractuelle sur les bases de données non protégées 207
1. Le contenu de la liberté contractuelle 207
2. Les conséquences de la liberté contractuelle sur l'accès aux bases de données 208
II. Les limites de la liberté contractuelle sur les contrats de l'agriculture numérique pour l'accès aux données 209
A. Les obligations liées à l'exécution du contrat 209
1. Le principe du devoir de loyauté dans les contrats de l'agriculture numérique 210
2. L'étendue du devoir de loyauté dans les contrats de l'agriculture numérique 210
B. Le contrôle du déséquilibre significatif dans les contrats de l'agriculture numérique 212
1. Le domaine d'application des droits spéciaux et du droit commun du déséquilibre significatif 212
2. Le contrôle du déséquilibre significatif dans les contrats de l'agriculture numérique 214
§2. Le contenu du contrat, la réservation d'informations confidentielles 217
I. Le principe de la protection des informations sensibles 219
A. La protection légale limitée des informations sensibles 219
1. Les secrets pénalement répréhensibles 219
2. L'obligation civile de confidentialité 221
3. L'obligation de sécurité des données à caractère personnel 221
B. La clause de confidentialité 222
1. Le secret protégé par le contrat 223
2. La rédaction de la clause de confidentialité 224
II. La reconnaissance légale du secret des affaires 225
A. La protection du secret des affaires 225
1. Une notion nouvelle 225
2. La récente réglementation portant sur les secrets d'affaires 226
B. La mise en œuvre du secret des affaires 228
1. Les conditions d'application du secret des affaires 228
2. Les effets de la violation du secret des affaires 234
Section 2. La sécurisation technique de l'accès aux données agricoles contre les actions des tiers 238
§1. Le principe légal de la protection contre les atteintes aux données 238
I. La répression pénale de l'atteinte aux données 238
A. L'abus de confiance 238
1. L'incrimination de l'abus de confiance 238
2. La prise en compte des choses corporelles 239
B. Le vol de données 240
1. La condition initiale de soustraction d'un élément matériel 240
2. Le vol de données sans support matériel 241
II. La reconnaissance légale de l'atteinte spécifique aux données 244

A. La répression de l'intrusion et de l'entrave à un STAD 244
1. Le contexte de la répression de l'intrusion et de l'entrave à un STAD 244
2. La reconnaissance légale de la répression de l'intrusion et de l'entrave à un STAD 244
B. L'extension de la répression de l'atteinte à un STAD au délit d'extraction des données 245
1. Répression de l'extraction de données 245
2. Répression des comportements délictueux en matière de données 246
§2. Le régime juridique de la protection contre les atteintes aux données 246
I. L'identification d'un système de traitement automatisé de données 247
A. La notion de STAD 247
1. La définition d'un STAD 247
2. Les contours de la notion de STAD 248
B. La caractérisation des STAD 249
1. Les caractéristiques du STAD 249
2. Le dispositif de sécurité non exigé 249
II. La répression des atteintes au STAD 250
A. Les comportements répréhensibles sur les STAD 250
1. L'accès ou le maintien frauduleux dans un STAD 250
2. L'atteinte ou l'entrave à un STAD 251
3. L'action frauduleuse sur les données d'un STAD 252
4. La détention ou l'offre d'un dispositif permettant la réalisation d'une atteinte à un STAD 252
B. La responsabilisation des entreprises de l'agriculture numérique sur la question de la sécurisation des données 253
1. La responsabilité légale 253
2. L'obligation de sécurisation 254

Partie II. La maîtrise de l'usage des données agricoles 257

Titre I. L'absence regrettée de contrôle de l'usage des données d'exploitation 259

Chapitre 1. L'absence de contrôle par l'agriculteur de l'usage des données d'exploitation non personnelles 260
Section 1. La libre réutilisation des données publiques d'exploitation 260
§1. Le principe de la libre réutilisation des données publiques 260
I. L'avènement du principe de la liberté de réutilisation 261
A. La consécration du principe de la liberté de réutilisation 261
1. L'introduction de la notion de réutilisation 261
2. La création d'un véritable droit à la réutilisation 262
B. Le fondement économique du droit de réutilisation 263
1. Le développement économique 263

2. Le fondement de la liberté du commerce et de l'industrie 263
II. Le périmètre de la liberté de réutilisation 264
A. Les informations publiques 264
1. Le lien entre informations publiques et documents administratifs 265
2. Les limites de la notion d'informations publiques 266
B. La réutilisation 267
1. Le principe de la réutilisation 267
2. La limite de la réutilisation : la protection des données et des personnes 268
§2. Les conditions de réutilisation des données publiques 269
I. Les contours de la réutilisation des données publiques dans les licences d'utilisation 269
A. L'existence conditionnée de la licence 270
1. Les conditions d'utilisation de la licence 270
2. Le principe de la gratuité de la réutilisation des données publiques 270
B. Les licences d'utilisation 274
1. Les licences types 274
2. Les licences homologuées 275
II. Le contrôle de la réutilisation des données publiques 276
A. Le contrôle contractuel 276
1. Le contenu des licences 276
2. Les contraintes de la licence 277
B. Le contrôle judiciaire 277
1. Les actes incriminés 278
2. Les sanctions 278
Section 2. La maîtrise de l'usage des données privées d'exploitation par le contrôle de l'accès 279
§1. La fermeture de l'accès aux données d'exploitation privées pour le contrôle de l'usage 279
I. L'absence de régime d'ouverture des données d'exploitation privées 279
A. Le silence de la loi sur l'accès aux données d'exploitation privées 279
1. L'apport limité du Règlement européen au sujet de la circulation des données privées 280
2. Le manque d'effectivité du règlement 282
B. Les restrictions d'accès aux données d'exploitation privées pour les tiers : l'exemple de la recherche scientifique 283
1. L'absence de mise à disposition des données pour la recherche scientifique 283
2. Les méthodes limitées de collecte des données à des fins de recherche 285
II. L'organisation de l'accès ouvert aux données privées 288
A. Le contrôle de l'accès des données privées par la licence d'utilisation 288
1. L'accès aux données dans l'économie des contrats de l'agriculture numérique 289
2. Les effets du contrôle de l'accès contractuel sur l'usage 290

B. Le contrôle de l'accès et de l'usage des données confidentielles par un tiers de confiance 294
1. Le Centre d'accès sécurisé aux données 294
2. Les modalités d'accès aux données confidentielles par le Centre d'accès sécurisé aux données 295
§2. La régulation de la réutilisation des données agricoles privées 296
I. Le constat d'échec du partage des données privées non personnelles dans le secteur agricole 297
A. Les nombreuses initiatives du partage des données non personnelles 297
1. L'écosystème du partage des données agricoles 297
2. L'organisation du partage des données dans le secteur agricole 298
B. Les raisons supposées de l'échec du partage des données privées non personnelles 300
1. Le manque de concertation des acteurs du secteur agricole 300
2. Les initiatives pour l'amélioration du partage des données agricoles 301
II. La régulation du partage des données privées non personnelles 302
A. Le règlement sur la gouvernance des données 302
1. Les objectifs du règlement sur la gouvernance des données 302
2. Le contenu du règlement sur la gouvernance des données 304
B. La régulation des comportements déloyaux des plateformes 306
1. Les comportements anticoncurrentiels des entreprises lors du partage des données 307
2. Le Digital Markets Act 309
3. Solutions envisageables pour l'organisation du partage des données agricoles 311
Chapitre 2. Le développement du contrôle de l'usage des données non personnelles d'exploitation par l'agriculteur 314
Section 1. Le silence de la loi sur le contrôle de l'usage des données d'exploitation 314
§1. L'absence de dispositif légal de contrôle de l'usage des données d'exploitation 314
I. L'inadaptation du droit de propriété aux données d'exploitation 314
A. Le principe de l'appropriation des biens 315
1. Les caractéristiques du droit de propriété 315
2. La catégorie extensible et malléable des biens 316
B. L'exclusion des données de la catégorie des biens 318
1. Les caractères non rival et reproductible des données 318
2. L'absence de valeur intrinsèque de la donnée 320
II. La difficile appréhension des données par le droit de la propriété intellectuelle 324
A. La création de forme : les données 324
1. Les choses immatérielles 324
2. Les données, des choses immatérielles ? 326
B. La création originale, les données traitées ou analysées ? 326

1. L'originalité des choses immatérielles 326
§2. L'inefficience du portage des données sur la maîtrise de l'usage 332
I. Le portage, outil réglementaire de la circulation des données 333
A. Le principe du portage 333
1. Le contenu du portage 333
2. Les titulaires du droit de portage 334
B. La mise en œuvre du portage 334
1. Le principe de transparence contractuelle 335
2. Le principe d'interopérabilité des systèmes 335
II. Le portage des données : entre manque de cohérence et insécurité juridique 336
A. L'incohérence des régimes de traitement des données 336
1. Le manque d'harmonisation entre les réglementations sur les données 336
2. Des outils de portée différente 337
B. L'insécurité juridique 337
Section 2. La contractualisation du contrôle de l'usage des données brutes d'exploitation non personnelles 338
§1. Le principe de la contractualisation du droit de contrôle de l'usage 338
I. La source contractuelle du droit de contrôle de l'usage 339
A. Le développement des modèles alternatifs de régulation 339
1. Les notions d'autorégulation et de co-régulation 339
2. L'intérêt des modèles alternatifs de régulation 340
B. L'émergence du droit souple dans le secteur agricole 341
1. Les textes déontologiques du secteur agricole 342
2. Les outils techniques pour la gestion des consentements 343
II. La création d'un cadre contractuel par le droit souple pour le contrôle de l'usage des données brutes non personnelles 344
A. L'apport de la Charte Data-Agri 345
1. Le contenu de la Charte Data-Agri 345
2. La mise en œuvre du droit de contrôle de l'usage 346
B. L'apport du Code de conduite de l'Union européenne relatif au partage des données agricoles par accord contractuel 347
1. Le contenu du Code de conduite 347
2. La mise en œuvre du contrôle de l'usage 348
§2. Les limites de la contractualisation du droit de contrôle de l'usage 351
I. La portée limitée du droit souple 351
A. L'absence de contrainte 351
1. Des sanctions non juridiques 351
2. Une faible participation volontaire des acteurs 352

B. Les risques de confusion 352
1. L'hétérogénéité des textes 352
2. Le manque de clarté des textes 354
II. L'inefficience du droit des contrats sur le contrôle de l'usage des données d'exploitation 355
A. Le mirage de la clause de propriété 355
1. Une clause inventée par la pratique 355
2. Une clause inefficiente 356
B. L'inefficacité du contrôle de l'équilibre contractuel sur l'usage des données agricoles 357
1. L'absence de contrôle de l'usage des données agricoles 357
2. Le devoir d'information sur l'usage des données 358

Titre II. La maîtrise envisagée de l'usage des données d'exploitation par l'exploitant agricole 361

Chapitre 1. La consécration souhaitée du droit de contrôle de l'usage des données d'exploitation à caractère non personnel 363
Section 1. Le principe du droit de contrôle de l'usage des données d'exploitation non personnelles 363
§1. Les fondements du droit de contrôle de l'usage des données d'exploitation non personnelles 363
I. L'accroissement de la sécurité juridique 364
A. Le renforcement de la maîtrise de l'usage des données non personnelles 364
1. Contrer le contrôle factuel de l'usage par les entreprises détentrices 364
2. Assurer l'autonomie des agriculteurs 365
B. L'harmonisation des normes d'usage sur les données non personnelles 365
II. L'amélioration de la circulation des données non personnelles 366
A. Favoriser la concurrence 367
1. Faciliter les transferts des données à d'autres fournisseurs de services 367
2. Favoriser les possibilités de multidomiciliation 368
B. Le renforcement de la maîtrise de l'usage des données non personnelles 368
1. Récupérer des données générées par les objets connectés 368
2. Rééquilibrer l'asymétrie de pouvoirs entre utilisateurs et services de l'économie numérique 369
§2. Les contours du droit de contrôle de l'usage des données d'exploitation 369
I. Le titulaire et le débiteur du droit de contrôle de l'usage des données d'exploitation 369
A. Le titulaire du droit de contrôle de l'usage 370
1. La notion d'« utilisateur » retenue par la Commission européenne 370
2. La notion envisagée de co-contractant générateur de la donnée 371
B. Le débiteur de l'obligation 373
II. L'objet du droit de contrôle de l'usage des données d'exploitation 373
A. La circulation et la maîtrise des données selon leur niveau d'enrichissement 374
1. L'inclusion de principe des données brutes, des données saisies et des métadonnées 374

2. L'exclusion des données enrichies 375
B. La protection des données sensibles d'exploitation 380
1. Les données sensibles d'exploitation 380
2. Les données non protégées 382
Section 2. L'esquisse du droit de contrôle de l'usage des données d'exploitation non personnelles 383
§1. Les aspects contractuels du contrôle de l'usage 384
I. Les mesures visant à renforcer les droits et les obligations des parties 384
A. Le renforcement des obligations des « détenteurs de données » 385
1. Le devoir d'information précontractuel 385
2. Les obligations liées à l'utilisation et au partage des données 387
B. Le renforcement des droits des « utilisateurs » 389
1. Le principe des droits de l'utilisateur 389
2. Les limites des droits de l'utilisateur 390
II. Les mesures visant à prévenir les abus de déséquilibre contractuel 391
A. Le contrôle des clauses contractuelles 391
1. Les clauses abusives 391
2. L'adoption de règles contractuelles par défaut 393
B. La mise en œuvre du contrôle du droit d'utilisation et de partage des données non personnelles 396
1. La désignation d'une autorité compétente nationale 396
2. Les sanctions du non-respect de la réglementation 396
§2. Les aspects techniques du contrôle de l'usage 397
I. L'interopérabilité des systèmes d'information et des services 397
A. Les enjeux de l'interopérabilité 397
1. La lente consécration du droit à l'interopérabilité des données non personnelles 397
2. Les obstacles dans l'appréhension de la notion d'interopérabilité 400
B. Le contenu de l'interopérabilité 401
1. L'étendue de l'interopérabilité 401
2. Les spécifications techniques des standards ouverts 402
II. La mise en œuvre de l'interopérabilité 403
A. L'élaboration de standards ouverts par les acteurs du secteur agricole 403
1. Les développements du secteur agricole sur l'interopérabilité des données des exploitations 403
2. Les limites de l'interopérabilité dans le secteur agricole 404
B. Les futures exigences réglementaires en matière d'interopérabilité 405
1. Le contenu des exigences d'interopérabilité 405
2. Mise en œuvre de l'interopérabilité dans l'Union européenne 406

Chapitre 2. La consécration actée du droit de contrôle de l'usage des données d'exploitation à caractère personnel 408
Section 1. La maîtrise de l'usage des données à caractère personnel de l'exploitation agricole 410
§1. L'objet de la protection : les données à caractère personnel de l'exploitation agricole 411
I. La notion de données à caractère personnel 411
A. La qualification de données à caractère personnel 411
1. Toute information se rapportant à une personne physique 411
2. Une identification directe ou indirecte 413
B. La distinction des notions de vie privée et de données à caractère personnel 413
1. Vie privée et protection des données à caractère personnel 414
2. Caractère autonome de la protection des données personnelles 415
II. La condition *sine qua non* de la protection : l'identification d'une personne physique 417
A. La caractérisation d'une personne physique 417
1. Les éléments d'identification d'une personne physique 417
2. Les données identifiantes du secteur agricole 419
B. L'exclusion nuancée des données de la personne morale 421
1. Une exclusion de principe 421
2. Une exclusion limitée 422
§2. La mise en œuvre de la protection des données à caractère personnel 423
I. La responsabilisation des entreprises de l'*AgTech* en tant que responsables de traitement 423
A. Le principe de licéité de l'opération de traitement 424
1. Le traitement des données à caractère personnel 424
2. La cause licite du traitement 426
B. Une responsabilisation renforcée des responsables de traitement 427
1. La notion de responsable de traitement 428
2. Les obligations à la charge du responsable de traitement 429
II. Des droits accrus pour l'agriculteur en tant que personne concernée 433
A. Un outil d'autodétermination informationnel 433
1. L'étendue des droits sur les données personnelles 433
2. Des droits propres à la personne concernée 434
B. La portabilité : un outil de renforcement de la maîtrise juridique sur les données à caractère personnel 434
1. Le contenu du droit à la portabilité 435
2. La mise en œuvre du droit à la portabilité 437
Section 2. Les solutions de traitement des données à caractère personnel issues des exploitations agricoles 438
§1. Le recueil du consentement 439
I. Les principes du recueil du consentement 439

A. La notion de consentement 439
1. La définition du consentement 439
2. Les caractères du consentement 440
B. Les effets du consentement 441
1. Le contrôle de la personne concernée sur ses données à caractère personnel 442
2. L'effectivité du contrôle sur les données à caractère personnel 442
II. Les écueils du recueil du consentement 445
A. Les difficultés liées au recueil du consentement 445
1. L'écueil d'un consentement libre 445
2. L'incompatibilité du consentement libre et du contrat 447
B. Les risques de l'utilisation du consentement comme base légale 449
1. Les risques pour le responsable de traitement 449
2. Les risques pour la personne concernée 449
§2. L'anonymisation, une solution risquée pour le traitement des données personnelles des agriculteurs 450
I. Les solutions techniques d'anonymisation 451
A. Les conditions de l'anonymisation 451
1. La non-identification des données anonymes ou anonymisées 452
2. Le caractère irréversible de l'anonymisation 452
B. Les effets de l'anonymisation 453
1. L'exclusion des données anonymisées du RGPD 453
2. La requalification en données à caractère non personnel 454
II. Les difficultés de mise en œuvre des techniques d'anonymisation 454
A. Les contraintes des méthodes d'anonymisation 455
1. Des techniques d'anonymisation complexes 455
2. Le paradoxe de l'anonymisation des données personnelles 456
B. L'efficacité relative des méthodes d'anonymisation 457
1. Les risques de réidentification 457
2. Les restrictions des techniques d'anonymisation : la mort annoncée de l'anonymisation ? 459

Conclusion ***463***

Bibliographie ***470***

Table de jurisprudence ***494***

Index ***509***