UNIVERSITE MONTPELLIER I
FACULTE DE DROIT

Année : 2010

N° attribué par la bibliothèque :

THESE

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITE MONTPELLIER I

Discipline : DROIT PRIVE ET SCIENCES CRIMINELLES

présentée et soutenue publiquement par :

Sophie BARDOU

le : Vendredi 5 Novembre 2010

Titre :

LES TRAITEMENTS DE DONNEES BIOMETRIQUES EN ENTREPRISE

Directeur de thèse :

Nathalie MALLET-POUJOL,

Directrice de recherche au CNRS, ERCIM, UMR-5815, Université Montpellier I

Jury :

Mme Marie-Christine PIATTI, Professeur à l'Université Lumière Lyon II, rapporteur

Mme Agnès MAFFRE-BAUGE, Maître de conférences à l'Université d'Avignon et des pays de Vaucluse, rapporteur

Mme Agnès ROBIN, Maître de conférences à l'Université Montpellier I

« La faculté n'entend donner aucune approbation ni improbation aux opinions émises dans cette thèse ; ces opinions doivent être considérées comme propres à leur auteur ».

LISTE DES PRINCIPALES ABREVIATIONS

Al.	Alinéa
Art.	Article
BO	Bulletin Officiel
Bull.	Bulletin des arrêts de la Chambre civile de la Cour de cassation
Bull. crim	Bulletin des arrêts de la Chambre criminelle de la Cour de cassation
CE	Conseil d'Etat
C. Civ	Code civil
C. Trav	Code du travail
C. Pénal	Code pénal
CCNE	Comité Consultatif National d'Ethique
CEDH	Cour européenne des droits de l'Homme
Circ. DRT	Circulaire de la Direction des Relations du Travail
CNIL	Commission Nationale de l'Informatique et des Libertés
Comm. Comm. Elec.	Communication commerce électronique
Com.	Commentaires
Cons. Const.	Conseil Constitutionnel
CPH	Conseil de prud'hommes
D.	Dalloz
D. aff.	Dalloz affaires
Direct.	Directive
Doct.	Doctrine
Doc. Fr.	Documentation française
Dr. Soc.	Droit social
Dr. Ouv.	Droit Ouvrier
Ecorev.	Revue critique d'écologie politique
Gaz. Pal.	Gazette du Palais
Jur.	Jurisprudence
JCP	Semaine Juridique
JCP aff.	Semaine Juridique des affaires
JO	Journal officiel
JOCE	Journal officiel des communautés européennes
L.	Loi
NTIC	Nouvelles technologies de l'information et de la communication
Préc.	Précité
Rapp. min. Travail	Rapport du Ministère du Travail
Rec. Lebon	Recueil Lebon
Soc.	Arrêts de la chambre sociale de la Cour de cassation
TGI	Tribunal de grande instance
TPS	Travail et Protection Sociale

SOMMAIRE GENERAL

INTRODUCTION GENERALE **7**

TITRE I – Le contrôle collectif de l'usage de la biométrie en entreprise **49**

Chapitre Préliminaire. Les différentes techniques biométriques 51
Section 1- La propagation contrôlée des outils biométriques 52
Section 2- Les différents usages de la biométrie 79
Section 3- Les défaillances potentielles des outils biométriques 98

Chapitre 1. La sujétion du traitement des données biométriques au principe de finalité 104
Section 1. Les procédures de création des dispositifs biométriques en entreprises 108
Section 2. L'intégration des finalités d'authentification et d'identification biométrique en entreprise 124

Chapitre 2. La sujétion du traitement des données biométriques au principe de proportionnalité 185
Section 1. L'appréciation de la balance des intérêts collectifs en entreprise 189
Section 2. La prise en compte de la traçabilité de la technologie biométrique 201

TITRE II –Le contrôle individuel de l'usage de la biométrie entreprise **236**

Chapitre 1. Les obligations d'information et de consultation des salariés dans l'environnement biométrique 239
Section 1. L'information loyale des salariés 242
Section 2. La consultation des représentants des salariés 270

Chapitre 2. L'exercice du consentement et des « droits actifs » 282
Section 1. La manifestation de la volonté du salarié dans l'environnement biométrique 284
Section 2. Le droit de regard du salarié sur le traitement de ses données biométriques 297

CONCLUSION GENERALE **313**

REMERCIEMENTS

« *A tous ceux qui se glissent chaque soir dans les draps froissés du doute…*[1] »

Le travail de thèse est empreint d'une certaine solitude qui fait penser aux traversées en solitaire, où l'on est à la fois seul devant son objectif et nombreux à suivre la même direction avec des doutes, des incertitudes, mais pendant lequel on est habité d'une ferme obstination pour atteindre enfin le port. Avec ce modeste travail, je rends aussi hommage à tous les « thésards » qui continuent leur course.

Je ne peux entrer dans le vif du sujet sans m'être acquittée auparavant de quelques remerciements qui mettent un terme à cette étude. Pour cela, il existe un mot simple et aux accents tellement usés par l'habitude, que l'on oublie combien il est sincère et réconfortant, « Merci ».

Merci à toutes les personnes que je vais citer, pour leur disponibilité, leur gentillesse et leurs précieux conseils.

Je tiens avant toute chose, à remercier très sincèrement et respectueusement mon directeur de thèse, Nathalie Mallet-Poujol, pour son investissement et les encouragements qu'elle m'a prodigués tout au long de ces années. Grâce à sa bienveillance, elle a su instaurer, lors de nos « rendez-vous de thèse », un climat de travail sympathique et convivial.

Je remercie sincèrement l'Equipe de Recherche sur le Droit des Créations Immatérielles – ERCIM UMR 5815 Université Montpellier I – et particulièrement Aurélie Bertrand, pour son accueil toujours chaleureux, sa patience et son aide lors de mes péripéties administratives.

[1] N. Panayotopoulos, « Le gène du doute », traduction G. Decorvet, Gallimard Coll. Du monde entier, 2004, p. 19 (exergue)

Mes remerciements vont aussi à Jean-François Mainguet, ingénieur de recherche au Commissariat à l'énergie atomique de Grenoble, tant pour sa relecture, l'autorisation de reproduire ses illustrations, que pour ses explications techniques qui m'ont permis de mieux appréhender certains points du sujet.

A Marc Renneville, directeur de publication du site internet criminocorpus et Didier Guillerm, consultant en biométrie et fondateur du portail internet biometrie-online, pour m'avoir permis d'utiliser certaines illustrations de leur site internet, dans le cadre de ce travail.

Je tiens aussi à remercier tout particulièrement Cécile Bonneau, du centre de documentation de la CNIL, pour sa gentillesse et son aide précieuse, lors de mes recherches à Paris.

A mes grands-parents et mon frère, pour leur soutien indéfectible durant toutes ces années d'études universitaires,
A mon père pour son mécénat, aspect non négligeable pour la réussite d'une thèse.
Je remercie tout particulièrement ma mère, pour son soutien et pour ses nombreuses relectures formelles sans doute fastidieuses mais néanmoins nécessaires.

A Jérôme, mon compagnon, pour son constant soutien, son « coaching moral », ses conseils avertis « d'ancien thésard » et son aide « informatique » qui ont contribué à mener à bien ce travail.

A Corinne et Jean-Baptiste, pour leurs multiples encouragements et leur aide précieuse dans la traduction du résumé, un peu plus précise que la mienne.

A vous mes amis, qui avez su m'apporter cette affection revigorante à certains moments de doute, affection doublée de distractions festives et sportives qui ont été, pour moi, des échappatoires bien souvent réconfortantes.

Enfin, à vous, membres du jury, pour avoir accepté de juger ces travaux, merci.

INTRODUCTION GENERALE

1. « *La crainte de voir l'homme s'emparer totalement de l'homme est devenue le cœur de toutes les angoisses*[2] ».

A l'heure de la profusion des nanotechnologies, de la vidéosurveillance, de la géolocalisation, ou de la biométrie que reste-t-il de la sphère privée des salariés sur leur lieu de travail ?

Bien que reconnue et protégée par les plus hautes autorités juridiques mondiales, la vie privée comme le relève fort justement les sénateurs A.M Escoffier et Y. Detraigne, fait l'objet de plusieurs remises en cause « *sous l'effet conjugué des enjeux de sécurité de l'après-11 septembre, du confort apporté par des nouvelles technologies par ailleurs intrusives, ainsi que d'une tendance sociologique profonde au narcissisme et à « l'exposition de soi*[3] ». En effet, les attentats du 11 septembre 2001 aux Etats-Unis d'Amérique ont ravivé le sentiment d'insécurité et parmi tous les nouveaux procédés techniques[4] de sécurisation des biens et des personnes, la biométrie a été élevée, sous l'impulsion du gouvernement américain, au rang d'une technologie-remède pour lutter contre le terrorisme, mais aussi contre les diverses fraudes liées à l'identité. Dans ce contexte international sécuritaire, la biométrie laisse aux Etats une grande marche de manœuvre.

---

[2] M. Contamine-Raynaud, Le secret de la vie privée, ouvrage collectif, L'information en droit privé, LGDJ 1978, page 454, n° 36.

[3] Y. Détraigne et A-M. Escoffier, Rapport d'information du Sénat n°441, Le respect de la vie privée à l'heure de la mémoire numérique, Session 2008-2009, p. 17, Disponible sur le site internet du Sénat au www.senat.fr

[4] Les nouvelles technologies (NTIC) désignent des procédés techniques permettant de faire circuler et rechercher l'information. Le Conseil européen en 1986 définit les technologies de l'information comme « *les systèmes, les équipements, les composants et les logiciels qui sont nécessaires pour assurer la recherche, le traitement et le stockage de l'information dans tous les domaines de l'activité humaine (foyer, bureau, usine, etc.) et dont la mise en œuvre fait généralement appel à l'électronique ou aux technologies similaires.* », définition issue de la décision 87/95/CEE du Conseil européen du 22 décembre 1986 relative à la normalisation dans le domaine des technologies de l'information et des télécommunications, Journal officiel n° L 036 du 7 fév. 1987 p. 0031 - 0037.

2. La biométrie est définie, étymologiquement, comme la mesure des choses vivantes. Appliquée à l'homme, elle est nommée anthropométrie et elle constitue « *l'étude mathématique surtout statistique des phénomènes biologiques* »[5], ou encore la « *science qui étudie à l'aide des mathématiques (statistiques et probabilités) les variations biologiques à l'intérieur d'un groupe déterminé*[6] ». Pour Eugène Schreider[7], la biométrie est « *la science des variations biologiques, des phénomènes qui s'y rattachent et des problèmes qui en découlent*[8] ». Nous retiendrons cette dernière définition.

Le cerveau humain effectue en permanence une reconnaissance biométrique. Le fait de mémoriser le son d'une voix ou la forme d'un visage, permet à la personne de reconnaître un proche, de l'identifier. Fort de ce constat, ce mécanisme naturel a été informatisé afin d'identifier de façon fiable les individus.
L'identité de tout homme peut être prouvée par différentes méthodes : d'abord, par la présentation d'un badge ou d'une carte d'identité, il s'agit là, de ce que l'on possède, ensuite, en composant son mot de passe, il est question, dans ce cas-là, de ce que l'on sait. Enfin, tout individu peut prouver son identité, grâce, par exemple, à ses empreintes digitales ou à l'iris de son œil. Cette identification atteste ce que l'on est. La biométrie est donc la reconnaissance d'une personne, par ses caractères physiques et physiologiques propres qui permettront de l'identifier avec certitude et de la différencier d'un autre individu.

Ainsi, selon la définition proposée par la CNIL, les systèmes biométriques sont « *des applications permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main, etc.), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche)*[9] ». La Commission nationale informatique et libertés (CNIL), ajoute que la biométrie « *recouvre l'ensemble des procédés tendant à identifier un individu à partir de la « mesure » de l'une ou de plusieurs de ses caractéristiques physiques, physiologiques ou comportementales. Il peut*

[5] Définition relevée dans le dictionnaire Hachette, édition 2009
[6] Dictionnaire Le Nouveau Petit Robert, édition 2009
[7] E. Schreider est le directeur du laboratoire de Biométrie humaine au Centre national de la recherche scientifique.
[8] E. Schreider, article sur la biométrie, Encyclopaedia Universalis en ligne, www.universalis.fr
[9] CNIL, Rapports d'activité 2001, Doc. Fr. 2002, pp. 157

s'agir des empreintes digitales, de l'iris de l'œil, du contour de la main, de l'ADN ou d'éléments comportementaux (la signature, la démarche) [10] ».

La biométrie a pour avantage d'éviter la perte ainsi que le vol de données et de réduire les risques de falsification de ces données. Toutefois, en ce qui concerne l'analyse ADN, cette automaticité n'est pas évidente. L'analyse ADN est tantôt classée comme faisant partie intégrante de la biométrie[11], tantôt exclue, selon les conditions dans lesquelles elle est pratiquée[12].

Dans le cadre de cette étude, l'analyse ADN a été délibérément exclue, dans la mesure où elle n'est employée que dans des cas précis (par exemple les prélèvements sur ordonnance judiciaire ou par la police scientifique sur une scène de crime) et n'a pas vocation à s'étendre en dehors de ces sphères[13]. Nous faisons, en conséquence, le choix de ne pas traiter de l'ADN, qui fait par ailleurs l'objet d'une controverse sur sa qualification ou non dans les techniques biométriques[14].

3. La biométrie, longtemps réservée aux services de police judiciaire, est devenue l'apanage des Etats qui collectent une quantité importante de données à caractère personnel[15], notamment pour la gestion des passeports, de l'immigration ou de la criminalité. Depuis quelque temps, certaines sociétés de production de matériels technologiques proposent aux particuliers des dispositifs biométriques dans un usage de confort. Il est évident que ces

---

[10] CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, rubrique biométrie, 28 décembre 2007, disponible sur le site www.cnil.fr

[11] Position de la CNIL en France, « Innovations technologiques », rubrique nos défis, disponible sur le site www.cnil.fr; de la Commission d'accès à l'information au Québec, « La biométrie au Québec : les enjeux », Document d'analyse, Juill. 2002, disponible au www.cai.gouv.qc.ca; ou bien de l'organisme allemand Biotrust.

[12] Il s'agit de la position du Parliamentary Office of Science and Technology britannique, du General Accounting Office américain ou de l'Electronic Warfare Associates canadien.

[13] Ces prélèvements sont effectués restrictivement et sont encadrés par les articles 16-10 et suivants du Code civil.

[14] Sur l'ADN voir infra n° 11.

[15] Les données à caractère personnel sont définies dans l'article 2 de la Directive de 1995, transposée en droit interne par la loi du 6 août 2004, modifiant ainsi la loi Informatique et libertés de 1978. Elles se déterminent comme « *toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* »

Ainsi, les personnes physiques peuvent être identifiées directement, par une image ou des données alphanumériques tels que le nom le prénom ou indirectement par un numéro d'identification.

Les données biométriques font directement partie des données dites sensibles au sens de l'article 25 I 8°) de la loi de 1978 modifiée en 2004, comme les données de santé ou de mœurs, même si elles ne sont pas explicitement déclarées ainsi. Cette qualification justifie qu'une entreprise doive procéder à une demande d'autorisation préalable auprès de la CNIL.

Certains pays, comme le Canada, considèrent aussi les données biométriques comme des données sensibles.

nouvelles technologies allaient très vite intéresser au plus haut point les entreprises, qui ont pressenti immédiatement tout ce que ces nouveaux produits pouvaient apporter, en matière de moyen d'identification des salariés, de sécurisation ou d'organisation des biens et des services. C'est ce dernier point qui a attiré notre attention et qui fait l'objet de cette étude.

4. L'entreprise a évolué au rythme des nouvelles technologies[16]. Certaines tâches traditionnelles ont disparu au profit de nouvelles, apportant avec elles une modification substantielle des conditions de travail. Il en est de même pour le droit du travail qui a dû s'adapter de la même manière et faire face à ces nouveaux défis, afin de veiller à la protection des salariés (respect de la vie privée sur les questions des consultations d'e-mails ou des sites internet, fichiers de données personnelles des salariés[17] etc.) sans entraver l'activité des entreprises. Corrélativement, la mondialisation des échanges a influencé l'organisation interne des entreprises. La biométrie, comme l'Internet, la vidéosurveillance, la géolocalisation ou les puces sans contact (RFID) sont désormais utilisées quotidiennement, quelquefois au détriment de la protection des données personnelles des salariés.

Les restructurations des entreprises notamment par fusions et absorptions élargissent considérablement les problématiques liées aux données personnelles en ce qu'elles accroissent la circulation internationale des fichiers[18]. Selon l'American Payroll Association[19], l'automatisation des processus de temps et de présence économise environ 1. 000 dollars par an et par employé. Ces économies résultent de plusieurs facteurs dont :

- la réduction du coût de traitement concernant les fiches de paie, la gestion des horaires et des emplois du temps.
- la diminution des erreurs humaines concernant l'enregistrement, le calcul et la saisie des heures.

---

[16] Le législateur en droit du travail n'a pas donné de définition. Nous retiendrons celle du Dictionnaire Robert qui définit les nouvelles technologies comme l'« *étude des techniques, des outils, des machines, des matériaux, des composants électroniques qui peuvent affecter notamment les conditions de travail, la formation professionnelle ou la rémunération* ».

[17] Selon l'article 2 de la loi n° 2004-801 Informatique et libertés du 6 août 2004 ce sont *« tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés* »

[18] Voir S. Gauthronet, « Le devenir des données personnelles dans le cadre des restructurations d'entreprises », 23ème conférence internationale des Commissaires à la protection des données, Paris 24, 25 et 26 sept. 2001

[19] Statistiques tirées de « Trends in Time and Attendance », présenté au 22ème congrès annuel de l'American Payroll Association, 27 avr. 200, disponible sur le site Internet : http://www.americanpayroll.org/

- l'élimination du « vol d'heures » ou temps supplémentaire de travail non autorisé. Cela implique une économie substantielle, du fait du non-paiement des heures de retard, des temps de pause trop longs ou des absences.

Par ailleurs, cette étude indique que les appareils biométriques de contrôle sont bien plus rentables que les systèmes non biométriques et ce, malgré le lourd investissement occasionné par l'emploi de cette technique. Ce constat s'explique par le fait qu'en biométrie, l'authentification des employés évite la falsification de données, comme le poinçonnage par les autres salariés afin de couvrir l'un d'entre eux, absent ou en retard. Cette diminution de coût prend aussi en considération les économies faites en termes de matériel de comptage, comme les cartes magnétiques. En somme, la biométrie permet un gain de temps considérable, la diminution d'erreurs récurrentes et rentabilise les coûts. Dans les pays étrangers, tous ces points justifient l'emploi d'appareils biométriques.

5. En France, la CNIL se montrait réticente à l'usage des techniques biométriques sur le lieu de travail, de peur qu'elles ne soient employées uniquement aux fins de surveillance des salariés. En effet, certaines entreprises ont essayé, sous couvert de l'impératif de sécurité, de surveiller l'effectivité du temps de travail des salariés par l'utilisation de la biométrie. Cette surveillance a pour origine une multiplication des fraudes aux badges qui nécessite de recourir à un moyen d'authentification plus fiable tel que la biométrie.

Toutefois, au fil des années et de l'évolution technologique, la CNIL a précisé sa « doctrine » et augmenté ses contrôles afin de limiter ce type de manquement aux libertés dans l'entreprise. Le tribunal de grande instance de Paris a pu se prononcer, à son tour, dans un jugement rendu le 14 avril 2005[20] et d'interdire à une société la mise en place d'une pointeuse biométrique, visant à contrôler le temps de travail des salariés. Cette finalité a été jugée inutile et disproportionnée au regard des activités de l'entreprise.

Plusieurs fondements légaux, qui proviennent du droit du travail, viennent soutenir la législation protectrice des données personnelles et règlementer la mise en œuvre d'un traitement automatisé dans l'entreprise. Certains articles du Code du travail ont été revus et

[20] TGI Paris, 1re ch. soc., 19 avr. 2005, CE Effia Services, Syndicat Sud Rail c/ Effia Services, commentaire A. Lepage, Comm. Comm. Elec. n° 10, Oct. 2005, comm. 164.

adaptés aux nouvelles technologies, pour imposer aux employeurs de nouvelles règles que nous développerons, telles l'information et la consultation du comité d'entreprise et des salariés, pour toute mise en œuvre, au sein de l'établissement, d'un traitement biométrique visant à collecter des données personnelles ou pour toute installation d'un traitement automatisé de gestion du personnel[21]. Par ailleurs, certains points ont été rajoutés au règlement intérieur des entreprises, telle la mention obligatoire de l'utilisation d'un procédé biométrique.

En ce qui concerne les techniques employées, les chefs d'entreprise n'ont pas la liberté de choisir tous les modes d'identification biométrique. S'ils veulent recourir à la technologie de l'empreinte digitale avec constitution d'une base de données, ils doivent justifier d'un fort impératif de sécurité. Si l'empreinte digitale est préférée à toute autre technique, elle doit être stockée sur un support individuel afin d'éviter tout détournement de bases de données et dans une finalité sécuritaire.

De ce fait, les empreintes digitales sont délaissées, pour d'autres technologies moins risquées, comme la reconnaissance du réseau veineux des doigts de la main ou la reconnaissance du contour de la main. C'est au sujet de ces dernières que la problématique de la biométrie en entreprise est particulièrement intéressante et constitue le fil conducteur des développements à suivre.

6. La perception, comme l'usage des dispositifs biométriques actuels, s'est forgée à travers l'Histoire. Les découvertes scientifiques appliquées au service de l'identification judiciaire ont permis de résoudre bon nombre d'affaires au XIX° siècle et a contribué à l'amélioration des dispositifs biométriques actuels (Chapitre 1). La biométrie est aujourd'hui la source de nombreux enjeux identitaires, économiques et politiques (Chapitre 2), source aussi de nombreuses craintes pour les libertés individuelles telles que la violation de la vie privée et d'une somme d'espoirs quant à son utilité sécuritaire (Chapitre 3). Toutefois, son utilisation croissante, au sein des entreprises, laisse en suspend de nombreuses interrogations, attachées notamment à l'exercice effectif des droits sur les données personnelles des salariés (Chapitre 4).

[21] Ord. n° 2007-329 du 12 mars 2007 relative au code du travail (partie législative), JO n° 61, 13 mars 2007 p. 4740 texte n° 5

Chapitre 1. Contexte d'implantation de la biométrie

7. L'histoire de la biométrie peut être divisée, selon Jacques Pierson, en trois grandes périodes[22] :

La période ancienne s'étend de l'Antiquité jusqu'à la fin du XIX° siècle. C'est une période durant laquelle la biométrie reste marginale.

La deuxième période s'étend de la fin du XIX° siècle jusqu'à la moitié du XX° siècle. Elle a été qualifiée par Jacques Pierson de « scientifique », car à ce moment-là, la biométrie a fait l'objet de nombreuses études.

Enfin, la troisième période, dite « industrielle », s'étend de la moitié du XX° siècle à nos jours, où la biométrie va considérablement être développée grâce aux progrès technologiques.

Nos sociétés ont toujours attaché de l'importance à l'identification des individus. Parce que l'être humain a des obligations individuelles et collectives, envers la société (fiscalité, service militaire), il ne peut s'en défaire par le seul fait de son anonymat. La prise de conscience des méfaits de l'anonymat qui entraînent, entre autres, la multiplication des délits et des crimes, a conduit à l'utilisation d'un système d'identification fiable.

8. L'analyse par empreinte digitale est le procédé anthropométrique le plus ancien.

A Babylone, en 6000 avant Jésus Christ, l'empreinte du pouce servait déjà de signature dans les contrats. Les Chinois de la dynastie Tang (618-906) procédaient de la même façon pour sceller leur accord dans les échanges commerciaux. Cette méthode a été reprise en 1858 dans un district des Indes britanniques par Sir William Herschel pour authentifier les contrats passés avec les hommes d'affaires indigènes.

Au fil du temps, plusieurs personnes se sont intéressées à ce mode de procédé. L'anglais Nehemiah Grew (1683), médecin et naturaliste britannique a écrit un traité sur les empreintes digitales en 1683, alors que l'italien Marcello Malpighi (1686), médecin et anatomiste, est le premier à les avoir étudiées sous un microscope. Ces différentes recherches n'ont toutefois pas donné de résultats concluants.

[22] J. Pierson, La Biométrie, l'identification par le corps, Collection Informatique, Ed. Hermès Science et Lavoisier, 2007, p. 18

9. Sous l'Ancien Régime en France, les fichiers de renseignements étaient incomplets. Seules les minutes des greffiers, sur lesquelles étaient mentionnées la marque GAL (galère) ou une fleur de lys, indiquaient les individus en état de récidive. Devant ces multiples dysfonctionnements, le législateur français a instauré, dès 1810, la mise en place de « sommiers judiciaires[23] » afin de centraliser les répertoires des condamnations du trimestre que chaque juridiction expédiait au ministère de la Justice. Les greffiers inscrivaient sur un registre les renseignements relatifs aux délinquants condamnés au moins à une peine correctionnelle. Tous les trois mois, le greffier adressait une copie de ces renseignements aux ministères de la Justice et de l'Intérieur. L'identification des individus par leurs empreintes digitales n'était pas utilisée.

Ce n'est qu'à la fin du XIX° siècle, que la biométrie a fait l'objet de nombreuses études scientifiques. Le docteur Henry Faulds, chirurgien dans un hôpital de Tokyo, a proposé l'empreinte digitale comme méthode d'identification des corps. Il fut le premier à établir une classification grâce à l'encre d'imprimerie et en informa le statisticien Sir Francis Galton, cousin de Darwin. Ce n'est qu'avec ce dernier, à partir de 1892, que l'utilisation de l'empreinte digitale a reçu une base scientifique, avec la démonstration qu'elle était unique pour chaque individu et ne changeait pas au cours d'une vie.

Edward Henry, administrateur du Bengale, a donné un caractère opératoire aux observations de Galton en élaborant un système de classification des empreintes. En 1887, le succès pour l'identification des criminels aux Indes fut tel, que New Scotland Yard a adopté ce procédé à partir de 1901, date à laquelle Edward Henry a été nommé à la tête du nouveau bureau des empreintes digitales.

Le procédé s'est diffusé très rapidement en France en 1903, grâce à Alphonse Bertillon, dans un contexte judiciaire particulier. A la fin du XIXème siècle, les criminels arrêtés étaient bien souvent des récidivistes. Pour changer cet état de fait, de 1885 à 1891, deux lois ont été promulguées dans le but d'aggraver les peines des multirécidivistes, peines à effectuer dans les bagnes en Guyane. L'anthropométrie judiciaire a grandement amélioré le travail des enquêteurs, parce que les criminels changeaient souvent d'identité. Il était donc difficile

[23] J. P. Gregogna, Casier judiciaire, Encyclopedia Universalis en ligne, disponible sur le site internet au http://www.universalis.fr/encyclopedie/casier-judiciaire/

d'identifier un individu impliqué dans d'autres affaires, sous des noms différents, avant le relevé des empreintes.



[24]

Alphonse Bertillon, alors jeune commis « auxiliaire aux écritures » était chargé du classement de ces sommiers judiciaires. Il a eu l'idée ingénieuse, de classer les fiches selon l'identité anthropométrique. Il a découvert tout d'abord, que le corps humain, à partir d'une vingtaine d'années, dispose d'une série de points de mensurations fixes qui rendent les chances de tomber sur deux individus identiques quasi nulles, de l'ordre de une sur deux cent quatre-vingt-six millions (1/286 000 000). Il en déduit que cet élément d'identification des personnes est suffisamment fiable pour être employé dans la résolution des affaires criminelles.

La première reconnaissance d'un récidiviste a été établie en 1883. A la fin de cette même année, Bertillon était parvenu à identifier quarante-neuf récidivistes par la comparaison des

[24] Représentation des sommiers judiciaires en 1912, disponible sur le site internet http://www.criminocorpus.cnrs.fr/article133.html. Tous droits réservés.

empreintes digitales. Il utilisa ces mesures dans le service de l'identité judiciaire, créé en 1893, sous sa responsabilité, au sein de la police judiciaire. Il améliora, petit à petit, sa méthode et son matériel. Ce matériel nommé « Bertillonnage », servit à constituer des mesures d'identification. Les empreintes digitales sont progressivement ajoutées à ses fiches pour compléter les différents profils criminels.

En 1902, Alphonse Bertillon résolut pour la première fois un crime grâce à sa méthode, uniquement en se basant sur les empreintes papillaires retrouvées sur la vitrine du magasin et en les comparant à ses fiches[25]. Il s'agit de l'affaire « Scheffer », sur laquelle il y avait peu d'indices, parmi lesquels quatre empreintes digitales, retrouvées sur des morceaux de vitre brisée. Cette affaire, qui tire son nom du criminel Maurice Scheffer dit « Georges l'artilleur », sera la première en Europe à être résolue grâce à l'utilisation des empreintes digitales.
Comme le soulève M. Marzouki[26], le terme anthropométrie a été délaissé au profit de « biométrie », comme s'il était nécessaire de faire oublier aux individus que l'origine première du mot est liée à l'histoire judiciaire. Xavier Guchet surenchérit et soulève que « *Parler de biométrie plutôt que d'anthropométrie c'est tenter d'effacer cette affiliation*[27] ».



28

[25] Cf. Annexe 10
[26] M. Marzouki, « Enjeux des techniques de biométrie – Une première approche », article publié dans les actes de la 23ème conférence internationale des Commissaires à la protection des données personnelles sur le thème : « Vie privée et droits de l'homme ». Paris. Septembre 2001.
[27] X. Guchet, G. Dubey et S. Craipeau, La biométrie : usages et représentations, Rapport final du projet incitatif du Groupe des Ecoles des Télécommunications 2003, fév. 2004, p. 5, disponible sur le site internet www.foruminternet.org
[28] Image de Maurice Scheffer, Service des archives de la préfecture de police de Paris, disponible sur le site internet http://www.criminocorpus.cnrs.fr/article133.html. Tous droits réservés.

10. Toujours est-il que ces découvertes scientifiques vont faire entrer la biométrie dans sa période industrielle, en partie grâce à l'émergence du « marché policier ». Cependant, la généralisation de la collecte d'empreintes digitales montre, assez rapidement, son inefficacité en raison de la lourdeur administrative attachée à la concentration, à la consultation ainsi qu'au personnel mobilisé pour effectuer les recherches de correspondances parmi les nombreuses fiches.

Dans les années 1980-1990, les polices des principaux pays développés ont souhaité centraliser leurs données afin de rendre les recherches plus efficaces. La biométrie s'est démocratisée et progressivement, en accord avec les Etats, les industriels ont principalement développé des dispositifs de sécurisation des zones aéroportuaires.

A ce jour, les enjeux liés à l'usage de dispositifs biométriques restent importants, puisque le passeport biométrique, qui est récemment entré en vigueur au sein de l'Union européenne, contribue à la maîtrise et au contrôle des flux migratoires.

Les pays développés possèdent ainsi des fichiers centralisés d'empreintes digitales, d'ADN, de portraits-robots de milliers d'individus, voire pour les Etats-Unis, de plusieurs millions d'individus. C'est dans ce contexte que sont apparus les produits industriels appelés AFIS (Automatic Fingerprint Identification System). Ceux-ci servent à automatiser la comparaison d'empreintes digitales entre différentes bases de données. La première à avoir commercialisé ce type de produit est la société Calspan Autonetics dans les années 1970, pour le compte du FBI.

En France, ce n'est qu'en 1984 que sera créé le Fichier national automatisé des empreintes digitales (FNAED) mais il ne fut autorisé qu'à partir du décret n° 87-249 du 8 avril 1987[29]. Il s'agit d'un fichier national qui vise la recherche, l'identification des auteurs de crimes et de délits ainsi que la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie. En 2010, ce fichier comporte plus de trois millions d'individus fichés et près de deux cent mille traces de personnes non identifiées.

Le marché de la biométrie s'est progressivement démocratisé et ne se limite plus aujourd'hui à un usage policier. Plusieurs sociétés cherchent à développer des outils biométriques destinés

[29] Décret n° 87-249 du 8 avril 1987, JO n° 84 du 9 avril 1987, p. 4046 modifié par le décret n° 2005-585 du 27 mai 2005 relatif au fichier automatisé des empreintes digitales gérées par le ministère de l'Intérieur, JO n° 124 du 29 mai 2005, p. 9533

aux particuliers. Il s'agit d'une biométrie dite « de confort ». Elle est plus employée comme un « gadget » que comme un moyen d'identification efficace qui répond à un réel besoin de sécurisation. Concrètement, elle est intégrée dans les téléphones mobiles, les ordinateurs portables et désormais dans les voitures pour lutter contre le vol. Les particuliers ne sont pas les seuls visés par les industriels. Les collectivités territoriales et les établissements scolaires en font la demande pour les accès aux cantines scolaires. Les applications sont diverses et variées de telle sorte que les outils biométriques prennent et prendront de plus en plus de place dans la vie quotidienne.

11. Parallèlement, la découverte scientifique de l'ADN a permis un nouveau développement de la biométrie. L'acide désoxyribonucléique plus couramment connu sous le sigle ADN, est une macromolécule présente dans toutes les cellules du corps de l'individu. La séquence ADN permet de définir le patrimoine génétique de chaque individu, patrimoine différent d'une personne à l'autre.
L'ADN est couramment utilisé de nos jours dans le cadre de tests, comme le test de paternité car il est fiable à 99,99%. Par ailleurs, il est employé plus largement par la police scientifique sur les scènes de crime tant sa fiabilité a permis, dans les affaires criminelles, de prouver la culpabilité de nombreux criminels depuis son utilisation.

Toutefois, si l'identification par ADN est fiable, elle est loin d'être efficace à cause du délai nécessaire pour l'obtention des résultats d'analyse qui demande parfois plusieurs semaines. Cet élément fait de l'identification biométrique par ADN, une des moins utilisées, en comparaison avec d'autres techniques biométriques (reconnaissance du réseau veineux des doigts de la main ou reconnaissance vocale). Le facteur temps est un élément déterminant dans le choix du procédé de reconnaissance. C'est à cause de cela que l'identification obtenue par l'ADN, la plus fiable, est la moins utilisée, du moins pour l'usage journalier que l'on en fait la plupart du temps. C'est une technique trop poussée et contraignante pour l'employer quotidiennement. On privilégiera donc, par commodité et pour la rapidité d'exécution, l'empreinte digitale et la géométrie de la main.

En France, le test ADN a permis de constituer, par la loi du 17 juin 1998[30], le Fichier national automatisé des empreintes génétiques (FNAEG). Comme son intitulé l'indique, ce fichier comporte les empreintes génétiques relevées au cours d'investigations de police (police et gendarmerie nationale). Depuis sa création, le fichier était au départ constitué pour les infractions sexuelles, la collecte ne cesse de s'étendre à d'autres types d'infractions. La loi du 15 novembre 2001[31] relative à la sécurité quotidienne, a étendu le champ d'application du FNAEG aux crimes d'atteintes graves aux personnes. Aujourd'hui, selon le syndicat de la magistrature, ce fichage s'applique « *aux trois-quarts des affaires traitées dans les tribunaux à l'exception de la délinquance financière ou de l'alcool au volant*[32] ».

La polémique sur la collecte et le fichage de l'ADN a été ravivée lorsqu'en 2007, le gouvernement français a proposé d'intégrer aux procédures d'immigration, ces tests ADN basés sur le volontariat des demandeurs, en vue du rapprochement familial[33]. Ces tests auraient été effectués pour les personnes, dans l'impossibilité de présenter leur acte d'état civil ou dans l'hypothèse d'un doute sérieux quant à l'authenticité de ce dernier.
Depuis la décision du Conseil constitutionnel le 15 novembre 2007[34], le test ADN a été reconnu comme conforme à la Constitution en ce que l'article 13 « *fixe les conditions et les modalités permettant à un enfant mineur demandeur d'un visa d'une durée supérieure à trois mois, ou à son représentant légal, de solliciter dans le cadre du regroupement familial qu'il soit procédé à son identification par ses empreintes génétiques pour apporter un élément de preuve d'une filiation déclarée avec sa mère lorsqu'il n'a pas été possible d'apporter cette preuve au moyen d'un acte de l'état civil* ». Lors des débats parlementaires, cet article a été violemment critiqué sur l'absence du respect de la vie privée, de la dignité humaine, du principe de légalité et du regroupement familial[35].

---

[30] Loi nº 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles, JO 18 juin 1998
[31] Loi n° 2001-1062 du 15 nov. 2001 relative à la sécurité quotidienne, JO 16 nov. 2001
[32] J.-M. Manach, La justice simplifie le fichage génétique, Quotidien en ligne Le Monde, 3 juil. 2007, disponible sur le site internet www.lemonde.fr
[33] Projet qui n'a pas été intégré dans la loi n° 2007-1631 du 20 novembre 2007 relative à la maîtrise de l'immigration, à l'intégration et à l'asile, JO n° 270 du 21 novembre 2007, p. 18993
[34] Conseil constitutionnel, Décision DC n° 2007-557 15 nov. 2007, décision consultable sur le site Internet du conseil au www.conseil-constitutionnel.fr
[35] Conseil Constitutionnel, « Les Cahiers du Conseil constitutionnel n° 24 », commentaire de la décision n° 2007-557 DC du 15 nov. 2007, loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile, disponible sur le site au www.conseil-constitutionnel.fr

12. La biométrie suscite de la méfiance mais aussi de la fascination. Elle est source de plusieurs enjeux d'ordres différents: politiques, sociaux, économiques (chapitre 2).

Chapitre 2. Les enjeux de la biométrie

13. Durant des siècles, les individus étaient identifiés par leur nom, puis par les registres paroissiaux tenus par le clergé et enfin par les titres d'identité papier. Ces différents modes d'identification des personnes ne sont pas parvenus à éradiquer les fraudes documentaires.

La biométrie, réputée fiable, est considérée comme la solution capable de déjouer les projets des fraudeurs. C'est pourquoi, aujourd'hui, le passeport biométrique se généralise dans la plupart des pays occidentaux. Cependant, ces changements ont pour effet négatif de modifier la perception qu'ont les individus de leur identité (A). A cette « crise identitaire » s'ajoutent des enjeux politico-stratégiques entre Etats (B).

Sous couvert du discours sécuritaire, les gouvernements contribuent à l'expansion de la biométrie. Les industriels sont encouragés à développer des dispositifs biométriques de telle sorte que la biométrie est désormais devenue un marché lucratif sur le plan national et international (C).

A. La déroute identitaire manifestée par l'emploi de dispositifs biométriques

14. Les techniques biométriques ont un impact incontestable sur la société. Cet impact se mesure à la fois sur la perception qu'a l'individu de son identité[36] mais aussi sur la perception qu'a une société donnée, sur cette technologie. Son emploi par les autorités gouvernementales, les entreprises et les individus en fait une technologie presque incontournable mais à quel prix ?

Paul Ricœur, dans son ouvrage intitulé « *Soi-même comme un autre*[37] », traite de la déroute identitaire en évoquant la disparition de « *l'ipséité* » au profit de « *la mêmeté* ». Il justifie son propos en expliquant que l'identité constitue deux réalités distinctes. La première est constituée objectivement par l'idée que certaines parties du corps d'un individu à travers les âges et malgré le passage du temps, ne se modifient pas, cet aspect est nommé par l'auteur, « *la mêmeté* ». On peut considérer la biométrie comme une partie de ce premier aspect car elle consiste à mesurer les éléments immuables sur lesquels le temps n'a aucune emprise comme les empreintes digitales, la reconnaissance de l'iris ou de la rétine. Seuls, les éléments qui les constituent, indifféremment de leur personnalité, contribuent à leur identification.

La seconde est composée du vécu de l'individu, de sa conscience de lui-même, l'auteur parle « *d'ipséité* ». L'ipséité rapporte les expériences affectives et constitue l'individu de l'intérieur et non plus de l'extérieur (mêmeté). L'individu cherche alors à préserver son identité personnelle, en disposant de zones d'accès à ses espaces d'intimité. Qu'il s'agisse d'intimité corporelle, sexuelle voire communicationnelle, ces différentes zones seront différentes selon le groupe social.

L'identité, somme d'éléments connus et reconnus par l'Etat, constitue une source de droits par le biais de l'état civil[38], le numéro d'identification au répertoire NIR, attribué à l'individu dès sa naissance et qu'il conservera tout au long de sa vie. Cette reconnaissance confère à l'individu la personnalité juridique, il est titulaire de droit, dès lors qu'il prouve qui il est.

---

[36] « *Ensemble des composantes grâce auxquelles il est établi qu'une personne est bien celle qui se dit ou que l'on présume telle (nom, prénoms, nationalité, filiation)* », Lexique des termes juridiques Dalloz, 13ème éd, 2001.
[37] P. Ricœur, « Soi-même comme un autre », Coll. Essais, éd. du Seuil, mars 1990, pp. 11
[38] « *Situation de la personne en droit privé, spécialement dans les rapports familiaux, telle qu'elle résulte des éléments pris en considération par le droit en vue de lui accorder des prérogatives juridiques* », Lexique juridique Dalloz, 13ème éd, 2001.

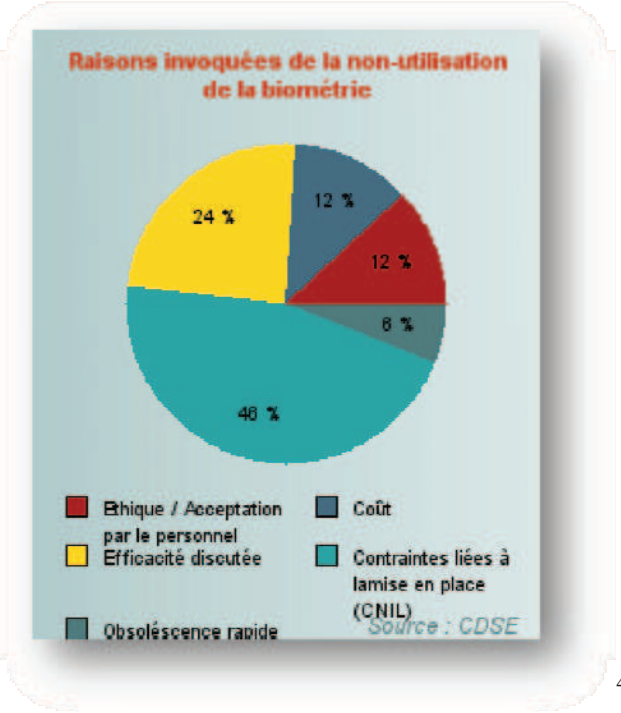
L'Etat fait appel à « *la mêmeté* », mais qu'en est-il de « *l'ipséité* » qui fonde les libertés individuelles ? Il s'agit de questions éthiques. Les techniques biométriques portent-elles atteinte à cet espace de liberté laissé à la personne au profit d'une « mêmeté » technique ? Existe-t-il la même liberté aujourd'hui comme hier ? Avec le temps et le triste constat de la multiplication des fraudes identitaires, la preuve de l'identité s'est considérablement compliquée.

15. La biométrie suscite un engouement pour les amateurs de nouvelles technologies qui vont l'employer comme un gadget de la vie quotidienne, mais elle provoque aussi des craintes d'immixtion dans la vie privée et la peur d'un glissement vers une surveillance généralisée de la population. Pour le sociologue G. Dubey cette technologie est observée *« comme une avancée technique dans la continuité des évolutions antérieures* (…) *Même si l'on ne perçoit pas toujours à court terme les avantages de la biométrie (...) cette dernière semble s'imposer du fait de la complexité même des dispositifs d'information et de leur nécessaire sécurisation*[39] ».

Pourtant, à en croire l'International Biometric Group, en comparaison à d'autres pays, la France se montre assez réservée en ce qui concerne l'emploi des techniques biométriques[40]. Ces réticences sont peut-être liées au statut de Nation des droits de l'Homme. Mais cette affirmation devient de moins en moins exacte et les justifications sont plus complexes[41].
Selon une étude faite par le Club des directeurs de sécurité des entreprises (CDSE), 35% des entreprises françaises auraient recours à des solutions biométriques. Parmi les 65% d'entreprises n'en faisant pas usage, la biométrie ne fait pas partie des faveurs des directeurs de sécurité. Les raisons invoquées pour la non-utilisation de la biométrie sont, en majeure partie, liées à la règlementation imposée par la CNIL et le processus de déclaration. En second lieu, vient l'efficacité puis les questions d'éthique et de coût.

---

[39] G. Dubey, « Nouvelles techniques d'identification, nouveaux pouvoirs. Le cas de la biométrie », Cahiers internationaux de sociologie 2008/2, n° 125, p. 263-279.
[40] Statistiques disponibles sur le site internet de l'International Biometric Group à l'adresse suivante http://www.biometricgroup.com/index.html
[41] Voir à ce sujet D. Duclos, « Ces industries florissantes de la peur permanente », Le Monde Diplomatique, édition imprimée, p. 16 – 17, Août 2005 ; Ligue des Droits de l'Homme, « Passeport biométrique : IRIS et la LDH demandent au Conseil d'État d'annuler le décret », communiqué du 4 juill. 2008 disponible au www.ldh-france.org ; « la biométrie… au risque de nos libertés », article du 10 oct. 2009, disponible au www.ldh-toulon.net



[42]

16. L'influence économique et politique de grandes nations, telles que les Etats-Unis et le Canada, peut amener les membres de l'Union européenne à être moins réticents et par là même, moins vigilants quant à la protection des libertés fondamentales des citoyens. L'exemple le plus concret est celui de l'insertion de la biométrie dans les titres de voyage. Sous l'impulsion des Etats-Unis, l'Union européenne a cédé et introduit des éléments biométriques dans tous les passeports[43].

Face aux menaces terroristes, et à l'apparition de nouvelles formes de violence, l'échec de chaque technologie ou procédés novateurs, en fait apparaître d'autres. Il y a une surenchère dans l'invention de nouvelles technologies « de méfiance » comme la vidéosurveillance, les puces RFID, la géolocalisation ou les nanotechnologies et la biométrie. Quelle nation trouvera le remède contre l'espionnage ou le stockage efficace de données afin de permettre le contrôle total de sa sécurité intérieure, tout ceci dans l'éventualité de l'attaque d'un ennemi certes invisible mais qui fait peur ?

---

[42] Schéma des raisons invoquées de la non-utilisation de la biométrie, étude faite par le Club de la sécurité en entreprise (CDSE).
Site Internet Journal du Net: http://www.journaldunet.com/solutions/securite/actualite/les-directeurs-securite-encore-frileux-a-l-egard-de-la-biometrie.shtml. Tous droits réservés.

[43] Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, disponible sur le site http://europa.eu

Notre société a peur, pas simplement de potentielles attaques terroristes, car pour la majorité des gens ces attaques restent hypothétiques, elle a peur de perdre la maîtrise de son identité et par là même, de sa liberté. La protection de son identité se joint alors à la protection des libertés mais plus encore, à la protection de sa vie privée. Il s'agit, dans les pays anglo-saxons du droit à « être laissé tranquille », qui est à l'origine même de la notion de vie privée[44].

17. La biométrie constitue un des nouveaux défis de la protection des données personnelles et des libertés individuelles. C'est une technologie qui s'adapte à une diversité de « besoins ». Elle est employée pour la gestion des contrôles d'accès, pour des programmes d'aide sociale, la gestion des populations déplacées, l'identification des victimes de catastrophe, la lutte contre la fraude électorale, etc. Il y a donc un enjeu politique et stratégique à faire accepter la biométrie à la population. Par ailleurs, l'insertion de données biométriques dans les passeports est aussi l'aboutissement de négociations et d'enjeux politiques à toujours collecter plus de données personnelles (B).

B. L'enjeu politico – stratégique de la biométrie

18. Le traumatisme, consécutif aux attaques terroristes du 11 septembre 2001 à New York, a ravivé cette crainte de l'étranger. L'exemple des Etats-Unis reste le plus représentatif de ce comportement. Initialement, le programme US-VISIT[45], voté par le Congrès américain en 1996, voyait son application repoussée pour des raisons de logistique (congestion aux frontières). Il est entré en vigueur le 5 janvier 2004[46].

Les techniques biométriques n'ont pas attendu l'année 2001 pour émerger, mais elles se sont, en revanche, considérablement développées après cette date. Les Etats se munissent de moyens technologiques de plus en plus évolués et mettent en place des coopérations avec d'autres Nations, dans le seul et unique but d'obtenir de plus amples informations sur la

[44] F. Rigaud, « L'élaboration d'un right of privacy par la jurisprudence américaine », Revue internationale de droit comparé, volume 32 n°4, 1980, pp. 701-730.Traduction littérale du "The right to let alone" évoqué par le Juge Cooley aux Etats Unis in Cooley on Torts, 2ème éd., 1888, p. 29, article disponible au www.persee.fr

[45] Acronyme de United States Visitor and Immigrant Status Indicator Technology. Ce programme est destiné à collecter les données biométriques des personnes pénétrant sur le territoire américain, il relève les empreintes digitales ainsi que la photographie des personnes.

[46] Department of Homeland Security, "DHS Begins Test of Biometric Exit Procedures at Two U.S. Airports", article disponible sur le site internet au http://www.dhs.gov/ynews/releases/pr_1243605893203.shtm

population mondiale. Ces données sont stockées, analysées, sans que le citoyen étranger puisse avoir connaissance de l'utilisation de ses données, ni qu'il puisse y contrevenir.
Les Etats-Unis et le Canada sont dotés de puissants outils biométriques et accumulent de nombreuses données personnelles. L'accord signé en juillet 2007 entre les Etats-Unis et l'Union européenne nommé Passenger Name Record (PNR)[47], en est la démonstration, puisque les autorités européennes viennent de permettre à plus de 15 administrations américaines d'obtenir toutes les données personnelles des citoyens arrivant sur le sol américain par le biais d'une compagnie aérienne européenne. Par ailleurs, ce transfert de données personnelles est effectué sans contrôle de l'Union européenne, pour une durée de quinze ans, ce qui pourrait entraîner des refus d'embarquement pour les personnes qui ne pourraient justifier leur identité. Les autorités américaines disposent de réels pouvoirs mais, en contrepartie, elles se sont engagées à assurer aux passagers un niveau de protection élevé, une utilisation minimale ainsi qu'un effacement immédiat des données personnelles.

19. Les attentats meurtriers de Londres, en Juillet 2005, ont conforté les différents gouvernements dans leur choix d'opter non seulement pour un fichage automatique de leurs citoyens, mais au-delà, pour un fichage de toute personne circulant sur leur territoire[48]. La biométrie a été une des réponses immédiates apportées par la classe politique, mais elle reste une des solutions sérieuses, puisque les terroristes étaient des ressortissants britanniques insoupçonnés de perpétrer de tels actes.

En France, le débat sur les analyses ADN a ravivé certaines craintes. Le Parlement français a eu l'occasion de délibérer sur ce sujet à plusieurs reprises, notamment dans un rapport sur « *la valeur scientifique de l'utilisation des empreintes génétiques dans le domaine judiciaire*[49] ». Avec l'adoption de la loi du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure[50] et de la loi du 18 mars 2003 sur la sécurité intérieure[51], les diverses mesures

[47] Décision 2007/551/PESC/JAI du Conseil du 23 juil. 2007 relative à la signature, au nom de l'Union européenne, d'un accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au ministère américain de la sécurité intérieure (DHS) (accord PNR 2007), disponible sur le site http://eur-lex.europa.eu/
[48] Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.
[49] C. Cabal, « La valeur scientifique de l'utilisation des empreintes génétiques dans le domaine judiciaire », n° 3121 Assemblée nationale (11ème législature) et Sénat n° 94 (2001-2002), disponible sur le site internet de l'Assemblée nationale à l'adresse suivante http://www.assemblee-nationale.fr/12/rap-off/i0938.asp
[50] Loi n° 2002-1094 du 29 août 2002 d'orientation et de programmation pour la sécurité intérieure, JO 30 août 2002

prises sont venues conforter les opposants et les citoyens réticents à la biométrie que ces procédés ne visaient qu'à attenter à leur intimité et à leur vie privée. En effet, ces lois renforcent particulièrement les moyens humains et matériels des forces de l'ordre, comme l'élargissement du champ de compétences du Fichier national automatisé des empreintes génétiques – FNAEG – la faculté d'effectuer des fouilles dans les véhicules sous contrôle de l'autorité judiciaire et la création de nouvelles incriminations, comme le racolage passif, les rassemblements "menaçants ou hostiles" dans les parties communes d'immeubles et les réseaux d'exploitation de la mendicité.

20. Les outils biométriques permettent d'identifier les individus mais ne peuvent en aucun cas anticiper leurs intentions. Ils n'apparaissent efficaces *a posteriori*, que dans la lutte contre la criminalité, mais à quel prix ? Pour quelle sécurité du citoyen ? Il n'est pas dit, à l'heure actuelle, que ces moyens ne soient pas plus souvent détournés aux fins d'espionnage de certains comportements, voire de discriminations (banques, emploi...) A courir derrière un ennemi invisible, les gouvernements partisans ne sèment-ils pas plus l'angoisse qu'un sentiment de sécurité ? « *On radiographie les voyageurs et le contenu de leurs bagages, on stocke les données biométriques, on surveille les portables, on archive des myriades de numéros de téléphone, on numérise les empreintes digitales, on croise les fichiers géants d'administrations ou d'entreprises (...) La politique de la peur l'emportera-t-elle ? Alors, les légendaires terroristes auront atteint leur but : en quatre ans, ils auront transformé les grandes démocraties en forteresses paranoïaques étouffant leurs propres citoyens*[52] ».

La lutte contre le terrorisme est devenue le leitmotiv pour accumuler des données mais elle risque aussi, de développer l'espionnage industriel. L'exemple de l'affaire SWIFT (Society for worldwide interbank financial telecommunication) permet d'éclaircir le propos. Les institutions européennes de protection des données ont été saisies, en juin 2006, suite aux révélations de la presse américaine selon lesquelles la CIA et le Trésor américain ont surveillé, pendant des années, des millions de données transitant par l'entreprise SWIFT, principal réseau international de messagerie, utilisé dans le domaine bancaire.

---

[51] Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure, JO 19 mars 2003

[52] D. DUCLOS, « Ces industries florissantes de la peur permanente », Le Monde diplomatique, Août 2005, pp. 16- 17

Les Etats-Unis, avait tout intérêt, du point de vue économique, bancaire et stratégique, à disposer d'un accès libre aux données bancaires européennes telles que le montant du contrat, son bénéficiaire et la société émettrice. Les CNIL européennes sont parvenues à rapatrier cette entreprise de droit belge en Europe, afin que les données intra-européennes ne soient plus accessibles aux institutions américaines. Les données transiteront par la Suisse et les Pays-Bas[53]. La stratégie est bien visible dans ce cas d'espèce, si l'on veut avoir des relations d'affaires avec les Etats-Unis. Pour ne pas prendre le risque d'un éventuel espionnage industriel, il faut leur laisser un accès aux fichiers de données personnelles. Là encore, après le dossier « PNR » (Passenger Name Records), dans lequel les compagnies aériennes doivent transmettre les données personnelles des voyageurs à destination des Etats-Unis, nous avons un autre exemple « *d'un certain unilatéralisme juridique américain*[54] ».

La biométrie est bel et bien source d'enjeux stratégiques. Sous couvert d'une coopération policière ou économique, certains Etats cherchent à rassembler des informations personnelles sur les citoyens. Il convient donc d'être extrêmement vigilants quant aux transferts internationaux de données personnelles, d'autant plus que les entreprises implantent de plus en plus de dispositifs biométriques et que les plus importantes d'entre-elles, dotées de ces systèmes, ont des succursales ou leur siège social, à l'étranger.

.

21. L'insertion d'outils biométriques dans les entreprises n'est que la suite directe des multiples initiatives étatiques. Cet engouement a fait de la biométrie un marché plutôt lucratif, si bien que l'International Biométric Group annonce chaque année des projections de croissance du marché toujours plus élevées (C).

[53] CNIL, « Affaire SWIFT : la CNIL demande de la transparence », article du 13 juin 2007, disponible au www.cnil.fr; Parlement européen, « SWIFT : les données bancaires européennes doivent être traitées selon les normes européennes, estiment les députés », communiqué de presse, 3 sept. 2009, disponible au www.europarl.europa.eu

[54] CNIL, 28ème Rapport d'activité 2007, Doc. fr., mai 2008, p. 9, consultable sur le site internet de la Documentation Française au www.ladocumentationfrancaise.fr/

C. Le marché lucratif de la biométrie

22. La biométrie a été en premier lieu employée dans le domaine judiciaire et elle était alors réservée aux seuls enquêteurs. Elle s'est démocratisée pour toucher plus récemment le domaine de la consommation privée. Ce marché est nommé par Charles Copin, journaliste spécialisé dans les problématiques liées aux techniques d'identification, la biométrie « *de confort* » [55]. Il oppose cette biométrie de complaisance, employée plus comme un gadget que pour ses fonctions en matière de sécurité, à la biométrie sécuritaire, employée par l'Etat ou les entreprises. L'expression « *biométrie de confort* » sera reprise tout au long des développements à venir tant il résume bien ce phénomène d'intégration aisée de la biométrie dans la vie courante des individus.
Les industriels qui commercialisent la biométrie ont joué la carte du « tout sécuritaire » de l'après 11 septembre 2001. La biométrie pour la sécurité privée s'est développée, parallèlement à l'essor de la biométrie pour la sécurité publique qui concerne par exemple les aéroports, les documents d'identité ou la protection du lieu de travail. Ce nouveau marché cible majoritairement les biens personnels que sont la voiture, l'ordinateur portable ou les serrures de porte. Il est devenu plus ludique de s'identifier en apposant son empreinte digitale qu'en entrant son code PIN ou même en associant les deux.

Les arguments avancés sont la rapidité d'identification, la fiabilité et la sécurité. A force de devoir mémoriser quotidiennement des codes de toute sorte, il arrive que l'on en oublie, la biométrie met un terme aux oublis en rassurant le consommateur sur la sécurité et la confidentialité des données.

23. Selon l'International Biometric Group[56], le chiffre d'affaires de la biométrie en 2003 a atteint les 700 millions de dollars. En 2005, le marché représentait environ 1,8 milliard de dollars et a dépassé les 3,4 milliards en 2009. D'ici 2014, le marché de la biométrie devrait atteindre les 10 milliards de dollars[57]. Une enquête menée par le FBI aux Etats-Unis auprès de deux cent quarante et une entreprises, a montré que 49% d'entres elles, avaient été victimes de

[55] D. Auger, « Biométrie : l'équilibre entre libertés individuelles et promesse sécuritaire serait-il possible ? », Mémoire pour l'obtention du DESS, sept. 2005, p. 71, expression employée par C. Copin, commissaire général du salon Identech et spécialiste des problématiques sécuritaires, lors de son intervention, mémoire disponible au www.univ-paris1.fr
[56] Cf. Annexe 1
[57] International Biometric Group, Biometric market and industry report 2009-2014, consultable sur le site http://www.biometricgroup.com/

vols électroniques et de diverses fraudes. Ceci équivaut à une perte d'environ 136,8 millions de dollars. Si l'on ajoute à ce chiffre les fraudes à la carte de crédit pour 4 milliards de dollars, le montant global des fraudes électroniques prend une ampleur considérable.

Parallèlement, au Japon, la hausse des fraudes sur Internet a entraîné l'accroissement de l'usage de la biométrie comme technique d'identification. Les pouvoirs publics souhaitent l'utiliser pour éradiquer les fraudes aux documents d'identité et améliorer la sécurité des aéroports et des bâtiments publics. Le projet de visa biométrique va lancer l'économie de la biométrie au Japon. Les entreprises japonaises s'intéressent à la biométrie et développent des dispositifs de reconnaissance de la main et du visage.

Selon le Yano Research Institute[58], en 2004, le marché de la biométrie était de 8,76 milliards de yens (65,5 millions d'euros) et devrait atteindre 27, 22 milliards de yens (200 millions d'euros). Elle est employée dans la sphère privée et plus particulièrement pour la protection les téléphones mobiles, les assistants personnels et les distributeurs automatiques de billets.
Ceci nous prouve donc qu'il n'est plus simplement question d'identification policière ou criminelle, mais qu'il s'agit réellement du marché florissant de l'authentification.

Sur son site, la CNIL constate une augmentation des demandes tendant à mettre en place des outils biométriques. Elle fournit à ce titre plusieurs chiffres : en 1997 elle a examiné son premier dispositif biométrique avec enregistrement des empreintes digitales dans une base de données. Depuis, le nombre de demandes d'autorisation ne cesse d'augmenter. En 2007, six cent deux traitements biométriques ont été examinés dont cinquante-trois demandes portaient sur la collecte des empreintes digitales. Seules trente-deux d'entre elles ont été autorisées. Les autres demandes concernaient des systèmes de reconnaissance du contour de la main.

24. L'enjeu économique de la biométrie est double. Dans un premier temps elle permet d'éradiquer des fraudes, en intervenant de façon curative. Dans un second temps, les industriels s'enrichissent et développent les dispositifs biométriques de prévention. En France, la CNIL peut désormais labelliser les dispositifs biométriques comme étant respectueux de la vie privée. Cette labellisation ira sans doute dans le sens de l'accroissement du marché de la

[58] Yano Research Institute, Biometrics market 2009, consultable sur le site http://www.yanoresearch.com/

biométrie. Si, pour l'instant, aucune solution universelle n'a été trouvée, une révolution de l'identification se profile. Il sera nécessaire de trouver un consensus international sur les outils à employer, mais aussi sur les droits à garantir en matière de libertés individuelles car la biométrie reste encore source de craintes (chapitre 3).

Chapitre 3. La biométrie, source de craintes

25. Les craintes exprimées concernant la biométrie sont majoritairement liées à la peur de voir disparaître la préservation de la dignité humaine ou le droit à la vie privée (A). Qu'adviendra-t-il des droits et libertés de l'individu si la biométrie se généralise à toutes les activités de la vie courante ? Au-delà de la problématique de la protection des libertés fondamentales, se pose la question de la valeur de la preuve d'une donnée biométrique (B) dès lors que cette dernière peut être l'objet d'un détournement.
Pourtant, l'emploi de dispositifs biométriques peut être, aussi, une source d'espoir et un générateur de libertés (C).

A. La dignité humaine et le droit à la vie privée

26. Selon l'article 34 al. 1 de la Constitution française « *La loi fixe les règles concernant : les droits civiques et les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; la liberté, le pluralisme et l'indépendance des médias ; les sujétions imposées par la défense nationale aux citoyens en leur personne et en leurs biens* ».
C'est dans cet état d'esprit que l'article 1er de la loi Informatique et libertés de 1978 rappelle que « *L'informatique doit être au service de chaque citoyen… 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 et publiques* ». La loi doit mettre en œuvre tous les moyens visant à garantir l'effectivité de l'exercice des libertés individuelles sur le lieu de travail notamment la protection de la dignité humaine des salariés (1°) ainsi que de la vie privée sur le lieu de travail (2°).

1°. La dignité humaine

27. Les dispositifs biométriques visent à identifier un individu par ses caractères physiques. Ce mode d'identification est souvent rejeté car il renvoie à la mémoire des atrocités perpétrées durant la Seconde Guerre mondiale pendant laquelle la dignité humaine a été bafouée, et où les êtres humains étaient numérotés, classés et déshumanisés. Depuis cette période, plusieurs textes internationaux placent la dignité humaine au rang de premier droit fondamental de l'homme. Ainsi, la Déclaration universelle des droits de l'Homme (DUDH) considère « *que la reconnaissance de la dignité inhérente à tous les membres de la famille humaine et de leurs droits égaux et inaliénables constitue le fondement de la liberté, de la justice et de la paix dans le monde.* » L'article premier poursuit « *Tous les êtres humains naissent libres et égaux en dignité et en droits. Ils sont doués de raison et de conscience et doivent agir les uns envers les autres dans un esprit de fraternité*[59] ». La Charte des droits fondamentaux de l'Union européenne s'est, plus récemment, inspirée de la DUDH puisqu'elle a fait, de la dignité humaine, la valeur première et fondamentale en son article 1er. « *La dignité humaine est inviolable, elle doit être respectée et protégée*[60] ».

Dans certains pays, comme l'Allemagne, la dignité humaine est intégrée à la constitution. La loi fondamentale de la République fédérale d'Allemagne énonce au sein de l'article 1 que *«(1) La dignité de l'être humain est intangible. Tous les pouvoirs publics ont l'obligation de la respecter et de la protéger.*
(2) En conséquence, le peuple allemand reconnaît à l'être humain des droits inviolables et inaliénables comme fondement de toute communauté humaine, de la paix et de la justice dans le monde. (...)[61] ».
En France, le Conseil constitutionnel élève la dignité humaine au rang de principe à valeur constitutionnelle depuis 1994[62] mais ne la mentionne pas directement.

---

[59] Déclaration intervenue le 10 décembre 1948, 58 Etats membres étaient présents pour sa signature. Disponible sur le site internet de la DUDH, http://www.un.org/fr/documents/udhr/
[60] Charte intégrée dans le traité de Rome en 2004, disponible sur le site : http://www.europarl.europa.eu/charter/pdf/text_fr.pdf
[61] Loi fondamentale pour la République fédérale d'Allemagne du 23 mai 1949, JO Fédéral, p.1, (BGBl. III 100-1), disponible en langue française sur l'adresse suivante http://www.bundesregierung.de/Webs/Breg/FR/Loifondamentale/loi-fondamentale.html
[62] Conseil constitutionnel, DC. n° 94-343/344 du 27 juil. 1994, loi relative au respect du corps humain et loi relative au don et à l'utilisation des éléments et produits du corps humain, à l'assistance médicale à la procréation et au diagnostic prénatal, JO 29 juil. 1994, p. 11024.

En droit français, l'article 16 du Code civil énonce que « *la loi assure la primauté de la personne, interdit toute atteinte à la dignité de celle-ci et garantit le respect de l'être humain dès le commencement de sa vie.* »

28. La collecte des données biométriques permet d'identifier un individu à travers certains éléments de son corps tels le contour de sa main, ses empreintes digitales, son iris, etc. Le fait que l'identification passe par l'étude du corps génère certaines craintes potentielles liées au respect de la dignité humaine.
Néanmoins, le professeur Roger Clarke a relevé trois autres sources de craintes qui concernent la vie privée (2°).

2°. La vie privée

29. Le premier niveau de crainte est grandement lié aux origines historiques de l'usage de la biométrie. La technique biométrique est assimilée à une technique répressive, allant à l'encontre de l'épanouissement et de l'autodétermination de l'individu. Pour Roger Clarke[63], par exemple, la biométrie constitue une des menaces les plus élevées pour les libertés parmi tous les autres modes de surveillance des individus. Ainsi, « *Biometric technologies, building as they do on a substantial set of other surveillance mechanisms, create an environment in which organizations have enormous power over individuals. Faced with the prospect of being alienated by employers, by providers of consumer goods and services, and by government agencies, individuals are less ready to voice dissent, or even to complain. That is completely contrary to the patterns that have been associated with the rise of personal freedoms and free, open societies. It represents the kind of closed-minded society that the Soviet bloc created, and which the free world decried. The once-free world is submitting to a 'technological imperative', and permitting surveillance technologies to change society for the worse. Biometrics tools are among the most threatening of all surveillance technologies, and herald the severe curtailment of freedoms, and the repression of 'different-thinkers', public interest advocates and troublemakers*[64] ».

[63] R. Clarke est professeur à l'Australian national university, spécialiste international en protection de la vie privée, fervent défenseur des libertés individuelles.
[64] « Les technologies biométriques, sont bâties sur des mécanismes de surveillance. Elles créent un environnement dans lequel les organisations ont un pouvoir énorme sur les individus. Face à la perspective d'être

La menace est constituée, selon R. Clarke, par la collecte accrue des données personnelles et par l'utilisation de ces données dans de nombreux domaines, tels l'entreprise ou les réseaux de consommation comme les cartes de fidélité biométriques de grands magasins. Ce fonctionnement est, selon lui, contraire au rayonnement des libertés individuelles. Il opte pour le droit à l'anonymat des données ainsi que la liberté d'utilisation des pseudonymes.

30. En France, la Commission consultative des droits de l'Homme, a affirmé que « *les problèmes posés dans un contexte technologique nouveau relèvent d'un dilemme classique pour les libertés publiques. Il y a évidemment de très bonnes raisons pour profiter du progrès technique, si ce progrès conduit à améliorer l'efficacité de tâches régaliennes d'identification. Mais il y a des risques inhérents à cette évolution et il s'agit de savoir s'il faut prendre ces risques*[65] ». Cette même Commission a rappelé la nécessité d'informer valablement les personnes et de garder une extrême vigilance quant à la collecte de ces données, si l'on tient compte de leur caractère sensible.

Le Comité consultatif national d'éthique (CCNE) a, dans cette même ligne directrice, rendu un avis en date du 26 avril 2007, dans lequel il soulève qu' « *une société qui passe de la vigilance à la surveillance met en jeu, au prétexte d'une demande croissante de sécurité collective, les libertés individuelles et le droit à l'anonymat et au secret. La collecte des données biométriques identifiantes risque de comporter une atteinte majeure à la vie privée, et pourrait donc aussi ne pas respecter l'article 8 de la convention des Droits de l'Homme qui stipule que « toute personne a droit au respect de sa vie privée et familiale*[66] ».

---

aliénés par les employeurs, par les fournisseurs de biens et services de consommation, et par des organismes gouvernementaux, les particuliers sont moins enclins à se plaindre ou à adopter des comportements dissidents.
C'est tout à fait contraire aux modèles qui ont été associés au rayonnement des libertés individuelles et des sociétés libres et ouvertes. Il représente l'état d'esprit existant dans une société fermée comme celle que le bloc soviétique a créé, et que le monde libre a décrié. Le monde libre se soumet à un «impératif technologique», et les technologies de surveillance permettent de changer la société de façon négative. Les dispositifs biométriques sont parmi les plus menaçants de toutes les technologies de surveillance. Ils annoncent la réduction sévère des libertés et la répression des « différents penseurs, défenseurs de l'intérêt public et fauteurs de troubles. », R. Clarke, « Biometrics and Privacy », 2001, disponible sur le site internet au www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html

[65] Commission nationale consultative des droits de l'homme, Problèmes posés par l'inclusion d'éléments biométriques dans la carte nationale d'identité : contribution de la CNCDH au débat », article 1er, Avis défavorable rendu en Assemblée plénière le 1er juin 2006, disponible sur le site internet de la Commission, http://www.cncdh.fr

[66] CCNE, avis n° 98, « Biométrie, données identifiantes et droits de l'homme », 26 avr. 2007, consultable au http://www.ccne-ethique.fr/

Dans l'objectif d'une uniformisation des législations européennes en matière de protection des données personnelles, le Parlement européen et le Conseil sont intervenus en premier lieu avec la Directive 2002/58/CE du 12 juillet 2002[67]. Elle énonce dans son article 1er que « *La présente directive harmonise les dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté*. »

La réforme de cette Directive[68] a étendu la protection des citoyens européens à la conservation des données générées ou traitées dans le cadre de la fourniture de services de communication électronique. La durée de conservation de certaines données a été largement étendue, notamment pour pouvoir tracer et identifier la source d'une communication, la destination d'une communication ainsi que l'heure, la date ou le type de machine employée.
Le groupe de travail « Article 29[69] », a toutefois invité les Etats membres à prendre garde aux collectes abusives de données et à mettre en place des garanties suffisantes comme la spécification de la finalité, la limitation des données et de l'accès à ces dernières, l'absence d'exploration des données. Ces recommandations sont également applicables aux données biométriques.

31. Le second niveau de crainte relève de la nature même de la donnée biométrique. Contrairement à une carte à puce ou à un mot de passe constituant une donnée que l'on connaît, externe à l'individu, la biométrie constitue ce que l'on est, c'est une donnée interne, propre à chaque personne. A cet égard, la personne doit accepter de se soumettre

[67] Directive 2002/58/CE du 12 juil. 2002 du Parlement européen et du Conseil 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), Journal officiel n° L 201 du 31 Juil. 2002 p. 0037 – 0047.
[68] Cette Directive a été modifiée par la directive 2006/24/CE du Parlement européen et du conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, et modifiant la directive 2002/58/CE, JO L 105 du 13 avr. 2006, p. 54–63.
[69] Groupe de travail « Article 29 », Avis 3/2006 sur la Directive 2006/24/CE du Parlement européen et du Conseil sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communication, et modifiant la Directive 2002/58/CE, adopté le 25 mars 2006, disponible sur le site internet Europa sur le lien suivant : http://ec.europa.eu/justice_home/

physiquement au processus d'identification, sachant qu'en cas de leurre[70], il lui sera impossible de changer d'empreinte digitale ou d'ADN.

32. Le troisième niveau de crainte relève des conditions de la collecte des données personnelles. La CNIL se base essentiellement sur le concept de traçabilité. Une technologie qui laisse des traces, comme l'empreinte digitale, ne peut être appréciée de la même manière que les autres. Les autorisations sont restreintes et obéissent aux impératifs étudiés.

Dans la même idée, au Québec, la Commission d'accès à l'information estime que la donnée biométrique est « *un identifiant bavard (...) un identifiant aussi collé à notre physiologie et à notre comportement que la mesure ou la caractéristique biométrique transporte souvent des informations sur notre état d'esprit et sur notre état de santé*[71] ».

Le principe de cloisonnement des données est utilisé au Québec comme outil permettant d'assurer une meilleure protection de la vie privée en restreignant le croisement des fichiers comprenant des données personnelles. Cet outil est un verrou qui pourrait disparaître si les autorités étatiques décidaient de permettre la centralisation des fichiers biométriques.
La Commission d'accès à l'information ajoute que « *La centralisation de l'information peut certes sembler une solution intéressante du point de vue économique et au niveau de l'accès à l'information par un plus grand nombre de personnes. Mais les lois de protection des renseignements personnels font toutes le même pari : le cloisonnement de l'information au sein de plusieurs organismes demeurera toujours la meilleure garantie de confidentialité et l'obstacle le plus approprié pour éviter que l'État ne puisse dresser des profils sur les individus ou autrement s'immiscer dans leur vie privée*[72] ».

33. Pour le philosophe Xavier Guchet, c'est la notion de « biopouvoir » développée par Michel Foucault qui offre la meilleure explication : « *L'intérêt de la notion de biopouvoir est qu'elle permet justement de décrire des mécanismes de pouvoir en abandonnant l'idée que le pouvoir est une réalité homogène , exercée par un individu ou un petit nombre d'individus*

[70] Infra n° 79.
[71] Commission d'accès à l'information du Québec, « Document d'analyse sur la biométrie au Québec, les enjeux », Juil. 2002, disponible sur le site internet de la http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_enj.pdf
[72] Commission d'accès à l'information du Québec, « Les enjeux de la biométrie au Québec », document d'analyse, juillet 2002, p. 26, disponible que le site internet www.cai.gouv.qc.ca

considérés comme les sujets du pouvoir. Le biopouvoir est plutôt un ensemble de mécanismes, de micro pouvoirs hétérogènes, régionaux, multiples, qui s'exercent en des points innombrables et n'émanent pas d'une instance souveraine qui leur serait extérieure[73] ».

Dans cette théorie, la biométrie ne serait pas simplement un moyen de contrôler l'identité des individus mais aussi un instrument de régulation des populations, un « biopouvoir » selon l'expression employée par Michel Foucault. Par exemple, le fait de contrôler par un système biométrique qu'un élève mange effectivement à la cantine permet, par la même occasion, de contrôler qu'il va bien se nourrir.

Cette théorie pourrait s'apparenter à l'univers orwellien qui perçoit notre monde comme un « Big Brother », mais elle reste sans doute quelque peu exagérée. Même si les technologies de surveillance se sont multipliées dans le quotidien des individus, les organismes de protection des données veillent, pour l'heure, au juste équilibre entre le développement des activités technologiques dans la vie courante et la protection des données personnelles des individus.

34. Les empreintes digitales peuvent constituer des moyens de preuve lors d'un procès pénal, par exemple. Avec la multiplication des techniques biométriques dans la vie courante, ce moyen de preuve, a priori fiable pour l'utilisateur d'un dispositif biométrique peut s'avérer risqué en cas de détournement. L'auteur d'une infraction pourrait employer un leurre, alors il importe de connaître la force probante de la donnée biométrique ainsi que du fardeau de la preuve (B).

[73] X. Guchet, « Le pouvoir biométrique », Revue EcoRev n° 25, 22 oct. 2007, disponible sur le site internet de la revue, http://ecorev.org/spip.php?article611

B. Le fardeau de la preuve en biométrie

35. La preuve se définit comme « *la démonstration de l'existence d'un fait (matérialité d'un dommage) ou d'un acte (contrat, testament) dans les formes admises par la loi*[74] ».
Au terme de l'article 1315 du Code civil « *celui qui réclame l'exécution d'une obligation doit la prouver* ». En droit français, la preuve de l'exécution des obligations se fait différemment, selon qu'il s'agisse d'un acte ou d'un fait juridique.
Depuis la loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique[75], la preuve littérale « *résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission*[76] ». Cette loi instaure un principe de non-discrimination du support électronique vis-à-vis du support papier.

Si, pour les faits juridiques, cette loi ne pose guère de difficultés eu égard à un principe de liberté de la preuve, il n'en est pas de même concernant les actes juridiques. En effet, l'importance que revêt l'écrit dans les actes juridiques est considérable. De la signature d'un contrat de location, en passant par un testament ou bien un accord international, l'écrit a une forte valeur probatoire. Or, avec l'avènement de l'informatique associée aux télécommunications, la manière de négocier les contrats a profondément changé, tout comme les modes de stockage des données.
La biométrie n'est plus circonscrite à la matière pénale, mais elle peut servir à payer des achats et à fidéliser la clientèle[77]. Or, l'usage frauduleux d'une donnée biométrique pose des difficultés en matière de preuve.

36. L'identification d'une personne par l'emploi des éléments de son corps atteint une sûreté quasi absolue. La donnée biométrique est une donnée personnelle, unique et immuable tout comme les empreintes génétiques. Elle ne peut être modifiée, c'est un identifiant

[74] G. Cornu, Vocabulaire juridique, Association Henri Capitant, PUF, Quadrige, 2003.
[75] Loi n° 2002-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique, JO du 14 mars 2000
[76] C. civ., Art. 1316, loi du 13 mars 2000 précitée
[77] La CNIL vient d'autoriser à titre d'expérimentation à la Banque Accord, l'usage d'un dispositif biométrique reposant sur la reconnaissance du réseau veineux des doigts de la main afin de payer ses achats.
Article disponible sur le site internet de la CNIL au lien suivant : http://www.cnil.fr/dossiers/identite-numerique/fiches-pratiques/article/319/payer-avec-son-doigt-cest-possible/

permanent et, par voie de conséquence, irrévocable. La donnée biométrique a pour avantage, de permettre à l'individu de ne plus se soucier de la perte de son badge ou de son mot de passe mais a, pour inconvénient, de ne pouvoir être remplacée.

37. En théorie, un individu est maître de son corps. S'il peut effectuer des modifications de son apparence physique en ayant recours à la chirurgie esthétique, il ne peut, sauf accident, modifier ses données biométriques. Or, si les données biométriques sont employées pour effectuer des transactions en ligne et qu'elles sont dérobées lors de leur transmission par un serveur, comment le porteur légitime de ces données, pourra-t-il démontrer de bonne foi, en cas d'usage frauduleux, qu'il n'est pas à l'origine de l'infraction et démontrer les failles d'un système complexe dont il n'a ni la maîtrise ni la connaissance ? Qu'en est-il dans le procès pénal ? Existe-t-il une primauté de la donnée biométrique ? Il s'agit de s'attacher à la force probante de la donnée biométrique tant en matière pénale (1°) qu'en matière civile (2°).

1°. La force probante de la donnée biométrique en matière pénale

38. La preuve est « *ce qui persuade l'esprit d'une vérité*[78] ». Dans le procès pénal, la preuve revêt une importance capitale en ce qu'elle détermine la culpabilité ou l'innocence de l'individu. Toute personne poursuivie est présumée innocente tant que sa culpabilité n'a pas été prouvée. La charge de la preuve incombe au Ministère public ou aux parties civiles. Elle permet de démontrer l'existence d'une infraction et d'établir qui en est l'auteur. A la différence du procès civil, le procès pénal est régi par un principe de liberté de recherche et d'administration de la preuve. Ainsi, l'article 427 du Code de procédure pénale, relatif à l'administration de la preuve devant le tribunal correctionnel dispose que « *Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction* ».

Le juge décide d'après son intime conviction. Il ne peut fonder sa décision que sur des preuves qui lui ont été apportées au cours des débats et qui ont été contradictoirement discutées devant lui.

[78] J. Domat, « Les lois civiles dans leur ordre naturel », (1689), Paris, veuve Cavelier, t. 1, 1771, p. 204 in ENCINAS DE MUNAGORRI (R.), Introduction au droit, Flammarion, Champs Université, 2002, p. 277

39. La biométrie est souvent employée dans la recherche et l'administration de la preuve. Elle permet, notamment, de confirmer l'identification du prévenu avec une exactitude proche de 100%. Par exemple, les empreintes digitales ou génétiques, sont relevées sur des scènes de crimes et sont ensuite comparées avec celles contenues dans les fichiers relatifs aux empreintes digitales et génétiques (FNAED, FNAEG). La confirmation de l'identité de l'individu en fera au moins un témoin principal de l'affaire.
En développant la biométrie pour la sécurité des biens, des services ou des informations, les risques de détournement de données s'accroissent. En effet, les individus laissent quotidiennement des traces que ce soit des empreintes digitales, des cheveux ou de la salive et autres traces dans des lieux publics. Dans ce contexte, la donnée biométrique a-t-elle toujours la même force probante si elle peut être prélevée ou copiée ?

Nous pensons que la donnée biométrique a la même force probante peu importe le domaine dans lequel elle est employée. Les progrès de la science dans le domaine judiciaire ont mis les technologies de l'identification sur un piédestal. Néanmoins, il est à supposer que le magistrat prendra en compte l'affection croissante de la biométrie dans tous les domaines de la vie d'un individu pour statuer. Par ailleurs, la preuve n'est pas irréfragable et peut être renversée par tous moyens.

40. En droit commun, la charge de la preuve est comparée à un jeu de raquettes[79] où celui qui allègue un fait doit en apporter la preuve. Ce mécanisme pose des difficultés quant à la force probante de la donnée biométrique dans le procès civil (2°).

[79] F. Terré, Introduction Générale au droit, Précis Dalloz, 5ème édition 2000, p. 530.

2°. La force probante de la donnée biométrique en matière civile

41. Contrairement au droit pénal, en droit civil, la personne qui allègue le bénéfice d'un acte ou d'un fait juridique doit le prouver. L'article 1315 du Code civil fait une distinction entre la personne qui réclame l'exécution d'une obligation et celle qui se prétend libérée de cette dernière. L'alinéa 1er énonce que « *Celui qui réclame l'exécution d'une obligation doit la prouver* ». Ainsi, la charge de la preuve incombe au demandeur, ce que le droit romain formulait de la manière suivante : *actori incumbit probatio*.

Généralement, celui qui se réclame créancier d'une obligation, « le demandeur à la preuve[80] », coïncide avec le demandeur à l'instance. Il saisit le juge afin de faire valoir ses prétentions. L'alinéa second de l'article 1315 du Code civil énonce que « *réciproquement, celui qui se prétend libéré, doit justifier le paiement ou le fait qui a produit l'extinction de son obligation* ».

Dans la même idée, la personne qui se sera libérée de son obligation devra aussi en apporter la preuve. L'apport de la preuve se fait donc de façon alternative au cours des débats, tantôt du côté du demandeur, tantôt du côté du défendeur. Il s'agit du « renversement naturel » de la charge de la preuve.

En matière de dispositifs biométriques, nous manquons de recul sur d'éventuels litiges au plan civil, consécutifs à l'emploi de la biométrie comme moyen de preuve. Cependant, les règles traditionnelles du Code civil pourraient s'avérer insuffisantes voire injustes, par exemple, en matière de transactions en ligne. La personne usurpée qui demanderait réparation de son préjudice devrait prouver qu'elle n'a pas donnée ses empreintes digitales ou que les données qui lui ont été dérobées n'ont pas été utilisées par elle. Comment le porteur légitime pourra-t-il prouver qu'il n'a pas donné son empreinte digitale pour contester une transaction passée à son insu ?

Pour l'heure, tous les ordinateurs ne sont pas équipés de dispositifs de reconnaissance par empreinte digitale, mais nous pourrions imaginer, d'ici quelques années, que ces lecteurs se développent dans le cadre privé afin d'effectuer des transactions en ligne.

[80] Ibid.

Comme le soulève si bien A. Cavoukian, « *Use of biometric identification is interpreted by some as a questioning of their reputation and trustworthiness. They perceive a requirement to give a biometric as a reversal of the presumption of innocence – as shifting the burden of proof*[81] ». Pour garantir une certaine sécurité juridique, il faudra assurer au propriétaire des données la fiabilité des transactions en ligne ou le cas échéant une adaptation du droit de la preuve à ce nouveau domaine.

42. Comme nous l'avons observé, l'emploi de la biométrie fait encore l'objet de nombreuses craintes et interrogations. Son avenir est incertain et ses avancées souvent empiriques. Cependant, elle peut, aussi, être une technologie employée au service de la protection de la vie privée (C).

C. La biométrie, technologie au service de la protection de la vie privée

43. L'article 8 1° de la Convention européenne des droits de l'Homme énonce que « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance* ». Tous les moyens doivent être mis en œuvre afin de garantir l'effectivité de ces droits. Les promoteurs de systèmes biométriques avancent l'idée que la biométrie s'est installée progressivement en prenant en compte les craintes des citoyens en matière de sécurité. Les craintes grandissantes de la population, ont fait apparaître de nouveaux dispositifs dits « plus efficaces » mais sont-ils en adéquation avec les impératifs de protection des données personnelles ?

44. L'informatisation croissante de notre société pousse les personnes à mémoriser de nombreux mots de passe. Dans certaines entreprises, les mots de passe doivent être modifiés à intervalles réguliers pour en limiter les utilisations abusives. Les dispositifs d'authentification par mot de passe connaissent de nombreuses failles dans les systèmes de sécurité et tendent à être délaissés au profit de nouveaux dispositifs d'authentification biométrique. Ces derniers,

[81] « L'utilisation de l'identification biométrique est interprétée par certains comme une remise en question de leur réputation ou de leur probité. Ils perçoivent l'emploi des ces dispositifs comme un renversement de la présomption d'innocence - comme le renversement du fardeau de la preuve », A. Cavoukian Ph.D., "Consumer biometric applications : A discussion paper", Information and privacy commissioner/Ontario, Sept. 1999, disponible sur le site au www.ipc.on.ca

plus simples d'emploi garantissent tout autant l'anonymat des personnes puisqu'ils ne révèlent aucune information sur les personnes.
En effet, selon monsieur Nitsche-Ruggles, représentant de la société Sagem, la donnée biométrique est une donnée anonyme, un gabarit qui ne donne aucune information sur le sexe ou des éléments physiologiques de la personne. En effet, la donnée biométrique ne révèle aucune information sur la personne si ce n'est son identité dès lors qu'elle a été enrôlée.

L'International biometric industry association (IBIA)[82], créée en 1998, regroupe plusieurs catégories dont une majorité de personnes morales. La première catégorie est composée d'entreprises de développement et d'intégration d'appareils biométriques. La seconde regroupe des agences gouvernementales et des entreprises consultantes en biométrie. La troisième catégorie est composée de personnes privées. Cette association a pour vocation d'améliorer et de développer les pratiques ainsi que les règlementations dans le commerce et l'industrie à l'échelle internationale. Elle postule pour une meilleure protection des données biométriques et, à ce titre, fait des propositions par secteur d'activité.

Dans le secteur privé de la biométrie, IBIA préconise de développer des procédures uniformes en matière de collecte, de stockage, de traitement et de consultation des données biométriques, dans le seul but d'éviter la diffusion massive des données. Quant au secteur public, l'association estime que les conditions dans lesquelles les services nationaux collectent, traitent et stockent les données biométriques devraient faire l'objet de règlementations spécifiques, de sorte à préserver la confidentialité et l'intégrité des bases de données.

45. Selon le huitième rapport d'activité 2000-2001 du Préposé fédéral suisse à la protection des données personnelles (PFPDT) « *l'étude menée par une école d'ingénieurs mandatée par le PFPDT tend à démontrer que les systèmes d'authentification par empreinte digitale sont aujourd'hui techniquement au point et remplacent avantageusement l'authentification classique par mot de passe. Quelques lacunes de sécurité au niveau de leur intégration dans les systèmes d'exploitation ont néanmoins été constatées. Ces défauts de jeunesse disparaîtront bien vite car ces nouvelles techniques d'authentification biométrique*

[82] International Biometric Industry Association, http://www.ibia.org/

sont le seul espoir de progrès dans le domaine de la sécurité d'accès aux innombrables services électroniques proposés sur le marché ».

La biométrie peut être un outil de protection de la vie privée, en ce qu'elle permet aux individus qui l'utilisent, de protéger leurs données, leurs biens ou leur identité, en cas de vol de leur passeport, par exemple.

46. Les différents motifs évoqués précédemment comme l'anonymat des données et la facilité d'emploi de ces systèmes ont concouru à l'avènement et au développement des dispositifs biométriques comme moyen d'identification. Néanmoins, les autorités mondiales de protection des données, comme la Commission nationale de l'informatique et des libertés (CNIL) en France, craignent qu'il y ait un détournement des données personnelles, par l'abus de l'usage de ces technologies, désormais employées dans les entreprises. Pour cela il importe de contrôler l'intégration des dispositifs biométriques et de garantir aux salariés l'exercice de leurs droits et la protection de leurs données (chapitre 4).

Chapitre 4. Position du problème

47. Un constat peut d'ores et déjà être fait : l'usage de la biométrie bouleverse totalement les modes traditionnels d'identification de l'homme. Alors que pendant des décennies, seule la carte d'identité en France suffisait à se faire reconnaître par son nom et sa photographie, les personnes doivent désormais prouver qui elles sont par l'emploi de dispositifs biométriques.

La société européenne et, petit à petit la société mondiale, sont entrées dans « l'ère de l'identification biométrique » et plus officiellement, sous l'impulsion des Etats-Unis d'Amérique, avec l'obligation de détenir un passeport biométrique, indispensable sésame pour pénétrer sur leur territoire.

La donnée biométrique est une donnée d'identité. Contrairement aux autres données d'identité ou données à caractère personnel, la donnée biométrique n'est pas choisie par l'individu, ni attribuée par un tiers. Elle représente les caractères fondamentaux de l'individu que lui seul peut générer, de façon unique et immuable.

A l'inverse des données génétiques, elle ne divulgue aucune information sur l'état de santé des personnes ou sur leur origine, mais, détenue par un porteur illégitime, elle ne permet plus de garantir l'identité de la personne. Dès lors, nous percevons plus aisément les craintes associées à l'emploi de la biométrie par l'Etat, dans la vie courante ou sur le lieu de travail. Le détournement ou le mauvais usage de cette donnée fait peser des risques considérables sur la fiabilité de l'identité de l'individu, de telle sorte que le remède pourrait être pire que le mal.

Le risque de corruption ou de divulgation de cette donnée est très sensible selon la technologie employée. Les empreintes digitales, par exemple, sont déposées quotidiennement dans différents lieux publics ou privés et peuvent être copiées grâce à des kits de relevé d'empreintes, en vente sur l'Internet[83].

[83] Comme nous le verrons ultérieurement il n'est pas non plus si aisé de créer une fausse empreinte. Cela nécessite du matériel mais aussi une certaine technicité.

Par ailleurs, la biométrie n'est plus circonscrite aux seuls passeports ou à quelques objets du quotidien. Elle s'est fortement développée ces dernières années et touche de plus en plus le monde du travail, dans le but de sécuriser les informations, les sites mais aussi d'améliorer l'organisation et la gestion des ressources humaines.

48. Il existe trois niveaux de développement de la biométrie en France[84] : L'Etat, l'entreprise et les individus. En matière de biométrie, l'Etat possède des règles propres sur lesquelles la CNIL n'a qu'un avis consultatif qu'il s'agisse de fichiers ou de passeports biométriques. L'individu, dans la sphère privée, choisit librement d'avoir recours à la technologie biométrique, il dispose intégralement de la maîtrise de sa donnée biométrique, lecteur biométrique sur ordinateur, serrures diverses etc., sans qu'il courre un grand risque de détournement.

L'entreprise, en revanche, va avoir la faculté de collecter les données biométriques de ses salariés et éventuellement celles de consommateurs. Par le biais de ses filiales, elle peut aussi faire circuler ces données à travers la planète, dans le cadre d'opérations de transferts de données ou de fusion d'entreprises. Les possibilités qui lui sont offertes sont grandes et avec elles, les risques inhérents à l'usage non maîtrisé de ces données. L'entreprise constitue donc « un laboratoire » idéal d'étude en matière de biométrie associé à la protection des données personnelles. C'est pourquoi nous avons fait le choix, d'étudier uniquement les traitements de données biométriques au sein des entreprises.

Les données personnelles qui circulent au sein des entreprises sont diverses et variées qu'elles soient d'identité, professionnelles ou biométriques pour certaines entreprises. Les risques de divulgations se sont multipliés avec l'usage des ordinateurs et, plus largement, des nouvelles technologies. Il faut, par ailleurs, distinguer plusieurs seuils de sensibilité, selon le stockage des données, sur un support individuel dont l'individu a la garde et la responsabilité ou dans une base de données qui échappe à son contrôle. Alors que les salariés, dans leur vie privée, peuvent choisir ou non d'avoir accès à la biométrie (passeport ou choix d'un dispositif biométrique), ce choix est moins évident sur le lieu de travail.
L'Etat français a laissé à la CNIL la mission d'établir un cadre juridique collectif de contrôle quant au développement des dispositifs biométriques. Pour la CNIL, le concept de traces et de

[84] Ces niveaux existent aussi par exemple pour le Canada ou l'Australie.

traçabilité est très intéressant, car pour l'heure, il fonde en grande partie, les autorisations de l'emploi ou non d'outils biométriques, au regard de la protection des données personnelles. Les principes fondateurs de la doctrine de la CNIL sont la finalité du dispositif, son caractère proportionnel, la sécurité des données ainsi que l'information et le consentement des personnes.

Au travers des différentes demandes d'autorisation préalable, la CNIL a dû adapter à la biométrie des principes déjà existants pour d'autres domaines de la protection des données personnelles. Or, les technologies biométriques évoluent si rapidement que l'on peut s'interroger sur la réelle adaptation des principes « traditionnels » de protection des données personnelles à ces traitements.

Il ne faut pas oublier que l'enjeu du développement de ces technologies est international. Tandis qu'un cadre juridique trop rigide desservirait les industriels, un cadre juridique trop souple mettrait en jeu le respect de la vie privée et la protection des données des salariés. L'Union européenne coopère avec les Etats-Unis, notamment pour l'uniformisation de bonnes pratiques « informatique et libertés », à l'instar des principes « Safe Harbor ». Cependant, ce n'est pas suffisant, des risques de divulgations persistent. A l'ère de la mondialisation, la biométrie a vocation à se développer au sein des entreprises qui voient dans ces techniques, une garantie quasiment infaillible d'identification des individus, gage de sécurité, ainsi qu'une aide à la gestion et à l'organisation. En somme, la biométrie lie rendement et protection. Il importe que la rentabilité ne prenne pas le pas sur l'information et le consentement des salariés.

L'information et le consentement des personnes sur l'intégration de la biométrie au sein de l'entreprise sont-ils suffisants ? Quelles mesures sont prises à l'égard des transferts de données transfrontaliers, lorsqu'une entreprise constitue une base de données ? Sur ces questions les Etats-Unis d'Amérique, le Canada et l'Australie n'ont pas les mêmes considérations au regard des données biométriques. Il est donc indispensable d'avoir une approche homogène, pour une meilleure coopération et une meilleure évaluation des risques encourus.

49. La technologie met, encore et toujours, le droit au défit de faire cohabiter l'emploi de dispositifs biométriques avec la protection des données personnelles des salariés. Ce défi passe nécessairement par un contrôle de l'usage de la biométrie non seulement collectif mais aussi individuel. Le contrôle est « *la vérification de la conformité à une norme d'une décision, d'une situation, d'un comportement* [85]».

Le contrôle est collectif, dès lors que l'Etat a donné à la CNIL la mission de vérifier l'intégration des dispositifs biométriques en entreprise et de rendre un avis qu'il soutiendra entièrement. C'est en ce sens que l'on se rend compte du réel contrôle de la Commission, puisqu'elle seule est chargée d'attribuer des autorisations préalables ou des déclarations de conformité et de sanctionner les entreprises contrevenantes (Titre I) Par ailleurs, la loi Informatique et libertés et le Code du travail donnent aux salariés la faculté d'exercer un contrôle individuel sur leurs données personnelles et sur l'exercice du droit d'accès, de communication, de rectification voire d'effacement de ces données.

Ce double contrôle, de la CNIL d'une part et du salarié d'autre part, assure l'intégration raisonnée des dispositifs, tout en garantissant les droits des salariés et notamment en les encourageant à exercer ces derniers (Titre II).

[85] G. Cornu, Vocabulaire juridique, Association Henri Capitant, PUF, Quadrige, 2003.

TITRE I. L'encadrement collectif de l'usage de la biométrie en entreprise

« *On mettra des gardes à la porte de la Cité.*
On mettra des gardes pour garder les gardes.
Mais qui gardera les gardes des gardes ? [86] »

50. A cette interrogation nous pourrions être tentés de répondre que la biométrie, au sein des entreprises, fait actuellement office de « garde des gardes ». Le déficit de confiance en l'homme, déjà mis en exergue par Saint Augustin, a, de nos jours, abouti au recours à la machine, pour « garder » les biens, les informations et les personnes. Les entreprises ont trouvé en la biométrie, un outil de plus, qui supplante les personnels habituellement chargés de la sécurité. La vidéosurveillance, la géolocalisation, les puces sans contacts, ont balisé le chemin des technologies dites « de surveillance ».

51. La loi Informatique et libertés n° 78-17 du 6 janvier 1978 modifiée par la loi du 6 août 2004 qui transpose la directive communautaire du 24 octobre 1995, s'applique à ces nouveaux défis informatiques.
Par ce biais, le législateur a laissé le soin à la CNIL, d'établir un contrôle collectif de l'usage de dispositifs biométriques au sein des entreprises. Les procédures de création ont été renforcées et les principes de protection des données personnelles tels que la finalité, la proportionnalité ou l'information des personnes ont été réaffirmés.

52. La profusion d'outils biométriques révèle l'existence d'une réelle demande de sécurité (Chapitre préliminaire) si bien qu'un chef d'entreprise avisé en matière de nouvelles technologies pourrait y perdre ses réelles intentions.
Dans un souci d'équilibre entre les intérêts économiques d'une entreprise et la protection des données personnelles des salariés, il est nécessaire, de placer au centre des demandes d'autorisation, les principes de finalité et de proportionnalité.
Le principe de finalité, doit être observé non pas comme une fin en soi, mais comme un moyen préalable de sonder les justifications de l'emploi de la biométrie (Chapitre 1er) avant

[86] Saint Augustin, La Cité de Dieu, édition Charpentier, 1855.

d’apprécier la proportionnalité du dispositif. Le principe de proportionnalité est le principe vecteur des bonnes pratiques « informatique et libertés » (Chapitre 2).

Chapitre Préliminaire. Les différentes techniques biométriques

« *Le marché national ne soutient pas suffisamment les développements possibles de ces technologies à cause des faibles budgets qui ont été jusqu'alors consacrés par les pouvoirs publics et par une législation contraignante.*
L'objectif est d'augmenter la sécurité tout en évitant de nuire à la liberté de chacun, l'informatique et la biométrie devraient y parvenir.
Le politique doit assouplir la législation afin de favoriser le développement des technologies de la sécurité électronique et informatique[87] »

53. Pendant longtemps, l'emploi des techniques biométriques était cantonné à l'usage militaire ou policier. Les gouvernements tentent d'avoir une emprise sur la criminalité. Ainsi, le leitmotiv sécuritaire justifie les atteintes à la vie privée. Les individus sont filmés plusieurs dizaines de fois dans la journée, sans pouvoir manifester leur volonté de s'opposer à de telles mesures. La biométrie s'installe progressivement, tant dans la sphère publique que dans la sphère privée.

54. La biométrie ne se limite plus à la sécurité aéroportuaire mais tend à s'étendre dans d'autres domaines tels le travail, le milieu hospitalier, ou les cantines scolaires, pas uniquement pour des mesures sécuritaires, mais aussi pour des raisons de facilité de gestion. Dans la sphère privée, elle s'étend aussi avec de nouvelles technologies de serrures biométriques pour automobiles, téléphones mobiles, ordinateurs et bien d'autres objets du quotidien. Elle est aussi bien employée pour l'authentification que pour l'identification des individus[88].
Le débat sur les dispositifs biométriques est d'abord de nature technique, avec des interrogations relatives à la fiabilité et à la performance accrue de la biométrie, face aux techniques déjà en place.

[87] Industries électroniques et numériques, Grands programmes structurants, Livre bleu, Juil. 2004, p. 35
[88] L'authentification n'existe pas dans la langue française. Il s'agit d'un anglicisme employé par opposition à l'identification, toutefois nous emploierons ce terme à plusieurs reprises au cours des développements pour nous conformer au vocabulaire technique. Il s'agit d'une identification biométrique. Elle est jugée moins intrusive, car elle revient à vérifier, à l'aide du dispositif biométrique, que le porteur d'une carte d'identification en est bien le propriétaire légitime. La machine procède à une simple vérification entre deux données. Ce mode est appelé « 1 contre 1 ». Une donnée sera confrontée à une autre donnée, toutes deux détenues par la même personne.

Parmi les différentes techniques biométriques existantes, lesquelles garantissent le plus la sécurité et la protection des données personnelles ?

55. Les industriels tentent aujourd'hui de forcer les verrous posés par la CNIL, afin de créer de nouveaux fichiers, internes aux entreprises, dans lesquels résideraient les données biométriques des différents salariés. Il y a une propagation contrôlée des différents usages de la biométrie (section1), tant qu'un consensus n'a pas été trouvé en matière de sécurité et de fiabilité. Toutefois, cela n'empêche en rien le développement de la biométrie dans différentes applications (section 2).

Section 1. La propagation contrôlée des outils biométriques

56. Dans le rapport rendu par l'Office parlementaire d'évaluation des choix scientifiques et technologiques de l'Assemblée nationale[89] intitulé « *Méthode scientifique d'identification des personnes à partir de données biométriques et techniques de mise en œuvre* », M. Christian Cabal constate le développement grandissant des outils biométriques, leur automatisation et leur élargissement au-delà des applications militaires ou policières. Il relève à ce titre que « *l'utilisation de la biométrie apparaît comme un élément utile voire indispensable aux autorités publiques de l'État ou des États, dans la nécessité qui est la leur, conformément aux lois qui régissent nos sociétés, de savoir si tel individu est bien celui qu'il prétend être et s'il est habilité à entreprendre un certain nombre d'actions correspondant à notre vie sociale en général*[90] »

57. L'usage de la biométrie paraît indispensable, en l'occurrence lorsqu'il s'agit de filtrer et de contrôler l'immigration. La loi du 24 novembre 2003 relative à l'immigration a réformé les méthodes d'identification des étrangers, et les procédures de vérification des visas.

[89] C. Cabal, Rapport de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur « Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre. », Assemblée nationale n° 938, Sénat n° 355, juin 2003
[90] Ibid. 3ème partie du rapport, p. 31

Après l'usage de la biométrie dans l'aviation civile pour le personnel naviguant, elle a commencé à être employée pour surveiller les frontières et les empreintes génétiques ont fait l'objet d'un débat[91].

La loi du 24 avril 1997 avait déjà prévu la possibilité de relever, de conserver et de traiter sous forme informatique, les empreintes digitales des demandeurs de titres de séjour, ainsi que celles des étrangers en situation irrégulière ou faisant l'objet d'une mesure d'éloignement du territoire. Ces dispositions, introduites dans l'ordonnance du 2 novembre 1945 (article 8-3), n'ont reçu aucune application à ce jour.

58. L'article 8-3 autorise également les agents expressément habilités du ministère de l'Intérieur ou de la gendarmerie à consulter, « *dans les conditions fixées par la loi du 6 janvier 1978* », le Fichier automatisé des empreintes digitales (FAED), géré par le ministère de l'Intérieur, afin d'identifier les étrangers, en situation irrégulière ou faisant l'objet d'une mesure d'éloignement ou encore qui n'auraient pas présenté les pièces justificatives nécessaires. Cette consultation n'a pas non plus, semble-t-il, été mise en œuvre. Les nouvelles dispositions introduites en 2003 étendent la possibilité de prise d'empreintes digitales et de leur traitement, aux étrangers qui, ayant été contrôlés à l'occasion du franchissement de la frontière, ne sont pas munis des documents et des visas d'entrée nécessaires, ou ne remplissent pas les conditions d'entrée sur le territoire, au sens de l'article 5 de la convention de Schengen du 19 juin 1990.

59. Pour comprendre les implications de l'usage des outils biométriques, il est nécessaire d'analyser préalablement le fonctionnement de ces dispositifs. Le choix du plan suivant n'est en rien traditionnel car il est lié essentiellement à la chronologie du traitement technique des empreintes digitales (A, B), aux erreurs des systèmes biométriques (C) ainsi qu'à la problématique des leurres qui peuvent être fabriqués pour voler l'identité d'un individu (D). Par ailleurs, nous faisons le choix de concentrer la majeure partie des développements de cette section sur l'empreinte digitale tant les implications pour la protection des données personnelles sont grandes. Néanmoins, nous traiterons le

[91] C. Cabal, « La valeur scientifique de l'utilisation des empreintes génétiques dans le domaine judiciaire », n° 3121 Assemblée nationale (11ème législature) et Sénat n°94 (2001- 2002), disponible sur le site www.senat.fr

fonctionnement des autres modalités biométriques (E), qui engendrent a priori moins de difficultés en matière « informatique et libertés » que le traitement des empreintes digitales.

A. La technique de reconnaissance par empreinte digitale

60. La technique biométrique de reconnaissance par empreinte digitale est la plus employée à travers le monde. C'est la technologie la plus aboutie et la plus connue du grand public, de part sa popularité dans diverses séries policières, notamment outre-Atlantique. La formation (1°) et la capture (2°) de l'empreinte digitale devront être développées afin de mieux appréhender les risques corrélatifs à sa collecte.

1°. La formation de l'empreinte digitale

61. « *Les empreintes digitales sont des dessins formés par la peau sur les doigts*[92] ». Ce dessin apparaît dès la treizième semaine de la vie intra-utérine et restera le même tout au long de la vie, il ne fera que grossir au fur et à mesure du développement physique de l'individu.

Les circonvolutions des crêtes, donnant ce dessin à l'empreinte digitale, ne sont pas seulement dues au bagage génétique. Il faut aussi prendre en considération le phénotype[93], c'est-à-dire le résultat combiné du génotype[94] et des pressions environnementales. Dès lors, la pression sanguine, le stress ou l'alimentation du fœtus étant différents d'un individu à un autre, deux jumeaux monozygotes ne peuvent avoir des empreintes digitales identiques même si, toutefois, elles peuvent avoir des points similaires.

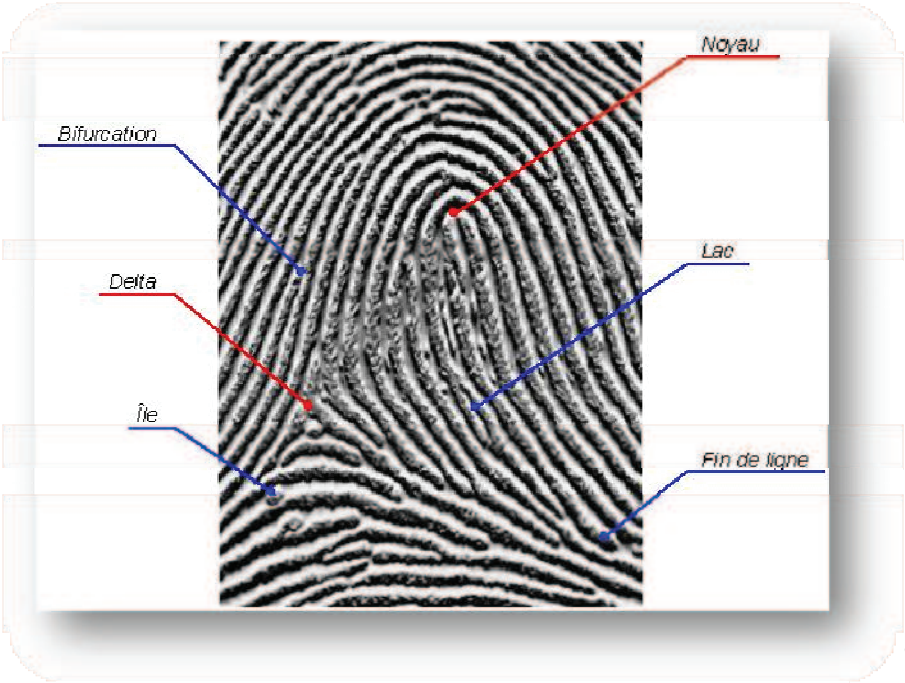
A cause de ces aspects aléatoires, l'empreinte digitale est unique et immuable pour chaque individu. Ses caractères font d'elle un mode d'identification fiable et constant.

---

[92] J. Pierson, « La biométrie, l'identification par le corps », Coll. Informatique, Hermès Science, Lavoisier, 2007, p. 74

[93] « *Ensemble de caractères anatomiques, physiologiques et antigéniques permettant d'identifier et de classer chaque type de bactérie ou de virus* », définition disponible sur le site Larousse en ligne au www.larousse.fr

[94] « *Ensemble des caractères génétiques d'un être vivant, qu'ils se traduisent ou non dans son phénotype* », disponible sur le site www.larousse.fr



95

62. Pour que cette fiabilité soit garantie, plusieurs étapes doivent être effectuées. La première concerne la capture de l'empreinte digitale (2°).

2°. La capture de l'empreinte digitale

63. L'informatique a contribué au développement accru de la biométrie, en ce sens que le temps d'acquisition du gabarit[96] a été considérablement réduit. Actuellement il faut en moyenne quelques millisecondes à partir d'un ordinateur pour identifier un individu. Ce qui signifie qu'il est possible de parcourir des millions d'empreintes digitales par heure. Cette rapidité est non négligeable lorsqu'il est question de l'identification de plusieurs milliers de personnes quotidiennement[97].

[95] Détail d'une empreinte digitale : site internet biométrie online www.biometrie-online.net, tous droits réservés.
[96] Le gabarit biométrique ou template en anglais est la mesure initiale effectuée par le lecteur biométrique lors de l'enrôlement. Les données enregistrées sont appelées le gabarit biométrique.
[97] L'exemple des aéroports américains en est la démonstration

64. La technique de capture de l'empreinte digitale peut être « aisée[98] » pour celui qui dispose du matériel informatique et des connaissances. C'est un état de fait qui inquiète la CNIL.

L'empreinte digitale est une trace générée par le corps humain, parmi toutes les traces qui sont laissées au quotidien, par l'individu, à son insu: on parle alors d'empreinte latente, que l'on peut aisément voir sur un support transparent en verre.

L'encre et le papier ont longtemps été utilisés par les policiers - et le sont encore - dans le but de créer une fiche décadactylaire.



[99]

L'étude de ces empreintes se fait en détaillant différents points. Les points de jonction, qui sont les bifurcations sont appelées « minuties ». Une douzaine de minuties peut suffire à identifier un individu. Les empreintes latentes ne sont pas toutes visibles à l'œil nu. Elles sont générées naturellement par le sébum de la peau ou par des graisses diverses. Seulement 10% de ces traces sont visibles à l'œil nu. Pour le reste il convient d'utiliser un mode de révélation efficace.

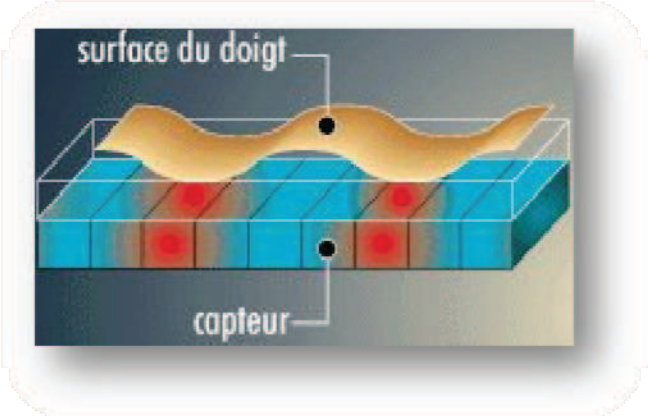
Selon Jacques Pierson[100], la méthode la plus couramment employée pour capturer les empreintes digitales consiste à combiner un prisme, un système d'éclairage, une lentille et une caméra. Le doigt est posé sur l'une des parois du prisme. La lumière, produite en général par

[98] Moyennant du matériel. Il n'est pas toujours évident d'y parvenir concrètement.
[99] Site Internet de Jean-François Mainguet : http://pagespersoorange.fr/fingerchip/biometrics/types/fingerprint_sensors_type.htm. Tous droits réservés.
[100] J. Pierson, « La biométrie, l'identification par le corps », Coll. Informatique, Hermès Science, Lavoisier, 2007

des LEDS et réfléchie par le doigt posé sur le prisme, est envoyée vers un capteur optique (CMOS) après concentration par une lentille.

Cependant, une difficulté existe : le capteur peut déformer l'image. Certains autres facteurs environnementaux peuvent l'affecter, comme la saleté s'accumulant au fur et à mesure du temps ou l'humidité.

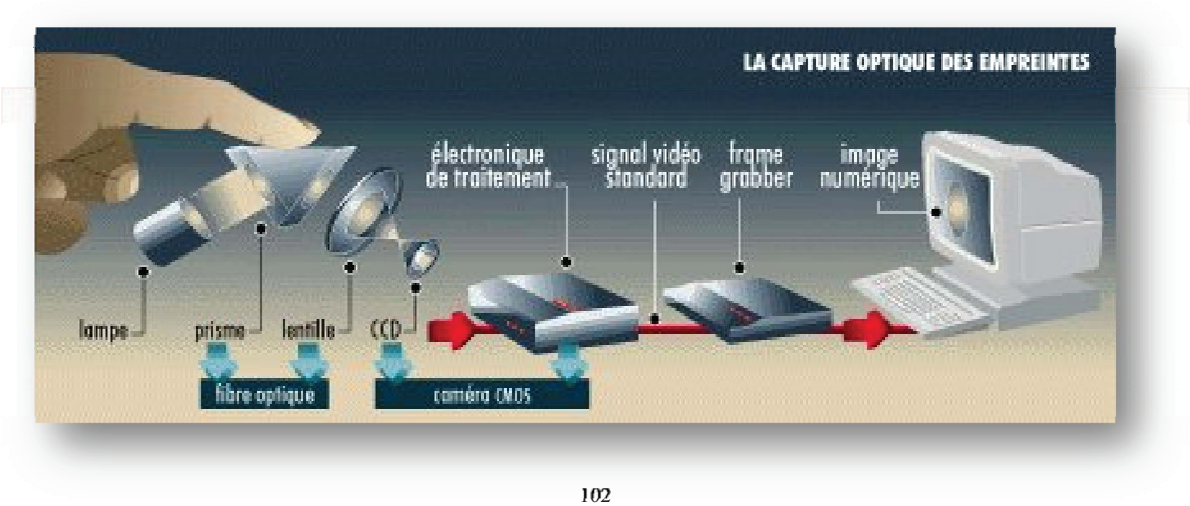
65. Les progrès technologiques en la matière permettent d'avoir une multitude de procédures de capture dont il convient de présenter les principales applications pratiques.



101

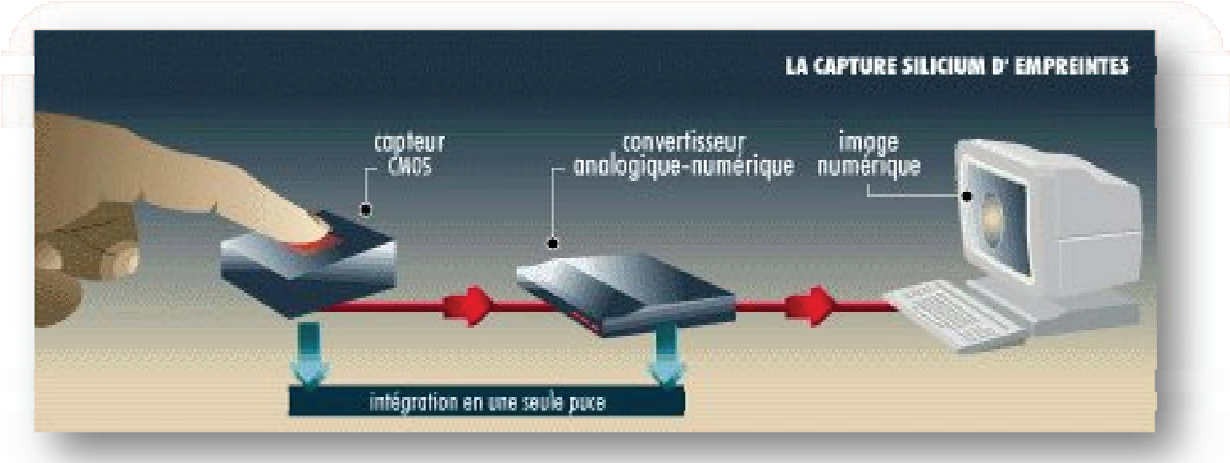
En premier lieu, il y a les capteurs optiques : caméras CCD, CMOS. Le doigt est apposé sur une platine en plastique dur ou en quartz qui capture l'image. Ce procédé est le plus ancien après l'encre. Il est fréquemment utilisé par les autorités judiciaires pour la qualité des images.

[101]J.F. Mainguet: "Une puce pour les empreintes digitales", La Recherche, Septembre 98 (312) p.46. Procédure de capture d'une empreinte digitale par capteur thermique. Tous droits réservés.



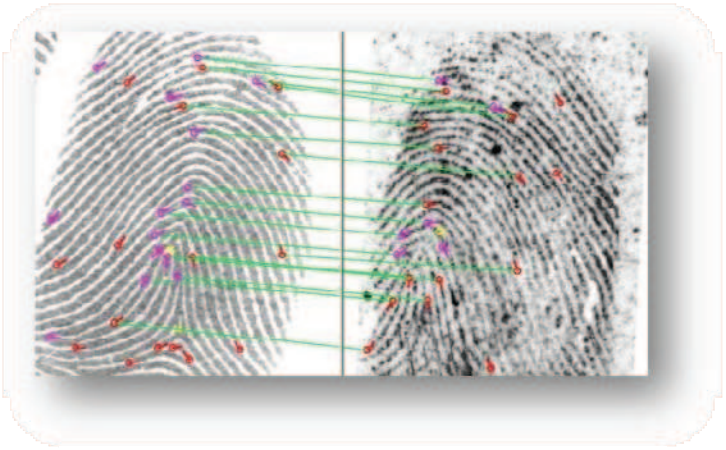
102

En second lieu, l'empreinte digitale peut être capturée par un lecteur en silicium qui a pour avantage d'être de petite taille et d'un coût relativement intéressant. Ce matériel peut utiliser plusieurs phénomènes physiques, l'effet capacitif étant le plus couramment employé, mais il existe également des capteurs thermiques. Ceux-ci permettent de capturer une image d'une grande qualité même avec des empreintes dites « difficiles » car elles ont un relief abîmé.



103

[102] J.F. Mainguet: "Une puce pour les empreintes digitales", La Recherche, Septembre 98 (312) p.46. Tous droits réservés.
[103] J.F. Mainguet: "Une puce pour les empreintes digitales", La Recherche, Septembre 98 (312) p.46. Tous droits réservés.



104

66. Le traitement des empreintes digitales s'effectue en plusieurs étapes (B).

B. Les étapes du traitement de l'empreinte digitale

67. Afin d'employer un dispositif de reconnaissance par empreintes digitales, l'utilisateur doit se soumettre à un enrôlement (1°) avant de procéder à la capture live[105] (2°) puis à la comparaison avant d'être, à l'issu, accepté ou non par le système (3°).

1°. L'enrôlement[106]

68. Pour que l'enrôlement soit correctement effectué, il est nécessaire d'enregistrer une identification « témoin », de préférence de bonne qualité qui servira de référence ultérieure. Pour l'obtenir, il faut procéder à l'enrôlement. C'est la première étape essentielle de toute identification biométrique.

---

[104] J.F. Mainguet. Tous droits réservés. Image d'une comparaison d'empreintes digitales. Cette image représente un « matching » c'est-à-dire une comparaison entre deux empreintes selon des points de concordance. A gauche il s'agit d'une image saisie par un capteur et le vrai doigt. A droite, il s'agit d'une empreinte latente récupérée et numérisée. Ici le « matching » est largement positif.

[105] La « capture live » est un anglicisme, il représente l'étape durant laquelle la capture de l'image s'effectue et est transformée en gabarit biométrique. Il n'y a pas d'équivalent français pour ce terme.

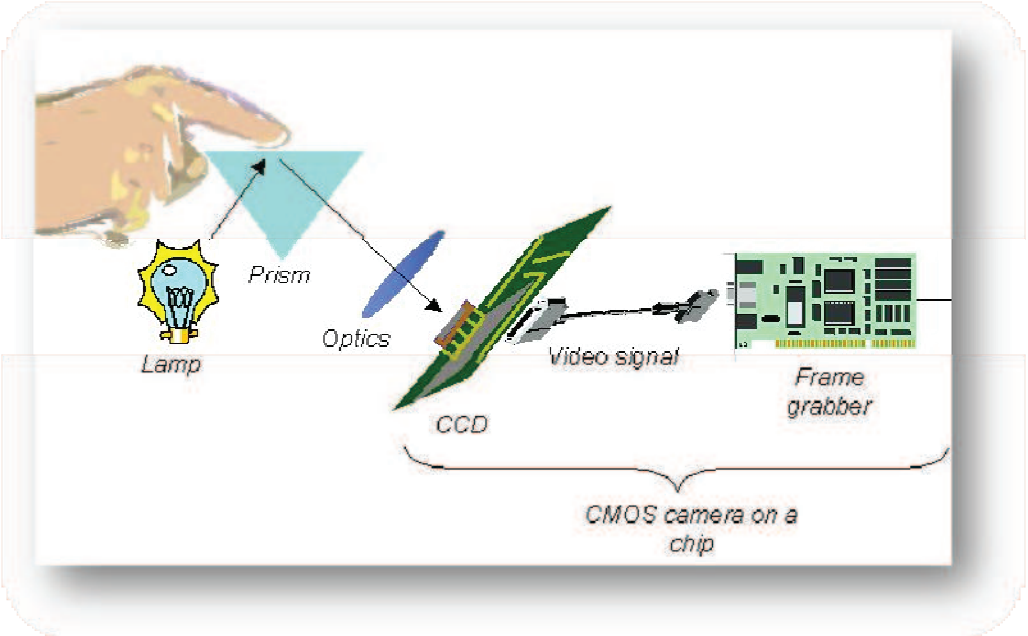
[106] C'est l'« *étape initiale au cours de laquelle sont capturées les données biométriques qui serviront de références lors des authentifications ou identifications futures. C'est aussi lors de cette étape qu'un identifiant est associé aux données biométriques de chaque personne. Un soin tout particulier doit être apporté à cette première capture, car c'est sa qualité qui déterminera les performances futures du système*», définition issue du site internet biometrie-online, disponible sur le site internet au www.biometrie-online.net

Concrètement, l'individu pose son doigt sur le capteur afin de saisir son empreinte (Ceci a été évoqué dans le paragraphe précédent) pour la réduire et la transformer en code informatique, nommé gabarit. Il s'agit, en fait, de la liste des minuties dans la plupart des systèmes basés sur les empreintes digitales. On peut en trouver de vingt à cent dans une image selon la surface de l'empreinte capturée.

69. Une seconde capture appelée « capture live », va permettre de constituer le gabarit biométrique qui sera conservé plus tard (2°).

2°. La capture live

70. La deuxième étape du traitement consiste à effectuer une nouvelle capture. La nouvelle empreinte qui en découle est dite « live ». Elle est réduite et transformée en gabarit de la même manière qu'à l'enrôlement.



[107]

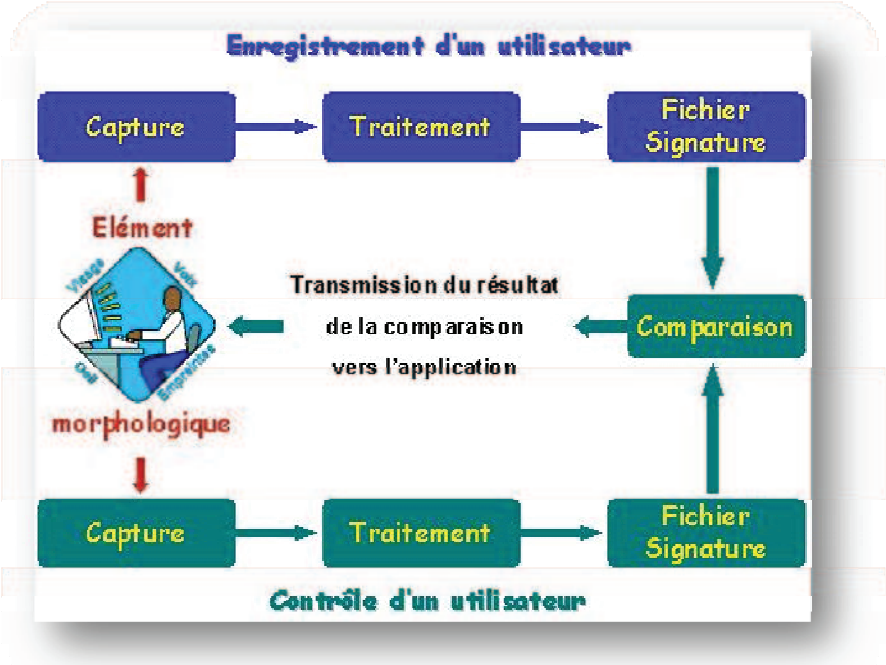
[107] Image représentant la capture « live ». Site Internet de Jean-François Mainguet http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint_sensors_physics.htm. Tous droits réservés.

71. La capture live s'effectue traditionnellement comme ci-dessus, par la réflexion totale du doigt sur le prisme en verre. Lorsque la peau touche le verre, la lumière n'est alors plus réfléchie, mais absorbée. Le doigt est éclairé à l'aide d'une diode électroluminescente par un côté du prisme. De l'autre côté, l'image est récupérée à l'aide d'une lentille et d'un capteur d'images.

72. Enfin, une comparaison doit être effectuée pour permettre à l'intéressé d'être identifié (3°).

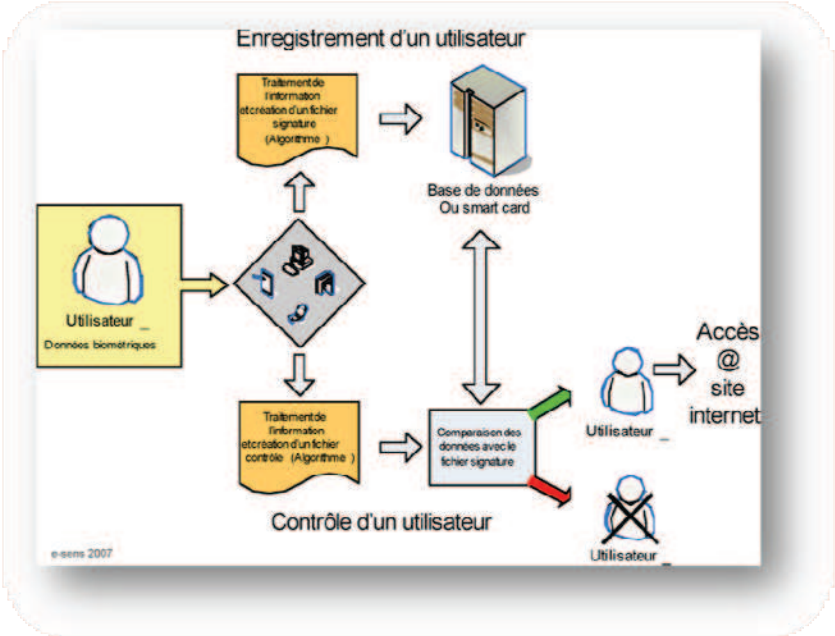
3°. La comparaison

73. On réalise alors une comparaison : ce processus vise à examiner les rapports de ressemblance – ou de différence – entre l'empreinte digitale « live » réduite digitalisée et celle, déjà existante, dans la mémoire numérique, la référence.



108

[108] Site internet biométrie-online : http://www.biometrie-online.net, tous droits réservés.



[109]

74. Selon Jacques Pierson[110], une minutie est caractérisée par deux informations :
D'une part, sa position spatiale dans l'image, qui correspond à deux coordonnées, abscisse et ordonnée, et se trouve définie par le point de bifurcation ou le point d'arrêt de la ligne.
D'autre part, son orientation, qui constitue la direction des lignes de l'empreinte digitale localement, mais avec un sens à cette direction.

75. On compare alors les deux jeux de minuties : celui enregistré à l'enrôlement et celui obtenu à partir de l'empreinte « live ». Plus le nombre de minuties en commun est important entre l'image capturée et celle enregistrée, plus il y a de probabilités que les empreintes relevées soient identiques à celles enregistrées dans une base de données. On utilise alors un seuil de décision.

76. Malgré le respect des différentes étapes, la biométrie n'a pas une fiabilité totale et laisse apparaître des probabilités d'erreurs (C).

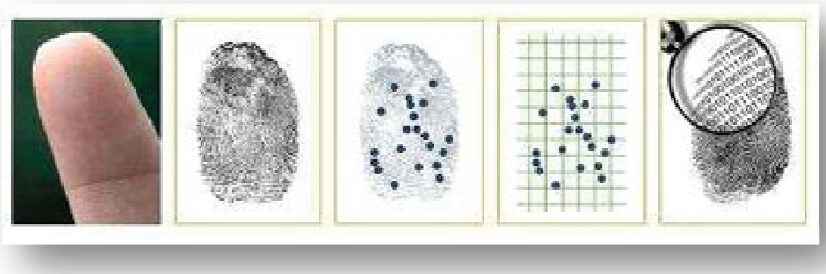
[109]Processus d'enregistrement et de contrôle d'un utilisateur. Site Internet http://e-sens.unige.ch/uploaded/image/img_schema_biometrie.jpg. Tous droits réservés.
[110] J. Pierson, « La biométrie, l'identification par le corps », collection informatique, éditions Hermès science et Lavoisier, p. 95

C. La probabilité d'erreur d'un système biométrique

77. La fiabilité d'une technique biométrique, dans le domaine du contrôle d'accès, est appréciée au regard de deux notions.
En premier lieu, le taux d'acceptations erronées (FAR : False Acceptance Rate) : deux relevés biométriques de personnes différentes sont déclarés concordants. Le score de comparaison des deux données est supérieur au seuil initialement configuré, ce qui conduit à l'acceptation d'une personne qui n'est pas la bonne. C'est un problème de sécurité, le taux doit être aussi faible que possible.

En second lieu, le taux de rejets erronés (FRR : False Reject Rate) : deux relevés biométriques de la même personne sont déclarés non concordants. C'est un problème de commodité et non de sécurité. L'utilisateur devra peut-être recommencer son identification.

Ces deux taux varient en fonction de la technologie et de la méthode d'utilisation employées. La reconnaissance sera effective, si la population à identifier a des empreintes digitales lisibles et si le réglage réalisé lors de la capture correspond au choix du nombre de points concordants.



[111]

78. Au-delà des taux d'erreurs, il existe les leurres qui peuvent amener le système à accepter une personne qui ne devrait pas l'être (D).

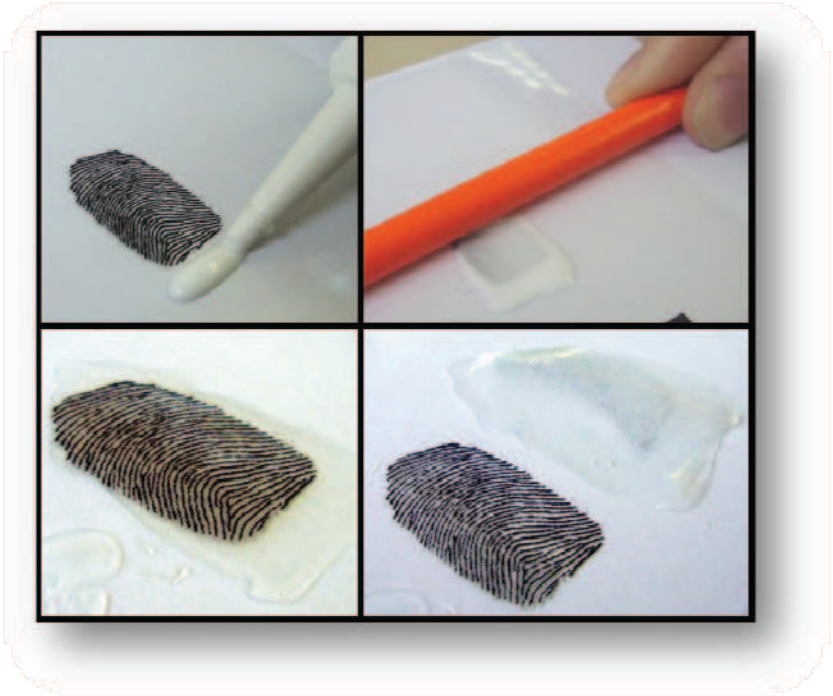
[111] Extraction et comparaison des minuties d'une empreinte digitale : http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint_algo.htm. Tous droits réservés.

D. Les leurres

79. La technicité du traitement de l'empreinte digitale étant expliquée, il subsiste alors la question des leurres.

Un leurre est la falsification d'un procédé technique, en l'espèce, une empreinte digitale visant à amener le système à reconnaître une personne illégitime comme étant légitime. Cette personne aura employé différentes techniques, pour s'introduire frauduleusement dans le système. Ces techniques seront survolées ultérieurement dans le développement.

Cette problématique a été énormément médiatisée dans les années 2001 et 2002, en montrant « l'aisance » avec laquelle une empreinte digitale peut être falsifiée. Les différents articles publiés sur le sujet ont jeté le discrédit sur la biométrie.

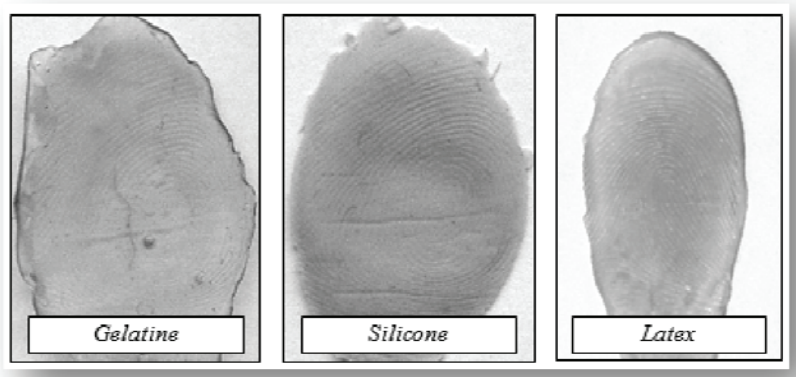


[112]

En effet, il est permis de s'interroger sur l'utilité de puissants algorithmes de cryptage, si lors de l'enrôlement ou de la reconnaissance, rien n'assure que le doigt apposé soit bien constitué de chair et de sang.

[112] Image issue d'un article publié par Jean-François Mainguet intitulé « Fake fingerprints » au sein de l'Encyclopédia of Biometrics, p. 458 et suivantes.

Heureusement, la plupart de ces leurres sont détectables, encore faut-il que les contre-mesures aient été correctement installées dans le système.



[113]

80. La copie d'une empreinte digitale, appelée un leurre, peut facilement se faire avec l'autorisation de son propriétaire. Il suffit que ce dernier appose son doigt sur une surface molle comme de la silicone, pour que le dessin de son empreinte apparaisse clairement. En utilisant de la gélatine en fusion afin de combler les creux, celle-ci épouse la forme du doigt, et en refroidissant, constitue un excellent leurre. Une empreinte digitale peut aussi être relevée à l'insu de son propriétaire. Ceci est peu fréquent et peu facile à réaliser, car même les professionnels dans la police scientifique ont des difficultés à les relever.

Certains produits facilitent l'acquisition d'une empreinte digitale directement prélevée sur un support. De plus, le vol d'empreintes digitales n'est pas à exclure des risques potentiels de détournement des données personnelles.
Pour ces raisons, le risque de falsification est sérieusement envisagé par la CNIL, qui classe la capture d'empreintes digitales dans la biométrie dite « à traces ».

La permanence et le caractère immuable de l'empreinte digitale font d'elle une donnée personnelle particulièrement « sensible » ce qui permet de comprendre les réticences de la CNIL à l'idée de la constitution de bases de données biométriques comportant uniquement des empreintes digitales.

[113] Moulage d'empreintes digitales provenant du site internet Biometric System Laboratory : http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=7&pathSubj=111%7C%7C7&Req=&. Tous droits réservés.

Toutefois, pour pallier cet inconvénient, les recherches progressent et par exemple Sagem a déjà mis en œuvre des capteurs d'empreintes avec détection de faux, mais néanmoins, au prix d'une complexité plus élevée.

Une autre société, Siemens, a annoncé en septembre 2005 vouloir aussi mettre sur le marché, une solution de détection des faux doigts nommée « *fingerfakes* ». La compétition entre les attaquants et les contre-mesures est largement engagée dans ce domaine.

81. Les dispositifs de reconnaissance par empreinte digitale suscitent de nombreuses interrogations liées à la protection des données personnelles, tant elles laissent des traces. La fiabilité et la faculté de confection de leurres remettent souvent en question l'usage de cette technique. C'est pourquoi d'autres modalités biométriques sont développées, en parallèle des dispositifs de reconnaissance par empreinte digitale et permettent d'utiliser la biométrie de façon « plus sereine » (E).

E. Les autres modalités biométriques

82. Les différentes recherches anthropométriques de ces deux derniers siècles, ont amené les chercheurs à découvrir que d'autres parties du corps humain peuvent être uniques.

La biométrie est basée sur l'analyse de données liées à l'individu. Ces données peuvent être classées en deux catégories : les analyses biologiques ou morphologiques d'une part et les analyses comportementales d'autre part.

Les analyses biologiques ou morphologiques comprennent les empreintes digitales, le réseau veineux, le contour de la main, la rétine, l'iris, la voix. L'ADN fait partie de cette catégorie mais il ne présente pas encore le caractère d'automatisation que les autres possèdent.

Les analyses fondées sur le comportement sont basées sur la frappe au clavier, la démarche des personnes, la signature manuscrite ou la voix.

Il est nécessaire de préciser que la frontière entre ces deux catégories n'est pas franche : pour la voix, elle a une part biologique, ce qui explique son emplacement dans ces développements au sein des caractéristiques biologiques ou morphologiques.

83. Seules, les techniques biométriques sont prises en compte dans l'analyse morphologique et feront l'objet de développements. L'analyse morphologique, en effet, est l'une des techniques les plus fiables et la plus répandue (1°) dans le cadre de l'entreprise. L'usage de caractéristiques comportementales tend à se développer, mais en l'absence de recul suffisant sur ces techniques, elles ne seront volontairement pas traitées. La biométrie multimodale, quant à elle, sera développée plus succinctement car elle reste encore le sujet principal de nombreuses études même si, ces dernières années, elle a pris de l'ampleur (2°).

1°. La prééminence des caractéristiques biologiques ou morphologiques

84. La biométrie morphologique comporte la technologie qui vise à relever, chez l'individu, des traits uniques issus de ses empreintes digitales, du réseau veineux de sa main, du contour de la main, de la rétine, de l'iris ou de la voix. D'autres modalités sont également étudiées, mais cela reste au niveau de la recherche fondamentale. Cette catégorie de biométrie est la plus employée sur le marché[114].

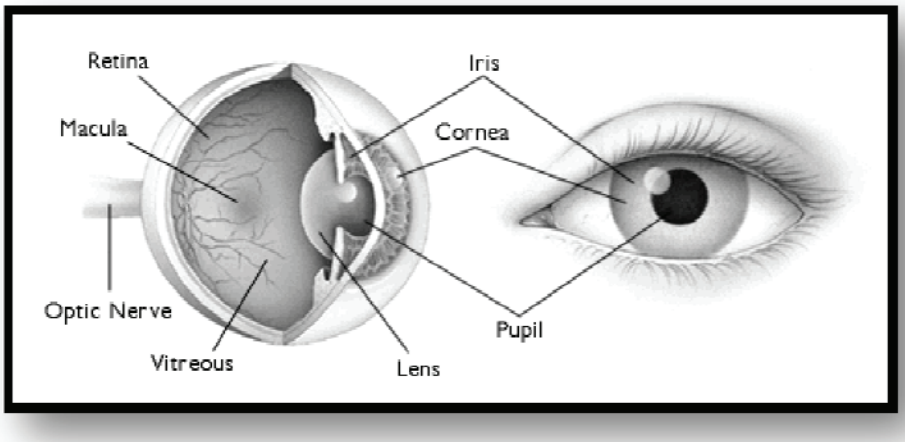
85. Les techniques de la reconnaissance de l'iris (1-1), du visage (1-2), du contour de la main (1-3) ainsi que de la voix (1-4) sont les dispositifs majoritairement choisis et installés dans le cadre des entreprises.

1-1. La reconnaissance de l'iris

86. L'iris est la zone colorée située entre le blanc de l'œil et la pupille. C'est une membrane circulaire et contractile de la face antérieure du globe oculaire. La luminosité

[114] Cf. Annexe 2

influe sur sa contraction ou sa dilatation, qui se produisent indistinctement, à l'aide d'un muscle, le sphincter[115].

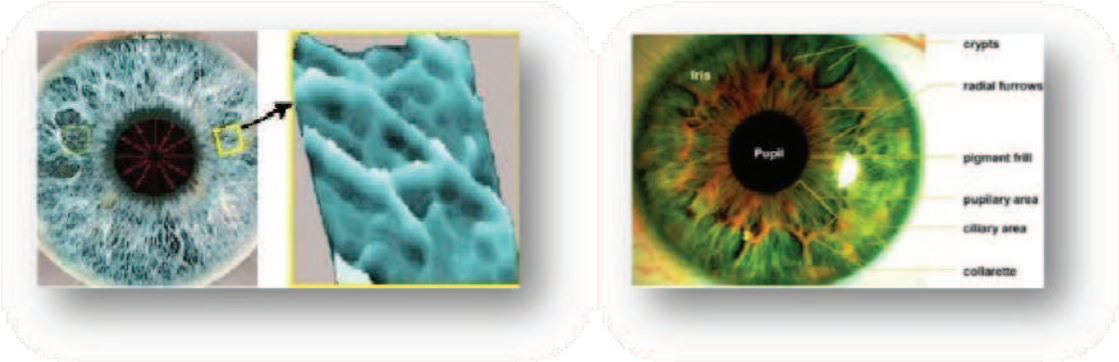


116

La reconnaissance de l'iris a été proposée pour la première fois en 1936 par l'ophtalmologue Franck Burch. Il semble pourtant, que durant de nombreuses années, cette idée n'a été reprise que dans les films de science-fiction, comme par exemple Minority Report.

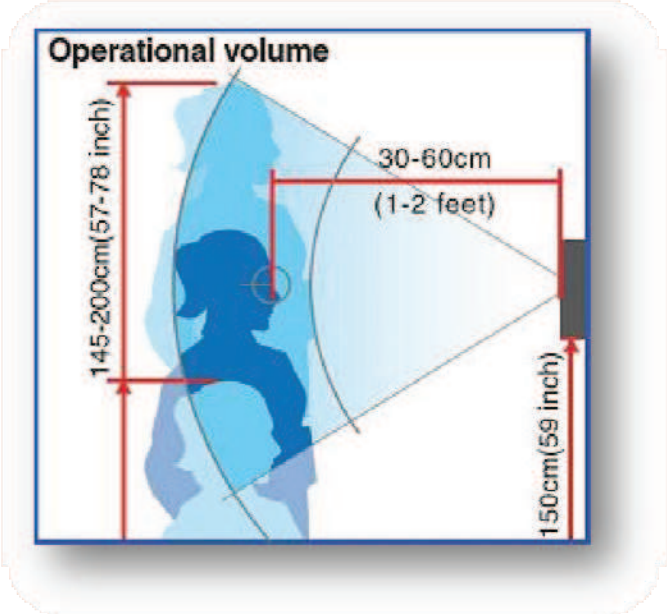
En 1987, deux ophtalmologues, Aran Safir et Léonard Flom ont breveté ce système qui permet d'identifier un individu par l'iris de l'œil, tout en contactant en 1989 John Daugman[117], à cette époque enseignant à l'université d'Harvard, afin que ce dernier recherche et crée un algorithme constituant aujourd'hui la base de l'identification par l'iris.
Selon John Daugman, la probabilité que deux iris humains soient identiques est de 1 sur 10 à la puissance 72, même lorsqu'il s'agit de deux jumeaux. Chacun d'eux va disposer d'assez d'éléments distinctifs pour que l'iris de l'un ne soit pas confondu avec celui de son frère.

[115] Définition du site internet Wikipédia.
[116] Image provenant du site internet www.biometrie-online.net. Tous droits réservés.
[117] Site internet de John Daugman : http://www.cl.cam.ac.uk/~jgd1000/



118

87. Cependant, la capture de l'image de l'iris n'est pas aisée et requiert une caméra infrarouge autofocus, matériel assez coûteux, ce qui explique sans doute le fait que cette technologie ne soit pas fréquemment employée, même si elle dispose d'un fort taux de fiabilité.



119

Les facteurs environnementaux sont une première difficulté. En effet, l'iris est un organe très sensible, sa taille varie selon la luminosité ambiante, il est de petite taille et dissimulé sous les cils. Si l'individu porte des lentilles de contact celles-ci peuvent gêner l'authentification biométrique.

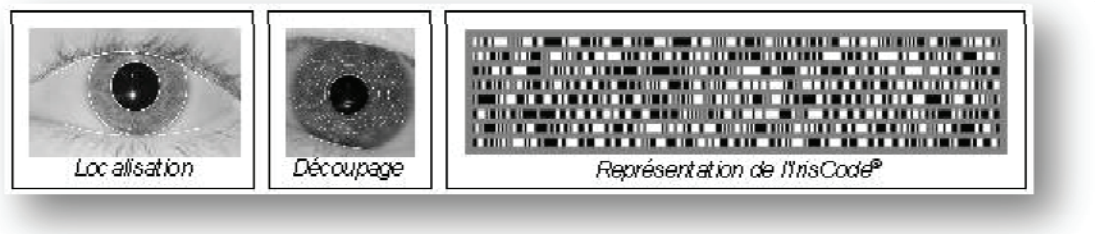
Par ailleurs, la seconde difficulté réside dans la capture de l'image. L'œil doit se trouver à une distance relativement proche de la caméra pour que la capture soit valide. Il ne faut pas que la

[118] Images de la structure de l'iris lors de la capture, site internet de Jean-François Mainguet : http://pagesperso-orange.fr/fingerchip/biometrics/types/iris.htm. Tous droits réservés.
[119] Capteur dédié à l'acquisition d'un iris, site internet http://www.nedapaeos.com/img/products/bio_iris.jpg. Tous droits réservés.

lumière se reflète, la prise d'images doit être précise et rapide, de manière à ce que le système de numérisation permette d'obtenir 70 pixels de rayon sur l'iris. Un matériel spécifique est nécessaire. La capture de l'iris se fait à partir de caméras monochromes dans le proche infrarouge car la couleur de l'iris n'est pas utilisée, mais plutôt son relief. L'iris est capturé à l'aide d'une lumière infrarouge, non invasive pour l'œil.

Cette technique est souvent considérée comme étant absolue, les résultats sont bons mais peuvent varier selon différents facteurs tels que des lentilles de contact, une morphologie tombante du cil qui dissimule l'iris ou la déformation de celui-ci.

L'image correspond généralement à l'intégralité de l'œil dans lequel l'iris est détecté automatiquement. Plusieurs méthodes peuvent être employées pour sa caractérisation, mais c'est la méthode brevetée par John Daugman qui est souvent préférée. Après avoir effectué la numérisation de l'image de l'œil, les contours, cils et paupières vont être détectés afin de les éliminer de l'image de l'iris.



120

88. Une fois l'image de l'iris acquise et les éléments secondaires éliminés, le capteur détermine le centre de la pupille et procède au découpage de l'iris. Un logiciel se charge alors de découper des bandes régulières, afin d'en établir un gabarit, c'est l'Iriscode créé par John Daugman.

Cette technologie a le privilège d'assurer un haut niveau de reconnaissance, l'iris de l'être humain étant stable tout au long de sa vie. Par ailleurs, il est difficilement falsifiable, ce qui garantit un haut seuil de sécurité pour les données personnelles de l'individu. Toutefois, ces

[120] Image du site internet biométrie online : http://www.biometrie-online.net/techno/iris/T-iri.php. Tous droits réservés.

applications ne sont pas fréquentes. Seules, certaines agences bancaires anglaises et américaines, ainsi que l'armée, ont recours à ce type de reconnaissance.

En France, ce système doit faire l'objet d'une autorisation préalable de la CNIL, même si cette technologie a l'avantage d'être une biométrie « sans traces », au sens de la loi Informatique et libertés. Le dispositif de reconnaissance de l'iris n'a pas été retenu, en France, comme élément pouvant être contenu dans les papiers d'identité[121]. L'argument avancé déclarait qu'il s'agissait « *d'une technologie brevetée appartenant à une seule et même entreprise américaine. Comme il s'agit d'une technique relativement récente (développée depuis 1992), elle n'est pas encore assez mature pour permettre une mise en œuvre dans des bases de données à grande échelle*[122] ». Le ministre de l'Intérieur français reconnaissait lui-même la préférence de l'Etat pour les empreintes digitales, à la différence de l'Allemagne qui préfère utiliser la reconnaissance de l'iris. Seules les empreintes digitales ont été retenues pour être insérées dans les titres et documents d'identité des citoyens européens.

L'argument d'opportunité tendrait à constater que les systèmes de reconnaissance de l'iris sont perçus comme étant bien plus intrusifs que les systèmes de reconnaissance des empreintes digitales et il est tout à fait envisageable qu'en choisissant cette méthode, l'Etat français se serait confronté à de vives oppositions, tant des partis politiques que de la population. Pour que de tels dispositifs soient mis en œuvre, il est nécessaire d'obtenir un consensus entre l'Etat et ses citoyens. Une technique biométrique efficace est aussi une technique acceptée.

89. Les systèmes de reconnaissance faciale, initialement utilisés dans les aéroports et les villes, commencent à se développer en entreprise à des fins sécuritaires, même si cette technique ne reçoit pas encore un franc succès (1-2).

---

[121] Cette décision tient aussi du fait que Sagem, entreprise française est spécialisée dans les dispositifs biométriques (empreintes digitales)

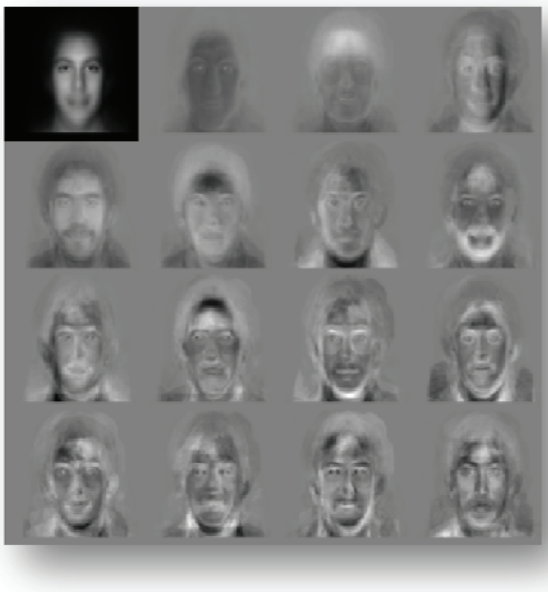
[122] Proposition de règlement du Conseil modifiant le règlement (CE) n°1683/95 établissant un modèle type de visa. Proposition de règlement du Conseil modifiant le règlement (CE) n°1030/2002 établissant un modèle uniforme de titre de séjour pour les ressortissants de pays tiers, E2403 - COM (2003) 558 final du 24/09/2003, texte adopté par les instances européennes le 18/04/2008.
Site internet du Sénat français : http://www.senat.fr/ue/pac/E2403.html

1-2. La reconnaissance faciale

90. Identifier un individu, c'est avant tout le reconnaître par les traits de son visage. C'est une action que le cerveau humain fait quotidiennement.
La reconnaissance faciale devrait être, à ce titre, le mode de reconnaissance biométrique le plus fréquemment utilisé, mais elle n'emporte que 11,4% du marché, selon les statistiques de l'International Biometric Group[123].

Dans les années 1970, cette technique était seulement basée sur les éléments mesurables du visage, tels que les lèvres, le menton, les sourcils et l'écartement des yeux et a toujours souffert d'un faible taux de reconnaissance par rapport aux autres modalités.

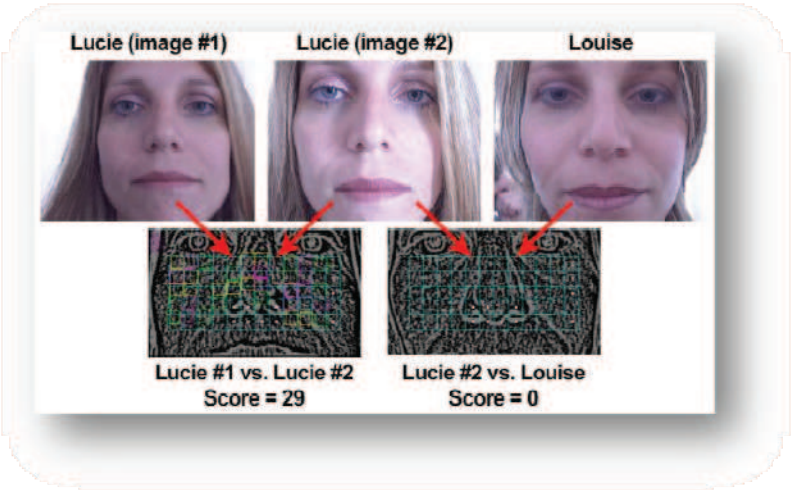
En matière policière, la multiplication des identifications a fait croître la nécessité de se munir d'une technologie qui permet, à l'aide de simples caméras, d'identifier un individu recherché au milieu d'une foule. Ce mécanisme consiste à prendre la photographie d'une personne, pour en extraire un maximum de facteurs distinctifs dans le but de l'identifier. Ces derniers sont choisis en fonction de leur faible degré de variabilité. Cette technologie ne s'adresse donc pas, en premier lieu, au grand public.



124

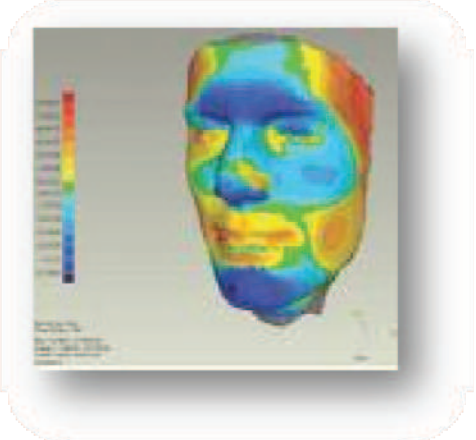
[123] International Biometric Group, Biometric Revenues by technology, 2009, http://www.biometricgroup.com/reports/public/market_report.php

Plusieurs variantes de technologies du visage ont été développées. La première est celle supportée par le MIT (Massachusetts Institute of Technology) « *Eigenface* ». Elle consiste à décomposer le visage en plusieurs nuances de gris, permettant ainsi de faire ressortir sur chaque image des caractéristiques différentes.



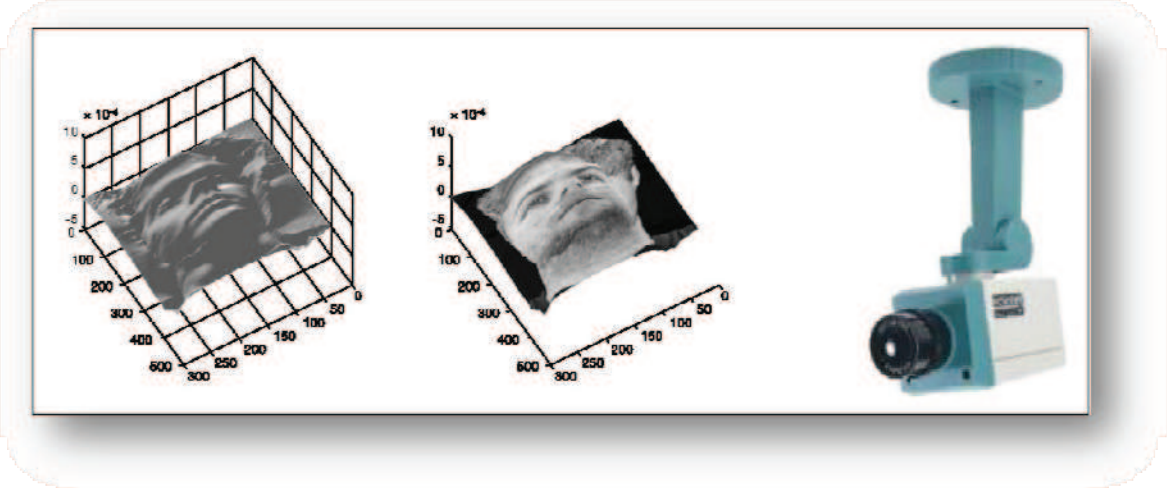
125

91. D'autres techniques sont utilisées comme, par exemple, la reconnaissance de la structure de la peau ou l'utilisation d'un thermographe qui permet de détecter la répartition de la température du visage.



126

[124] Image de capture servant à la reconnaissance faciale, site internet biometrie-online.net. Tous droits réservés.
[125] Image de démonstration provenant du MIT. Site Internet : http://vismod.media.mit.edu/vismod/demos/facerec/. Tous droits réservés.
[126] Utilisation d'un thermographe : site internet biométrie-online. Tous droits réservés.



127

92. La reconnaissance faciale reste encore marginale au sein des entreprises multinationales. Elle est trop souvent assimilée aux techniques sécuritaires et, de ce fait, elle est généralement très mal acceptée par les utilisateurs, à la différence des dispositifs de reconnaissance du contour de la main qui se sont démocratisés dans le quotidien des individus depuis une dizaine d'années déjà (1-3).

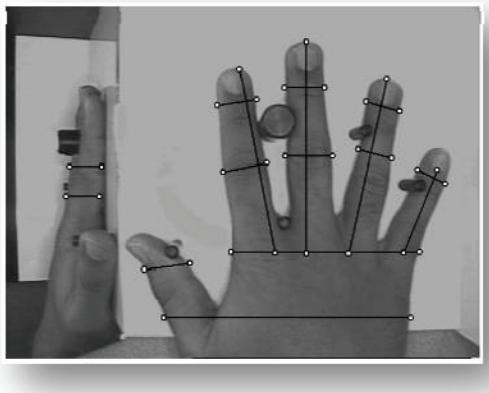
1-3. La reconnaissance du contour de la main

93. Cette technologie se nomme aussi géométrie de la main, car c'est la silhouette de la main qui est utilisée. Cette technique ne doit pas être confondue avec l'empreinte palmaire en ce qu'elle ne relève pas la paume de la main mais simplement son contour.
Ce système a été le plus couramment utilisé ces dix dernières années, depuis sa création pour le marché du contrôle d'accès physique et la gestion des horaires.

94. L'acquisition de l'image se crée par une photographie de la main, effectuée à l'aide d'une caméra infrarouge qui va étudier les principales caractéristiques divergentes, selon les individus (longueur, largeur, épaisseur des doigts, de la paume). Les emplacements des doigts sont matérialisés sur la photo ci-dessous. La photographie, présentée sous deux

[127] Images représentant les autres techniques de reconnaissance faciale, la première à gauche représente la technique de reconnaissance thermique, site internet http://umfacts.um.edu.my/gallery/index.php?page=7. Tous droits réservés. La seconde représente la reconnaissance faciale à l'aide du grain de peau, cette image provient du site internet biometrie-online.net

angles différents, grâce à un miroir sur le côté, permet d'obtenir une image de la main en trois dimensions.



128



129

Ce système est simple à mettre en œuvre et il est mieux accepté par la population. La CNIL a une préférence pour cette technologie dite « sans traces » à l'inverse de l'empreinte digitale. Son développement dans les entreprises est croissant depuis ces dix dernières années mais la faiblesse de ses performances en reconnaissance réduit ses possibilités d'utilisation à l'authentification uniquement. La personne doit décliner son identité avant la vérification.

95. Une autre technologie doit être évoquée car elle tend à prendre de l'ampleur, il s'agit du réseau veineux des doigts de la main ou de la main complète, paume ou dos.
Ce réseau veineux est différent d'un individu à un autre. La capture se fait à l'aide d'un capteur infrarouge ou d'une caméra CMOS. Cette technologie est dite « sans traces » ou « cachée » puisqu'il est quasiment impossible, au regard des moyens actuels, de reproduire l'image du réseau veineux à l'insu de son propriétaire. La CNIL a même permis la constitution d'une base de données biométriques fondée sur le réseau veineux de la main, pour les mêmes raisons de traçabilité.

96. D'autres technologies sont développées dans les différents marchés cités, comme la reconnaissance vocale, la reconnaissance de la rétine, ou l'empreinte palmaire (1-4).

---

[128] Image d'un capteur pour géométrie de la main, site internet : http://researchweb.watson.ibm.com/ecvg/biom/handgeometry.html. Tous droits réservés.

[129] Image de la capture de la géométrie de la main en trois dimensions grâce au miroir intégré sur les côtés. Site internet de Jean-François Mainguet : http://pagesperso-orange.fr/fingerchip/biometrics/types/hand.htm. Tous droits réservés.

1-4. La reconnaissance vocale

97. Tout comme le visage, la voix est un élément de reconnaissance des plus naturels, utilisé en permanence par les êtres humains. La voix donne des informations sur la personne que l'on entend, le débit de parole, l'accentuation de certains mots ou le timbre. Tous ces éléments permettent de différencier deux individus.

Les industriels se sont basés sur ce constat, pour créer des dispositifs biométriques de reconnaissance vocale, dispositifs qui sont à distinguer des programmes du même nom, ne visant pas à identifier vocalement un individu, mais à déterminer et retranscrire le contenu des mots entendus, des mots prononcés. Dans le premier cas, celui qui nous intéresse, la voix, et seulement la voix, est prise en compte par la biométrie, et non la parole traduisant la pensée de la personne.

Dans les cas d'authentification automatique du locuteur (AAL), il s'agit de reconnaître l'identité d'une personne en lui faisant prononcer plusieurs phrases. Les différentes applications existantes en la matière (applications sur site, judiciaires ou dans les télécommunications) font naître différentes difficultés inhérentes à l'environnement dans lequel elles évoluent.

Dans une application sur site, l'environnement est plus facilement contrôlé pendant la prononciation d'une phrase qu'en utilisant un serveur téléphonique.
Une fois la capture accomplie, il est nécessaire d'effectuer un traitement numérique de la voix. Le signal acoustique vocal est analysé afin d'en extraire les paramètres essentiels. Ces paramètres conduisent à la création d'un modèle reporté ensuite dans un classifieur qui permettra de déterminer l'identité du locuteur.

Cette technologie tend à faire son entrée dans les entreprises, depuis l'autorisation donnée par la CNIL à la société des pneumatiques Michelin, d'employer un système de reconnaissance vocale ayant pour finalité la réinitialisation des mots de passe[130].

[130] CNIL, Délibération n° 2007-248 du 13 sept. 2007 autorisant la mise en œuvre par la Manufacture française des pneumatiques Michelin d'un traitement automatisé de données à caractère personnel reposant sur un procédé de reconnaissance vocale et ayant pour finalité la gestion des mots de passe, disponible sur le site www.cnil.fr

Cependant, selon l'application choisie, les exigences qualitatives de la capture ne seront pas les mêmes. Plus clairement, la qualité de la voix du locuteur peut être altérée (maladie, état émotionnel ou qualité du microphone) et l'environnement de capture peut être bruyant. Tous ces facteurs jouent sur la qualité de la capture et a fortiori sur le résultat. De fait, en pratique, les performances de reconnaissance vocale sont assez faibles.

98. L'efficacité de ces techniques ne réside pas seulement dans leur technicité mais tient compte de la normalisation. Cette normalisation joue un rôle fondamental en permettant d'établir une compatibilité des outils biométriques et des interfaces. C'est dans ce but qu'a été créé le Comité international de normalisation ISO SC37 qui émet tous les standards biométriques.

99. Un autre type de biométrie intéresse tout particulièrement les industriels et les groupes de recherche tel le GET (Groupe des Ecoles des Télécommunications), il s'agit de la biométrie multimodale. Elle vise à diminuer les taux d'erreurs en associant plusieurs modalités biométriques (2°).

2°. La biométrie multimodale

100. Aucune modalité biométrique ne peut avoir et n'aura jamais, une exactitude de 100% de reconnaissance. L'idée d'utiliser simultanément plusieurs modalités est vite apparue comme un moyen d'améliorer les performances des dispositifs. L'authentification sera positive si, par exemple, l'empreinte et l'iris sont reconnus simultanément. La multimodalité est donc la fusion entre différents systèmes anthropométriques, qui permet ainsi d'assurer de meilleures statistiques de reconnaissance, sans la difficulté d'une mise en œuvre.

En France, un projet collaboratif, « *Biomet* », initié en 2001 et financé par le Groupe des Ecoles des Télécommunications (GET) a fait de nombreuses recherches dans ce domaine.
Pour parvenir à une identification avec un excellent taux de réussite, on utilise la multimodalité qui consiste à sélectionner les meilleures combinaisons entre les paramètres des différents outils biométriques, plutôt que de choisir une seule de ces techniques.

Ce projet est clos depuis 2003. Il a permis de constituer une base de données expérimentale stockant cinq modalités sur 130 volontaires. Les cinq modalités sont les suivantes : la voix, les empreintes digitales, la reconnaissance faciale, l'iris et la signature électronique. Ce système a l'inconvénient d'être bien plus coûteux que les systèmes biométriques usuels car il nécessite de disposer de plusieurs capteurs pour effectuer différentes mesures.

L'objectif était de fiabiliser les résultats afin de rendre les systèmes de vérification plus adaptés. Comme argument, les développeurs des systèmes employant la multimodalité, assurent qu'elle est mieux acceptée par la population. Selon Jean-François Mainguet, cette affirmation est contestable dans la mesure où l'usage de la multimodalité est nettement moins pratique pour les individus.

Le risque majeur de la biométrie multimodale est la constitution de bases de données. Ce risque est déjà évoqué, en ce qui concerne les techniques biométriques « traditionnelles » mais il devient croissant lorsqu'il s'agit de cumuler certains types de données afin d'obtenir un meilleur résultat statistique.

101. La biométrie est souvent présentée comme une somme de techniques sécuritaires. Or, elle s'est développée pour différents usages autres que la sécurité (section 2).

Section 2. Les différents usages de la biométrie

102. Deux usages principaux de la biométrie peuvent être mis en exergue, d'une part la sûreté publique où l'individu est soumis à la biométrie par les autorités administratives ou gouvernementales (A) et d'autre part la biométrie de confort, correspondant au choix délibéré d'un individu d'avoir recours à ce type de technique comme mode de sécurisation de ses biens ou d'accès aux services (B).

A. Les usages de sûreté publique ou la « biométrisation[131] » de l'identité

103. La sûreté publique est l'enjeu de départ qui justifie l'usage de la biométrie. Chaque pays souhaite sécuriser les papiers d'identité de ses ressortissants (1°), contrôler les flux migratoires aux frontières (2°), empêcher les fraudes aux élections (3°) et, depuis les attentats terroristes de 2001 aux Etats-Unis, s'assurer de la sécurité au sein des aéroports (4°).

1°. La sécurisation des papiers d'identité

104. La fraude des titres d'identité touche actuellement tous les pays développés. Elle a pris des proportions inquiétantes qui nécessitent de recourir à certaines mesures tendant à l'éradiquer. Au-delà du coût financier que ces fraudes engendrent, la sécurité intérieure des pays est affectée. Ces fraudes permettent aux faussaires de commettre des actes délictueux à travers le monde tout en voyageant librement.

Un constat est à prendre en considération[132]. Entre 1999 et 2004, le ministère de l'Intérieur français a recensé le vol de 84 464 titres d'identité vierges (passeports, permis de conduire, cartes grises, visas). Le pourcentage de vol a augmenté de 67,7% de 2001 à 2003.

---

[131] Néologisme employé pour exprimer le tout biométrique de l'identité de l'individu. Cette expression est aussi employée dans l'ouvrage « *Du papier à la biométrie, identifier les individus* » sous la direction de X. Crettiez et P. Piazza, 2006 éd. Science Po les Presses.

[132] J-R, LECERF, Rapport d'information fait au nom de la Commission des lois et de la mission d'information de la Commission des lois, sur « la nouvelle génération de documents d'identité et la fraude documentaire », n° 439 (2004-2005), 29 juin 2005.

En 2002, 2835 fausses cartes nationales d'identité ont été interceptées par la police aux frontières. Les passeports ont aussi été touchés, 90 000 documents ont été perdus ou volés entre 1999 et 2004.

Les autres pays européens comme l'Espagne, le Royaume-Uni ou l'Allemagne sont, eux aussi, fortement touchés par la fraude documentaire. Aux Etats-Unis, le passeport et la carte verte (destinée aux étrangers), sont des documents exclusivement délivrés au niveau fédéral, les fraudes de ces documents sont d'autant plus préjudiciables qu'il n'existe aucun document « national ». Lorsqu'il existe des documents nationaux comme la carte nationale d'identité, d'autres difficultés apparaissent, soit au niveau des justificatifs d'identité, qui varient selon la situation personnelle du demandeur, soit au niveau des conditions de délivrance.

C'est pourquoi, *a priori*, la biométrie est considérée comme la meilleure technique, permettant à la fois d'identifier rapidement des milliers de personnes et dans une certaine mesure, de dissuader les faussaires. Elle permet aussi d'éviter les problèmes d'identités multiples, puisque l'empreinte digitale est unique et stockée dans une base de données centralisée avec comparaison systématique de cette base à chaque demande. Par ailleurs, lors de chaque présentation du titre d'identité, le porteur est authentifié en fonction des données biométriques enregistrées dans la base de données, la vérification de son identité est ainsi plus fiable.

En revanche, la biométrie ne peut vérifier l'émission du document d'identité par l'administration compétente. Les données biométriques peuvent appartenir au porteur de la carte ou du passeport, alors que ce dernier a usurpé l'identité de quelqu'un d'autre. Par conséquent, il n'est donc pas garanti, malgré les données biométriques, que l'identité d'un individu soit prouvée. Il serait donc nécessaire d'implanter dans le passeport, une donnée spécifique, une sorte de certificat électronique authentifiant le logo de l'administration responsable de la délivrance du document d'identité.
La biométrie ne résout ni ne remplace, en aucun cas, les problèmes usuels liés à la cryptographie. Seule la partie relative à l'identification est améliorée.

105. L'idée du passeport biométrique a émergé après les attentats du 11 septembre 2001 aux Etats-Unis, qui ont démontré, malgré la puissance de ce pays, sa faiblesse face aux

attaques terroristes. Le gouvernement américain a pris des mesures pour contrôler les flux migratoires aux frontières. Le Congrès américain a adopté le « Patriot Act[133] » le 26 octobre 2001. Cette loi d'exception, au départ promulguée pour quatre années, visait à renforcer la sécurité intérieure et la législation pénale contre le terrorisme. Le 14 mai 2002 a suivi le « Enhanced Boarder Security and Visa Entry Reform Act[134] » qui veille à renforcer les procédures d'obtention des visas.

Le « Visa Waiver Program » américain, issu du « Patriot Act », énonce qu'à partir du 26 octobre 2006, les détenteurs de passeports biométriques seront exemptés de visa pour une durée inférieure à trois mois sur le territoire. Cette initiative a entraîné de nombreux pays à adopter le passeport biométrique, puisqu'à l'heure actuelle, une quarantaine d'Etats, essentiellement européens, font partie de cette liste. Afin de mener ce projet à bien, dès 2003, le G8 s'est réuni afin de mandater des experts (français et américains pour la plupart).

Il ne s'agit que d'un premier pas, car les Etats-Unis n'exigent pas que les empreintes digitales ou autres traits biométriques soient présents dans le passeport. Seule, la puce RFID située à l'intérieur de celui-ci est exigée.

Par ailleurs, l'Organisation internationale de l'aviation civile (OACI) soucieuse des problèmes d'interactions des différents systèmes de lecture, a établi des normes de compatibilité. Le 9 mai 2003, elle a établi une recommandation qui prévoit l'insertion d'au moins une donnée biométrique dans les documents de voyage d'ici 2015.

Au sein de l'Union européenne, le règlement CE n° 2252/2004 du Conseil du 13 décembre 2004[135] a établi des normes de mise en place sur les éléments de sécurité et les éléments biométriques qui doivent être intégrés dans les passeports et les documents de voyage délivrés par les Etats membres.

---

[133] Public Law 107-56 «Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism » (Unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme)

[134] Public Law 107-173

[135] Règlement CE du Conseil, n° 2252/2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, JOCE L 385 du 29 déc. 2004 p. 1-6

A partir du 28 août 2006, ces derniers devront délivrer des passeports biométriques. Les données biométriques sont stockées dans une puce comprenant la photographie faciale ainsi que les empreintes digitales.

La CNIL s'est prononcée au sujet du passeport biométrique le 11 décembre 2007, dans une délibération n° 2007-365[136]. Elle a émis un certain nombre de réserves concernant la création de cette première base de données biométriques à visée administrative. Parallèlement, ce décret vient modifier le fichier de gestion des passeports DELPHINE, puisqu'il prévoit la conservation de certaines données du demandeur, telles que la photographie du visage et les empreintes digitales des huit doigts. Par le décret n°2007-240 du 22 février 2007[137], la France a créé un organisme nommé Agence nationale des titres sécurisés (ANTS). C'est un établissement public national, à caractère administratif, placé sous la tutelle du ministre de l'Intérieur. Selon l'article 2 de ce décret, l'Agence a pour mission « *de répondre aux besoins des administrations de l'Etat en matière de titres sécurisés. Ces titres sont des documents délivrés par l'Etat et faisant l'objet d'une procédure d'édition et de contrôle sécurisée.* »
Cette agence n'enlève pas le monopole à l'imprimerie nationale mais elle est chargée de la conception et de l'achat du matériel nécessaire.

106. Parallèlement, en France, s'est développé le projet d'une carte nationale d'identité électronique appelée INES (Identité Nationale Electronique Sécurisée). Cette carte a été explicitement exclue du règlement CE de 2004[138] mais reste au choix du gouvernement. Toutefois, dans la mouvance sécuritaire, le projet reste d'actualité. Cette carte serait payante mais ne serait pas obligatoire. Le premier objectif est d'authentifier les citoyens, le second consiste à la recherche d'identités multiples.

La carte comprend une puce électronique à lecture sans contact lisible à un centimètre, incluant, en plus des données d'identité, des données biométriques. La carte ne peut être lue qu'à l'aide d'un lecteur approprié et avec le consentement du citoyen. Concernant la

[136] CNIL, Délibération n° 2007-365 du 29 nov. 2007 autorisant la mise en œuvre par LG Electronics Mobilecomm France d'un transfert de données à caractère personnel hors de l'Union européenne, autorisation n° 1190581, disponible sur le site www.legifrance.gouv.fr
[137] Décret n° 2007-240 du 22 fév. 2007 portant création de l'Agence nationale des titres sécurisés, JO n°47 du 24 fév. 2007
[138] L'art. 1 al. 3 du règlement CE 2252/2004 précité énonce que « *Le présent règlement s'applique aux passeports et aux documents de voyage délivrés par les États membres. Il ne s'applique pas aux cartes d'identité délivrées par les États membres à leurs ressortissants.* »

recherche d'identités multiples, cette dernière nécessite la constitution d'une base de données d'empreintes digitales. Les empreintes seraient stockées dans cette base sans y associer le nom du propriétaire afin de déterminer si l'empreinte est déjà fichée. Elle doit, a priori, compléter le fichier de données alphanumériques des détenteurs de carte d'identité.

107. La biométrie permet aussi de contrôler les flux migratoires. Du passeport aux visas biométriques, les pays développés veulent gérer le déplacement des populations (2°).

2°. La sécurisation biométrique des flux migratoires

108. La mondialisation des échanges a entraîné une plus grande mobilité des personnes, de ce fait, les gouvernements des pays développés ont de plus en plus de difficultés à gérer les flux migratoires et sont confrontés à la question de l'immigration clandestine.
En France, la plupart des clandestins sont entrés légalement sur le territoire, à l'aide d'un visa. Cependant, la durée de leur visa a été largement dépassée. L'OFPRA (Office français de protection des réfugiés apatrides) a relevé qu'entre 1999 et 2005, plus de 260 000 individus se sont vu refuser la prolongation de leur visa et sont restés illégalement sur le territoire, faute de reconduite à la frontière.

Dans le cadre de l'Union européenne, depuis la mise en place de l'espace Schengen, les citoyens européens bénéficient d'une liberté de circulation sur le territoire de l'Union qui assure la réalisation du marché unique. Toutefois, pour assurer la pérennité de cette liberté, il est nécessaire de contrôler efficacement les flux migratoires. C'est là qu'intervient le visa biométrique.

Il ne faut pas confondre passeport et visa. Le passeport permet à un ressortissant de voyager dans un pays tiers, alors que le visa a pour objet de contrôler l'entrée d'un étranger sur un territoire. Contrairement au visa traditionnel, le visa biométrique permet d'assurer un contrôle plus fiable de l'identité et de gérer informatiquement la durée du séjour sur le territoire. Ce visa est issu de deux initiatives.

La première est française avec la loi n°2003-1119 du 26 novembre 2003 relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité. Cette loi prévoit dans son article 8-4 la prise de la photographie du visage et des empreintes digitales pour les demandeurs de visa[139]. La CNIL a émis quelques réserves concernant la constitution d'une base de données centralisée d'empreintes digitales même si celle-ci n'est pas mentionnée dans le décret. Conforme à sa doctrine en la matière, elle a rappelé que ce fichier pouvait être admis à titre expérimental mais ne pouvait en aucun cas être pérennisé sans en être précisément informée.

La seconde initiative provient de l'Union européenne, par une décision du Conseil du 8 juin 2004 visant à déployer le « système d'information sur les visas » plus couramment appelé « *Visa Information System* » (VIS) [140]. Ce système vise à améliorer la mise en œuvre de la politique commune en matière de visa. Cette infrastructure comprend un système d'information central (CS-VIS) ainsi qu'une interface dans chaque Etat membre (NI-VIS). Ce système assure une connexion permanente entre le système central et le système national.
Le règlement n°1987-2006 du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen de deuxième génération (SIS II), a pour objet d'assurer un niveau de sécurité élevé et fait suite à la décision de 2003. Le règlement établit le fonctionnement du système, la procédure de signalement des ressortissants du pays tiers aux fins de non-admission et il prévoit en outre, les droits d'accès et de protection des données personnelles.

109. Une autre initiative française par le décret n°2004-1266 du 25 novembre 2004 a mené à la création du projet BIODEV (*Biometric Data Experimented in Visas*). Ce projet a d'abord été une expérimentation conduite de janvier 2005 à mars 2006 autorisée par décret du Conseil d'Etat le 26 novembre 2004 après avis de la CNIL.

---

[139] Art. 8-4 « *Afin de mieux garantir le droit au séjour des personnes en situation régulière et de lutter contre l'entrée et le séjour irréguliers des étrangers en France, les empreintes digitales ainsi qu'une photographie des ressortissants étrangers qui sollicitent la délivrance, auprès d'un consulat ou à la frontière extérieure des Etats parties à la convention signée à Schengen le 19 juin 1990, d'un visa afin de séjourner en France ou sur le territoire d'un autre Etat partie à ladite convention peuvent être relevées, mémorisées et faire l'objet d'un traitement automatisé dans les conditions fixées par la loi n° 78-17 du 6 janvier 1978 précitée. Ces empreintes et cette photographie sont obligatoirement relevées en cas de délivrance d'un visa.* » Loi n° 2003-1119 du 26 nov. 2003 relative à la maîtrise de l'immigration, au séjour des étrangers en France et à la nationalité

[140] Décision du Conseil 2004/512/CE du 8 juin 2004 visant à déployer le système d'information sur les visa, JOCE L 231 du 15 juin 2004

Il tendait à expérimenter, au niveau européen, le traitement et la gestion des visas. La France, leader de ce projet, a été rejointe par la Belgique, l'Allemagne, la Hongrie, l'Italie, les Pays-Bas et la Pologne. Le visa contenait une puce sans contact, qui intègre les recommandations de l'OACI en assurant ainsi une meilleure interopérabilité entre les systèmes.

Cette expérimentation a montré certaines difficultés concernant le recours à la technique biométrique. Tout d'abord, des contraintes géographiques ont été soulevées, le demandeur devait se déplacer à son consulat pour y déposer ses empreintes. Par ailleurs, les consulats devaient être équipés des capteurs nécessaires à l'enrôlement, pour recevoir l'intégrité des demandeurs. Le coût de cette expérimentation s'est élevé, pour cinq consulats, à 145 millions d'euros dont 105 exclusivement destinés aux investissements immobiliers.

Toutefois, le 14 mars 2006, à l'issue du 6ème conseil franco-allemand de Berlin, il a été décidé de lancer BIODEV II. Cette fois, ce programme vise à vérifier l'identité aux frontières de l'Union européenne et d'arrêter les personnes en situation irrégulière. L'Allemagne et la France ont considéré que « *la garantie de la sécurité intérieure des deux pays impose une architecture de sécurité, comportant non seulement l'usage des technologies de l'information modernes mais encore le recours renforcé aux procédures biométriques pour les visas et des titres de séjour*[141] ».

L'usage de la biométrie dans ce domaine, permettrait de contrôler l'identité des porteurs de visas, d'éviter les demandes de visa multiples, de déceler les identités multiples ainsi que d'identifier sur le territoire, les personnes en situation irrégulière. Elle faciliterait ainsi les demandes des porteurs de bonne foi, au sein de l'espace Schengen.

110. Ces deux projets sont complémentaires : dans les consulats, BIODEV se centre sur les interfaces d'enrôlement et les différents impacts des terminaux, tandis que le programme VIS est axé sur la centralisation des données, et l'interopérabilité entre le système central et le système national.

[141] Site Internet de la coopération Franco-allemande : http://www.france-allemagne.fr/Cooperation-franco-allemande-en,238.html

111. La biométrie est employée, plus récemment, pour sécuriser les élections afin de lutter contre la fraude électorale (3°).

3°. Sécurisation des élections

112. Pour un pays démocratique, les élections sont, pour les gouvernants, le moyen légitime d'exercer leur fonction. L'organisation des élections obéit à des normes internes déterminées par chaque Etat, mais elle doit aussi se conformer à un standard défini par la communauté internationale. Le vote manuel traditionnel est souvent source de contestations et avec l'avènement des nouvelles technologies, il tend à être délaissé au profit d'autres techniques telles que le vote électronique par internet ou la biométrie. Néanmoins, cette évolution ne doit pas se faire au détriment de la sécurité et de la confidentialité des informations nominatives jusqu'à présent protégées.

Sur ce sujet, la CNIL a adopté une recommandation n° 03-036 le 1er juillet 2003, relative à la sécurité des systèmes de vote électronique, sur place ou à distance, dans laquelle elle définit les conditions techniques qui garantissent la protection des données personnelles[142].
La CNIL recommande « *des mesures rigoureuses comme la séparation des données nominatives de l'électeur et du fichier des votes (l'urne électronique) sur des systèmes informatiques distincts ainsi que le chiffrement du bulletin de vote dématérialisé dès son émission sur le terminal* ».

Par ailleurs, les personnels chargés de la gestion ou de la maintenance des systèmes ne doivent pas avoir accès à ces données nominatives. Elle préconise, en outre, de respecter la transparence « *par le recours systématique à l'expertise indépendante des systèmes de vote électronique, l'accès au code source des logiciels et l'utilisation d'algorithmes de chiffrement publics. Par ailleurs, le système de vote doit pouvoir fournir la traçabilité complète de son fonctionnement interne lors d'un scrutin afin de garantir une base solide aux audits externes, notamment en cas de contentieux électoral.* »

[142] CNIL, Délibération n° 03-036 du 1er juil. 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, disponible sur le site de la CNIL au http://www.cnil.fr/index.php?id=1356

113. La CNIL donne des pistes de réflexion et instaure un cadre général. Elle est ouverte au vote électronique, toutefois, il est regrettable qu'à l'heure actuelle, aucune disposition législative ne soit prise en la matière.
Elle a établi un dossier approfondi le 28 mai 2006 sur « le vote par internet aux élections politiques, les éléments du débat[143] » dans lequel ressortent des résultats mitigés sur l'efficacité du vote électronique. Ainsi, certains pays poursuivent l'expérience (Suisse, Estonie, Corée du Sud) alors que d'autres préfèrent y mettre un terme, eu égard aux résultats peu concluants (Grande-Bretagne, Etats-Unis, Espagne). Ce désengagement est essentiellement lié au manque de maturité des différentes technologies qui ne sont, à l'heure actuelle, pas assez performantes pour garantir la protection des droits fondamentaux.

La biométrie peut aussi intervenir dans ce domaine afin d'authentifier l'identité des porteurs et de s'assurer de l'unicité de leur vote. La CNIL rappelle, dans cette même recommandation, que la biométrie reste acceptable dans la mesure où elle ne laisse pas de traces.
Pour les pays en voie de développement qui ne disposent pas de registres électoraux fiables, la biométrie constituerait un moyen de légitimer des élections, bien trop souvent remises en question dans le manque de fiabilité de leurs résultats.

Pour illustrer le propos, pour les élections de 2004, le Venezuela voulait avoir recours à la biométrie afin d'assurer la fiabilité de ses élections. Les instances dirigeantes avaient confié à la société américaine Cogent, la charge d'établir une base de données centralisée d'empreintes digitales, qui permettrait ainsi de stocker les empreintes des citoyens obligés de voter avant les élections. Ensuite, le jour des élections, il suffisait alors de procéder à la vérification de l'identité et d'assurer l'unicité du vote. La base de données était nominative et devait être effacée à l'issue du vote. Cependant, le jour des élections, de nombreuses difficultés techniques sont apparues. Tout d'abord d'ordre matériel, car tous les bureaux de vote n'étaient pas équipés. Des perturbations radio et satellitaires ont empêché certaines personnes de voter. Ensuite, des difficultés d'ordre technique sont apparues : le taux de faux rejets. Certaines personnes se sont trouvées dans l'impossibilité de voter car elles n'étaient pas reconnues par le système.

[143] CNIL, Le vote par internet aux élections politiques, les éléments du débat, dossier disponible sur le site de la CNIL au www.cnil.fr

D'autres pays comme le Cap-Vert, le Sénégal ou le Gabon cherchent à développer la biométrie dans le but d'éradiquer toute fraude électorale.

114. Depuis les attentats terroristes du 11 septembre 2001 à New-York, les Etats ont pris conscience des défaillances dans leur système de sécurité aéroportuaire. Pour sécuriser les accès aux zones sensibles, les normes et le matériel employé étaient différents d'un pays à l'autre. Ainsi, un individu pouvait voyager hors de sa patrie et se voir imposer des règles de sécurité plus strictes que celles de son pays d'origine. La technologie biométrique est la solution choisie pour assurer la sûreté aéroportuaire (4°).

4°. Le marché de la sûreté aéroportuaire

115. Depuis lors, aux Etats-Unis, les technologies biométriques ont été imposées comme moyen d'éradiquer le terrorisme. Le Committee on Homeland Security a légiféré en 2008 afin de perfectionner les règles en vigueur et intégrer plus efficacement la biométrie comme moyen d'identification[144].
Les mesures prises consistent à améliorer les systèmes biométriques, tout en permettant d'établir une certaine interopérabilité entre le personnel travaillant dans les aéroports et les usagers du transport aérien.

116. Au sein de l'Union européenne, l'insertion de systèmes biométriques dans les aéroports ne fait pas l'unanimité entre les pays membres.

En France, la CNIL a autorisé le directeur général de l'établissement public Aéroport de Paris dans une délibération n° 2005-020 du 10 février 2005, à tester des systèmes biométriques au sein des aéroports de Roissy-Charles de Gaulle et Orly[145]. Un décret paru au Journal officiel

[144] "This bill is an innovative approach towards legislating smart security, it ensures there is a comprehensive plan in place before airports begin using biometric identification for its workers," said Thompson. "This is not about re-inventing the wheel or putting a stop to any good work at TSA – it is about helping us build upon smart, efficient, and effective airport security measures needed to secure Americans and protect a vital industry to our economy and resiliency." Extrait du H.R. 5982, The Biometric Enhancement and Airport-Risk Reduction (BEAR) Act of 2008. Discours de Bennie G Thompson, Président de la Commission. Site Internet du Committee on Homeland Security : http://homeland.house.gov/

[145] CNIL, Délibération portant avis sur un projet de décret en Conseil d'Etat relatif à une expérimentation ayant pour objet d'améliorer, par comparaison d'empreintes digitales, les conditions et la fiabilité des contrôles

du 28 mai 2005, a autorisé l'expérimentation de ce dispositif, nommé « PEGASE », basé sur le contrôle par empreintes digitales, des voyageurs inscrits au programme[146]. Cette expérimentation a duré un an et a eu pour finalité de faciliter la circulation des passagers à la frontière ainsi que d'améliorer les contrôles de la police des frontières en constituant une base de données centralisée, incluant les minuties d'empreintes digitales des deux index des intéressés. Elle a pour autre objectif de « *tester la performance du système d'authentification biométrique choisi, de mesurer les bénéfices que l'automatisation partielle du contrôle du passage aux frontières est susceptible d'apporter et d'étudier son impact sur les passagers s'y soumettant volontairement.* » La CNIL a autorisé cette expérimentation au regard des précautions prises lors de l'enrôlement des données et à condition que soient définies « *les conditions de mise en œuvre, d'alimentation, de consultation, de mise à jour et d'effacement de cette base.* »

L'OACI cherche à adopter un standard de normalisation tendant à uniformiser les systèmes biométriques dans les aéroports qui emploient ces technologies. Ce standard est une norme ISO (International Standard Organisation).

117. Les industriels ne se sont pas contentés d'implanter la biométrie dans les grands marchés de la sécurité mais ont développé des dispositifs pour les particuliers. L'expression de Charles Copin pour désigner ce phénomène est la biométrie de confort. C'est le fait pour les individus d'avoir recours à des techniques biométriques afin de sécuriser certains de leurs biens particuliers comme les ordinateurs et les serrures par exemple (B).

effectués lors du passage de la frontière à l'aéroport Roissy-Charles-de-Gaulle, disponible sur le site au www.legifrance.gouv.fr

[146] Décret n° 2005-556 du 27 mai 2005 portant création à titre expérimental d'un traitement automatisé de données à caractère personnel relatives à des passagers de l'aéroport Roissy - Charles-de-Gaulle, JO n° 123 du 28 mai 2005, p. 9353

B. Les usages de sécurité de confort

118. Parallèlement à l'usage de la biométrie sécuritaire, s'est donc développée la biométrie dite de confort. Cette expression reprise à Charles Copin[147] résume parfaitement le développement croissant de la biométrie pour les particuliers, celle qui est accessible chez soi pour la protection de ses biens personnels. Elle apparaît dans le contrôle d'accès logique (1°), dans la sécurisation des paiements (2°) et dans bien d'autres marchés (3°).

1°. Le marché du contrôle d'accès logique

119. En préambule, il est nécessaire de distinguer le contrôle d'accès physique, le pointage et la gestion du temps de travail, du contrôle d'accès logique.
Le contrôle d'accès physique permet de pénétrer dans des bâtiments hautement sécurisés, type banques, mais aussi à des bâtiments d'entreprise ou bien à des appartements de particuliers.
Le contrôle d'accès logique est mis en place dans le cadre de la gestion d'entreprise et permet de veiller à une meilleure organisation de la gestion des emplois du temps ou du pointage du personnel. Il est employé sur des postes plus restreints comme des ordinateurs, serveurs, ou plus largement sur un poste de travail informatique.
C'est cette troisième catégorie du marché du contrôle d'accès en biométrie qui est développée chez les particuliers désirant assurer une meilleure protection de leurs biens personnels.

L'environnement pris en considération est plus restreint, (bureaux, salles d'ordinateurs) et la solution proposée s'apparente plutôt à remplacer le mot de passe par de la biométrie tout en conservant l'utilisation du nom d'utilisateur.

Certains produits sont externes à l'ordinateur, comme le clavier ou un port USB, tandis qu'une caméra peut être intégrée à l'ordinateur afin de procéder à un système de reconnaissance faciale.

[147] C. Copin, journaliste spécialisé dans les nouvelles technologies est à l'origine de cette expression. Il y a fait référence lors du salon Identech (juin 2005), dont il est le commissaire général.



148



149

120. Ces technologies se sont aussi étendues à la sécurisation des paiements (2°).

2°. La sécurisation des paiements

121. L'Afrique du Sud, a, la première, développé des techniques biométriques, suivie par le Cameroun, dès le printemps 2009 (2-1). La biométrie est intervenue aussi dans le domaine de la sécurisation des paiements par carte bancaire (2-2). Dans ce cas, elle peut être efficace à deux niveaux : d'une part, pour déjouer les pièges d'identités multiples en attribuant à chaque utilisateur une carte nominative et d'autre part, afin de contrôler l'identité des personnes percevant l'argent.

2-1. La sécurisation des versements de pensions et salaires

122. Les techniques biométriques permettent un haut niveau de sécurisation en ce qui concerne les paiements. C'est la société Sagem, pionnière en la matière, qui a mis en place avec succès, un système biométrique pour le versement des salaires et des pensions de ses employés, en Afrique du Sud.

Il en va de même pour le Cameroun, où la Caisse de Prévoyance des pensions sociales, verse depuis le mois d'avril 2009, les pensions aux 80 000 assurés de ce pays. Des capteurs et des lecteurs biométriques ont pour mission de faciliter la procédure de paiement. Ce moyen de règlement tend à éviter les paiements fictifs.

---

[148] www.afjv.com. Tous droits réservés.
[149] www.techni-contact.com. Tous droits réservés.

123. Ces procédés se sont étendus aux paiements par carte bancaire (2-2).

2-2- La sécurisation des paiements par carte bancaire

124. C'est dans ce domaine qu'il a été nécessaire de développer, le plus rapidement possible, des solutions anti-fraude. En effet, en corrélation avec l'avènement de l'Internet, s'est développée la cybercriminalité. Les utilisateurs, dans la crainte d'oublier leur mot de passe, le notent à proximité de leur carte. Cependant, en cas de perte ou de vol, les fraudeurs ont accès à leurs comptes. La biométrie, en la matière, est utilisée dans le cadre du contrôle d'accès. La plupart du temps elle sert à remplacer le mot de passe par l'empreinte digitale d'un ou deux doigts.

Selon Cybersource, les e-fraudes en 2008 ont fait perdre aux commerçants américains la somme de 4 milliards de dollars. Actuellement, de nombreux procédés se sont développés au Japon, où en 2005, la fraude bancaire s'est élevée à 2,3 milliards de yens soit environ 265 millions d'euros.

Afin de réduire considérablement ces fraudes, le groupe Mitsubishi Tokyo Financial Group a développé un distributeur de billets, qui, à l'aide de la carte bancaire propre à la banque ainsi qu'un système de reconnaissance du contour veineux, permet de retirer l'argent des clients en toute sécurité. Le coût de ce service est répercuté sur l'utilisateur japonais qui paie un abonnement annuel d'un montant égal à 8050 yens, soit environ 76 euros.

Plus récemment, en 2006, la Sumitomo Mitsui Banking Corporation a utilisé un système presque identique à celui du groupe Mitsubishi. La seule différence, c'est qu'il se base uniquement sur le réseau veineux d'un seul doigt.

D'autres équipements vont, à l'avenir, être dotés de systèmes de reconnaissance biométrique. Plusieurs autres groupes, tels Visa, travaillent actuellement sur ce type de projet.

L'insertion de la biométrie, au Japon, pose visiblement moins de difficultés. La population accepte plus facilement l'usage de techniques biométriques, ce qui facilite considérablement son expansion.

Grâce à de nouvelles machines, la société Hitachi permet à ses clients de faire leurs courses dans les magasins partenaires de l'opération, sans sortir d'argent. Il suffit d'apposer à la caisse du supermarché un de ses doigts précédemment enregistré, pour que le paiement soit débité directement du compte bancaire du client. Cette technologie se base sur la structure des vaisseaux capillaires du doigt et serait, selon Hitachi plus fiable que la reconnaissance par empreintes digitales.



150



151

125. Au fur et à mesure, de façon plus ou moins insidieuse, la biométrie s'est hissée dans notre quotidien. De plus, elle est devenue ludique depuis qu'elle a été développée pour les voitures, les sacs à main et d'autres applications (3°).

[150] Image d'une publicité japonaise Visa prônant le paiement par carte bancaire à indentification biométrique. Site internet Clubic : http://www.clubic.com/actualite-79880-live-japon-payer-personne-biometrie.html.Tous droits réservés.
[151] Disponible au www.programmation.fr. Tous droits réservés.

3°. Les autres utilisations de la biométrie

126. La biométrie tend à se développer de plus en plus dans les objets de la vie courante. Les exemples les plus flagrants se trouvent dans le domaine de la téléphonie mobile. Si pour le moment, cette technologie n'est pas massivement implantée en Europe et aux Etats-Unis, rien, en théorie, n'empêche son déploiement comme en Asie, où des millions d'appareils ont été vendus. La société SecurePhone envisage l'implantation de la biométrie dans ses téléphones mobiles « trust-ES ». La société Toshiba, partie du constat que près de 90% des cadres dirigeants conservent des informations sensibles sur leur téléphone a, quant à elle, développé un téléphone mobile avec reconnaissance d'empreintes digitales.
D'autres technologies pourraient être employées puisque les téléphones mobiles sont, à ce jour, équipés de caméras ou capteurs à reconnaissance vocale. Toutefois, l'usage de la reconnaissance par l'empreinte digitale est la plus prometteuse dans ce domaine.





[152]

127. Au-delà des applications biométriques précédemment envisagées, il en existe de plus marginales. Le marché de l'automobile tend à se développer dans ce domaine. En effet, en ce qui concerne le contrôle d'accès, un système antidémarrage biométrique basé sur un système de reconnaissance par empreinte digitale est déjà mis en place. Il permet au propriétaire du véhicule d'être seul identifié et autorisé à conduire son véhicule. A l'occasion du salon de l'automobile de Tokyo au Japon, le groupe Hitachi a présenté un système biométrique, qui permet à la fois de sécuriser l'accès au véhicule et de personnaliser le poste de conduite (position du siège ou du volant) en fonction des préférences des automobilistes.

[152] Exemples d'applications biométriques sur téléphones mobiles. Site internet de Jean-François Mainguet http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint_products_pdaphones.htm. Tous droits réservés.

Pour se faire, la technologie de reconnaissance de l'ensemble des veines du doigt est préférée à celle de l'empreinte digitale.



[153]

Aux Etats-Unis d'Amérique, l'identification biométrique s'est aussi développée dans la vie courante. La société pétrolière Exxon, a fait placer dans ses stations-service, un système d'identification biométrique aux pompes. Ainsi, les clients de cette enseigne n'ont plus à sortir leur carte bleue pour payer, seul un porte-clés ou une montre communique avec le système de la pompe à essence. Ce système, appelé « speedpass », est basé sur une identification par radiofréquence qui transmet le code de sécurité et l'identification. Aucune information financière ou personnelle n'est stockée sur le dispositif.

Dans la même démarche, la société Shell a développé un système de paiement par reconnaissance biométrique des empreintes digitales, dans dix stations essence de la ville de Chicago. Les systèmes mis en place permettent la numérisation des empreintes digitales à la pompe. Les clients peuvent, par ce moyen, faire débiter l'argent de leur carte de crédit et retirer de l'essence sans difficulté. La seule contrainte réside dans le fait d'être préalablement enregistré dans le système. Pour la société Shell, le but de cette opération est de diminuer le temps d'attente aux pompes et de fidéliser la clientèle.
Des applications plus ludiques ont été crées par des marques telles que Louise Wilson qui a développé un sac à main à ouverture biométrique.

[153] Exemple de dispositif biométrique installé par Audi sur certains de ces modèles. Site de Jean-François Mainguet : http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint_products_cars.htm. Tous droits réservés.



154

128. La recherche compte ainsi s'attaquer par la suite aux différents freins qui limitent l'adoption de ces nouvelles techniques.

Premier inconvénient de la biométrie, le stockage d'informations personnelles. Face à ce problème, les industriels envisagent le stockage des informations sur une carte à puce ou des tags USB personnels. De cette façon, seule, la personne identifiée conserve son empreinte digitale sur un support qui lui est personnel. La CNIL est d'ailleurs favorable à ce type de stockage de données et ne pourra l'empêcher dans la mesure où il n'y a pas de constitution de bases de données.



155

129. Deuxième inconvénient, les différences socio-culturelles et juridiques entre pays. Alors que certains pays sont très avancés en matière de biométrie, d'autres craignent ces systèmes. Les avancées ne sont pas homogènes et peuvent poser des difficultés. L'exemple le

[154] Site Internet de Jean-François Mainguet : http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint_products_misc.htm. Tous droits réservés.

[155] Exemples de stockages USB biométriques développés par les marques Trek ou Mémory Expert. Site de Jean-François Mainguet : http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint_products_drives_flash.htm. Tous droits réservés.

plus probant est la comparaison qu'il est permis de faire entre les Etats-Unis et la France. Cette difficulté ne peut être résolue que par une coopération accrue entre nations utilisatrices de la biométrie. La normalisation tient une place fondamentale dans l'insertion de la biométrie à l'échelle internationale.

Enfin, dernier inconvénient, la diversité des solutions du marché. Cet inconvénient ne peut être résolu dans la mesure où la biométrie constitue un marché et que des standards commencent à exister. Les groupes industriels tentent de trouver toujours plus de solutions de sécurisation et tentent de plus en plus de faire entrer la biométrie dans le quotidien des individus.

Tenter de contrôler la diversité des solutions du marché reviendrait à tenter de limiter la propagation des ordinateurs ou autres outils technologiques. Le déploiement de la biométrie ne peut pas être freiné.

130. Elle est considérée aujourd'hui comme une des techniques de sécurité les plus fiables et son taux de reconnaissance avoisine souvent les 100%. Cependant, des erreurs surviennent et peuvent avoir des conséquences sur les données personnelles (Section 3).

Section 3. Les défaillances potentielles des outils biométriques et les éventuelles conséquences sur la protection des données personnelles

131. « *Il n'existe pas à ce jour de système biométrique infaillible et il n'en existera sans doute jamais. Cette phrase d'introduction, assez provocatrice, exprime pourtant une réalité incontournable. On touche là, un point sensible qui surprend souvent l'interlocuteur qui découvre la biométrie. Puisqu'une technique comme l'empreinte digitale, par exemple, est réputée infaillible pour identifier un individu, il est surprenant de parler en termes d'erreurs : on s'attendrait à avoir des systèmes absolument sans failles*[156] ».
Cette affirmation n'est pas uniquement l'opinion de Jacques Pierson mais celle de nombreux professionnels dans le domaine[157].

132. Ces défaillances potentielles ne sont pas seulement imputables aux techniques biométriques elles-mêmes mais dépendent aussi de l'environnement dans lequel elles sont utilisées.
Différents facteurs entrent en ligne de compte, tels que les facteurs humains (A), ou statistiques (B).

A. L'influence du facteur humain sur la fiabilité des systèmes biométriques

133. Il faut garder à l'esprit que la biométrie reste la « *science des variations biologiques, des phénomènes qui s'y rattachent et des problèmes qui en découlent.* » La définition d'Eugène Schreider prend tout son sens lorsque l'on s'interroge sur la fiabilité des systèmes biométriques. Il s'agit de mesurer des variations humaines, dont les erreurs sont souvent plus imputables au sujet qu'à la machine.

La reconnaissance biométrique intervient en deux phases. D'abord la phase d'enrôlement, pendant laquelle, l'individu va, par exemple, apposer son doigt, pour la capture d'une empreinte digitale sur le capteur. La mesure effectuée est alors traduite informatiquement sous

[156] J. PIERSON, « La Biométrie, l'identification par le corps », Coll. Informatique, éd. Hermès Science, Lavoisier, 2007, p. 158.
[157] Opinion affirmée par le UK Biometrics Working Group "Use of Biometrics for Identification and Authentification" Advice on Product Selection – Issue 2.0 – 21 janvier 2003 p. 4

forme de gabarit. Ensuite pendant la phase d'identification, l'individu appose à nouveau son doigt pour être identifié. L'individu, sollicité à deux reprises, à des intervalles plus ou moins importants dans le temps, peut influer sur le résultat. Par exemple, une personne qui a subi un traumatisme comme une brûlure ou une entaille sur le doigt utilisé lors de la phase d'enrôlement, peut ne pas être reconnue pendant la phase d'identification. Par ailleurs, un facteur psychologique est aussi à prendre en considération, non pas pour être utilisé comme critère de performance technique, mais comme critère d'opportunité de l'implantation d'un système.
Chaque individu a un seuil d'acceptabilité à l'égard des systèmes de reconnaissance biométrique. Ces derniers seraient bien plus efficaces s'ils étaient acceptés par la population qui s'y soumet.

Ainsi, ils ne sont pas acceptés de la même façon selon la culture, le pays et l'histoire de ce pays. Par exemple, au Japon, les systèmes de reconnaissance biométrique sont bien plus acceptés par la population qu'en France. Une des explications résiderait dans le fait qu'en France, la reconnaissance biométrique a commencé à être utilisée par la police scientifique, lors de scènes de crime. Aujourd'hui, par manque de communication et de dialogue démocratique sur ces questions, la biométrie est toujours perçue comme une technique d'identification à seul objectif sécuritaire ou judiciaire.
De ce point de vue, il est difficile d'espérer une bonne coopération de la population.

De plus, certaines techniques sont plus « invasives » que d'autres et nécessitent d'avoir certaines exigences techniques. Une étude menée par la National Security Agency[158] a démontré que l'âge, le sexe, l'origine ethnique ou sociale pouvait affecter la performance de certaines techniques. Ainsi, le taux de faux rejets seraient plus important chez les jeunes et les personnes âgées.

Enfin, plus influent, le facteur démographique portant sur la généralité et la permanence des caractéristiques biométriques, leur évolution dans le temps.

[158] National Security Agency, "Guidelines for placing biometrics in smartcards" version 1.0, 15 Sept. 1998, p. 18, disponible sur le site www.biometrics.org

Le General Accounting Office américain[159] a déclaré qu'il y a entre 1 et 3% des individus qui ne présentent pas la donnée biométrique correspondant à la technique employée (membre amputé ou manquant, défaut d'empreinte digitale, doigts abîmés par un travail manuel, muets) et a déclaré que la reconnaissance faciale constituait sur ce point la technique biométrique la moins discriminante.

Les conséquences sur les données personnelles peuvent être nombreuses. La plus excessive serait de discriminer à l'identification, une personne ne disposant pas de la donnée biométrique employée. Ce principe de non-discrimination doit être garanti à la personne et lui permettre d'être identifiée par un autre procédé, qu'il soit ou non biométrique.

134. Tout en ayant une incidence sur la fiabilité de l'outil biométrique, ces difficultés ne sont cependant pas insurmontables, ce qui n'est pas le cas des limites constituées par le facteur statistique. (B)

[159] GAO "Biometrics for Border Security", évaluation technique de l'utilisation de la biométrie pour la sécurité des frontières, nov. 2002.

B. L'influence du facteur statistique sur la fiabilité des systèmes biométriques

135. La statistique est définie, selon le dictionnaire Robert, comme étant la « *science et techniques d'interprétation de données trop complexes et trop nombreuses pour être appréciées sans calcul* ». La statistique fait donc partie intégrante de la biométrie car elle vise à prouver l'identité certaine d'une personne en la reliant à une donnée.

Il est souvent dit que la biométrie n'est pas et ne peut être infaillible et ce, même si la donnée biométrique est considérée comme unique et immuable. Cet argument ne tend toutefois pas à démontrer scientifiquement la fiabilité des systèmes biométriques. D'autres critères doivent être étudiés, comme les critères de performance.

Les taux d'acceptation et de rejet constituent des critères de performance des systèmes biométriques, au point que cette « *guerre des taux*[160] », n'a plus simplement des enjeux techniques, mais aussi économiques et politiques. Il y a une concurrence croissante sur le marché et la technique qui obtiendra le plus faible taux d'erreurs sera celle qui sera choisie par les organismes gouvernementaux ou par les entreprises privées.
Le FAR (False Acceptance Rate) [161] tend à accepter une personne qui n'a pas été enregistrée dans le système. Il caractérise la sécurité de ce dernier et constitue le ratio entre le nombre de personnes faussement acceptées et le total des personnes enregistrées.
Le FMR (False Non Match Rate) et le FRR (False Rejection Rate)[162] sont des taux qui déterminent la probabilité d'un système de ne pas reconnaître une personne normalement autorisée par celui-ci. Le FRR n'engage pas la sécurité de ce dernier, car il va rejeter des personnes qui y ont initialement accès. Ce taux caractérise le confort du système.
La conséquence est que la personne n'est pas apparentée à sa donnée biométrique enregistrée.
Le taux de faux rejets est donc le ratio entre le nombre de personnes enregistrées.
Ces taux sont issus des réglages qu'opèrent les hommes sur ces machines et du seuil fixé préalablement.

[160] Expression employée dans le rapport (1ère partie) de l'Office parlementaires d'évaluation des choix scientifiques et technologiques sur « les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre » Christian CABAL, 16 juin 2003, p. 31.
[161] Taux de fausses acceptations
[162] Taux de faux rejets

Dans le cadre de l'authentification, Jacques Pierson rappelle que « *le score de comparaison entre deux données biométriques est considéré comme croissant avec la probabilité que les deux données soient identiques. Il est comparé à un seuil fixé préalablement : si le score est supérieur au seuil, les données biométriques sont déclarées identiques, mais si, au contraire, le score est inférieur au seuil, les données sont déclarées différentes*[163] ».

Pour l'identification, le système possède une base de données dans laquelle sont préalablement enregistrées les données biométriques. La donnée de référence est intégrée au système, de ce fait si la donnée de l'individu est enregistrée, il sera reconnu en apposant son empreinte.

136. Si la biométrie n'est pas fiable à 100% parce que la statistique donne des probabilités et non des certitudes, il convient de s'assurer que les données personnelles sont efficacement protégées. La CNIL a pour mission principale, dans ce domaine, de faire appliquer des règles de droit protectrices des individus en matière « d'informatique et libertés ».
Ces règles sont contenues dans « sa doctrine », établie au fur et à mesure des autorisations, depuis maintenant quelques années.

[163] J. Pierson, « La biométrie, l'identification par le corps », Coll. Informatique, Hermès Science, Lavoisier, 2007, p. 173

137. Le choix d'implanter un dispositif biométrique est souvent l'aboutissement d'une réflexion menée sur la politique de sécurité et la stratégie de gestion des activités humaines au sein de l'entreprise. Ce choix n'est pas sans conséquences sur la collecte et la gestion des données personnelles. C'est pourquoi cette réflexion sur la maîtrise collective des traitements de données biométriques doit nécessairement être guidée par des principes fondateurs développés par la Commission nationale de l'informatique et des libertés tels que le principe de finalité et le principe de proportionnalité.

Ces principes qui régissent la maîtrise collective de la biométrie en entreprise peuvent s'avérer hétérogènes dans les effets qu'ils produisent : le principe de finalité sera malléable (chapitre1) alors que le principe de proportionnalité sera réellement efficace (chapitre 2)

Chapitre 1. La sujétion du traitement de données biométriques au principe de finalité

« *On peut définir la Science-fiction*
comme la branche de la littérature
qui se soucie des réponses de l'être humain
aux progrès de la science et de la technologie[164] ».

138. L'évolution de l'être humain va de pair avec l'évolution scientifique et le progrès technologique. La mise sur le marché d'appareils techniques plus performants, a permis de développer les dispositifs biométriques à grande échelle.
En ce qui concerne la biométrie, une grande disparité existe à ce jour entre les pays quant aux législations du travail. Elle est liée, d'une part, à l'acceptation par la population de cette technologie et, d'autre part, à la facilité avec laquelle ces techniques sont introduites tant dans le monde du travail (contrôle d'accès et ressources humaines) que dans la vie quotidienne (passeport biométrique, biométrie sur les ordinateurs portables et autres applications) [165].

Alors que les Etats-Unis sont « en inflation législative » depuis 2001 d'abord sur la sécurité publique (Patriot Act I et II, création du Department of Homeland Security), ensuite sur l'insertion de données biométriques dans les documents de voyage[166], le Canada reconnaît sa difficulté à intégrer la biométrie dans sa législation, devenue désuète en matière de protection de la vie privée[167]. Pour le secteur privé, des règles protectrices des données personnelles sont envisagées mais par domaine d'activités (assurance, santé, banque), peu d'entre elles évoquent directement la biométrie.

---

[164] Isaac Asimov, extrait de la préface à « David Starr, justicier de l'espace », Isaac Asimov, éd. Lefrancq, 1993
[165] Supra n° 53 et s.
[166] Passenger Name Record est un accord passé entre les Etats-Unis d'Amérique et l'Union européenne autorisant les compagnies aériennes européennes à fournir les données personnelles de leurs passagers aux autorités américaines, sous condition d'une protection adéquate des données personnelles dans ce pays.
Commission européenne, décision 2004/535/CE du 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis, disponible au http://eur-lex.europa.eu
[167] L. Acharya, « La biométrie et son usage par l'Etat », Division des sciences et de la technologie, bibliothèque du Parlement, 11 septembre 2006, disponible sur le site www.parl.gc.ca

Parallèlement, l'Office du commissaire à la protection des données australien a anticipé cet engouement pour la biométrie, puisqu'il a accepté d'introduire dans sa politique de protection de la vie privée, un code de conduite sur les données biométriques, établi par un institut indépendant australien.

Au sein de l'Union européenne, la Directive de 1995[168] a posé les jalons des lignes directrices de la protection des données personnelles, en chargeant les Etats membres en vertu de l'article 5, de « préciser » les conditions de licéité des traitements de données à caractère personnel[169]. Comme ce sont des données sensibles, en France, le législateur a précisé les grands principes de protection de ces dernières, et a confié à la CNIL le soin de contrôler la mise en place de la biométrie dans son contenu comme dans ses formalités.

Les enjeux de la biométrie en entreprise sont divers et variés. Ils offrent bien sûr des garanties d'identification, de fiabilité et de sécurité, mais aussi une meilleure rentabilité, dans la gestion des ressources matérielles et humaines. Pour tout cela, la biométrie représente, pour les dirigeants de sociétés un attrait qui n'est plus à démontrer. Cependant, il importe de trouver impérativement un juste équilibre entre l'utilisation de ces nouvelles technologies et la protection des données personnelles des salariés, protection qui doit être en tous points garantie.

139. Depuis la modification de la loi Informatique et libertés, opérée par la loi n° 2004-801 du 6 août 2004[170], les entreprises doivent procéder à une demande d'autorisation préalable d'implantation d'un dispositif biométrique. Antérieurement à 2004, seul, le secteur public était soumis à la procédure de demande d'autorisation. Les entreprises du secteur privé avaient pour seule obligation de déclarer le dispositif biométrique auprès de la CNIL, quelle que soit la technologie employée. Cependant, la propagation des dispositifs biométriques au

[168] Directive 95/46/CE du Parlement européen et du Conseil, 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 n° L 281 du 23 nov. 1995 p. 0031 – 0050.

[169] Le traitement automatisé de données à caractère personnel concerne « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction* » Art. 2 de la directive du Parlement européen et du Conseil n° 95/46/CE du 24 octobre 1995 précitée

[170] Loi n° 2004-801 du 6 août 2004, JO 7 août 2004.

sein des entreprises, ajoutée à leur facilité d'implantation, ont laissé entrevoir la diffusion non maîtrisée de données à caractère personnel.

Depuis la loi de 2004, « *tous les traitements comportant des données biométriques doivent faire l'objet d'une autorisation préalable de la CNIL*[171] ». En cas de contrôle par l'inspection du travail, l'employeur ou son responsable de traitement doivent être en mesure de fournir le récépissé attestant de la déclaration préalable de traitement[172]. A défaut, l'article R. 8114-2 du Code du travail sanctionne l'absence de présentation des documents d'une amende prévue pour les contraventions de troisième classe[173].

Nous excluons d'ores et déjà, la procédure de déclaration de l'article 27 I 2° de la loi du 6 janvier 1978 modifiée[174] applicable aux traitements effectués par l'Etat et qui ne concerne en rien les entreprises. Cette procédure spécifique fait l'objet d'un avis motivé et publié par la CNIL avant d'être autorisé par le Conseil d'Etat.

En revanche, les procédures d'autorisation préalable et de déclaration simplifiée sont les procédures ouvertes aux entreprises désirant installer des dispositifs biométriques selon les cas dans lesquels elles se situent.
La procédure d'autorisation préalable devient la procédure « de droit commun »[175] pour l'implantation d'un dispositif biométrique, que les traitements relèvent du secteur public ou privé[176]. Pour les traitements qui ont fait l'objet d'une autorisation unique de la CNIL, seul un engagement de conformité à ce traitement est exigé[177].

---

[171] CNIL, La biométrie sur les lieux de travail, rubrique identité numérique, fiche pratique, disponible sur le site internet de la CNIL au www.cnil.fr
[172] C. trav. art . D. 8113-3 « *En cas de traitement automatisé de données nominatives pour la tenue d'un registre, l'employeur ou le responsable du traitement justifie à l'inspecteur du travail de la délivrance du récépissé attestant qu'il a accompli la déclaration préalable prévue par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* »
[173] Les amendes peuvent s'élever à 450 euros pour les personnes physiques et 2250 euros pour les personnes morales.
[174] « *Sont autorisés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés :*
2° Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'identification ou au contrôle de l'identité des personnes. »
[175] Traditionnellement, la procédure de déclaration disposée à l'art. 22 est la procédure dite de droit commun. Cependant, au regard du seuil de sensibilité des données biométriques, nous considérons que la procédure de droit commun, est la procédure d'autorisation préalable.
[176] Art. 25-I 8° de la loi n°78-17 du 6 janvier 1978
[177] Art. 25-II de la loi précitée

140. Si la forme du document conserve toute son importance, le fond de la déclaration ne doit pas être négligé. Un traitement de données à caractère personnel ne peut être créé que si les données « *sont traitées de manière loyale et licite* » et si elles « *sont collectées pour des finalités déterminées, explicites et légitimes*[178] ».

Le principe de finalité a un intérêt majeur puisqu'il est un des éléments fondamentaux avec son corollaire, le principe de proportionnalité, qui fonde l'autorisation de la CNIL dans l'encadrement collectif de la biométrie. Il constitue la justification en vue de laquelle le traitement est sollicité, et sans laquelle la collecte des données biométriques des salariés ne pourrait intervenir. Comme il s'agit de la justification du traitement sans laquelle l'autorisation peut être donnée, ce principe est malléable, au gré des délibérations rendues par la CNIL.

Face à une technologie de plus en plus courante, ce principe est-il suffisant pour garantir la protection des données à caractère personnel des salariés ? Si tel est le cas, est-il un frein trop important au développement de la biométrie ?

141. L'aspect procédural, lié à la création d'un traitement automatisé de données biométriques, est souvent soulevé par les chefs d'entreprise comme un frein au développement de la biométrie (Section 1). En effet, si depuis la réforme de 2004, il existe pour une certaine catégorie de traitements, une procédure simplifiée de déclaration de conformité, la majeure partie des traitements est soumise à une procédure d'autorisation préalable. Au sein même de ces autorisations, les responsables de traitement doivent s'acquitter d'un certain nombre d'obligations. Le principe de finalité est l'un des principes « phare », déterminant l'autorisation de la CNIL. Il est différemment apprécié, selon qu'il est utilisé lors d'une authentification ou lors d'une identification (Section 2).

[178] Art. 6 1° et 2° de la loi n°78-17 du 6 janvier modifiée

Section 1. Les procédures de création des dispositifs biométriques en entreprise

142. Avant que la loi du 6 août 2004 ne vienne apporter quelques changements, la loi Informatique et libertés du 6 janvier 1978 ne donnait à la CNIL, dans le secteur privé, qu'un contrôle restreint en matière de biométrie. Une des explications se trouvait dans le critère organique et dans la nature, publique ou privée, du responsable du traitement. Alors que le secteur public devait obtenir une autorisation ou un avis préalable, dans une certaine mesure, le secteur privé devait simplement déclarer son traitement. Dans ce cas précis, la CNIL n'avait qu'une faculté de recommandation.

Une autre explication résidait dans le critère matériel du seuil de sensibilité des données traitées. En fonction des cas, la décision était prise, d'une déclaration préalable du traitement, ou d'un allègement des formalités pour les données courantes. La CNIL ne pouvait s'opposer a priori, à l'installation de matériel biométrique, mais elle disposait d'un contrôle sur les traitements, que par ce biais elle pouvait interdire. Avec la diffusion massive des technologies de surveillance, telles la vidéosurveillance, la géolocalisation, les puces RFID et la biométrie, et de surcroit leur développement croissant dans les entreprises, il devenait donc indispensable d'avoir un contrôle sur leur implantation et leur utilisation.

143. Depuis la loi du 6 août 2004, tous « *les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes*[179] » ont besoin, pour leur installation, de l'autorisation préalable de la CNIL, à l'exception de ceux mis en œuvre par l'Etat, pour lesquels un avis est seulement requis. Pour les traitements biométriques les plus courants, cette énonciation peut être tempérée, lorsqu'il s'agit de la procédure de déclaration de conformité. En effet, pour une catégorie de données biométriques répondant aux mêmes finalités, la CNIL permet au demandeur de déclarer simplement la conformité de son traitement. Pour la biométrie elles sont, à ce jour, au nombre de quatre (007, 008, 009, 019) et tendent à augmenter au gré des progrès technologiques[180].

[179] Art. 25 de la loi du 6 août 2004
[180] Cf. Annexes 6, 7, 8 et 9

144. Désormais, selon les dispositifs biométriques envisagés, la CNIL opère, soit un contrôle a priori des demandes d'autorisation (sous section 1), soit une déclaration de conformité (sous section 2).

Sous section 1. Le contrôle a priori de la CNIL sur les traitements de données biométriques

145. Antérieurement à la réforme, les entreprises du secteur privé devaient simplement déclarer leur traitement sans avoir à demander d'autorisation à la Commission, les traitements de données biométriques échappaient donc à son contrôle. Cette procédure, plutôt libérale, aboutissait à une multiplication de traitements, et particulièrement ceux visant à implanter un dispositif biométrique de reconnaissance par empreintes digitales.

La directive a imposé la mise en place d'un régime de contrôle a priori des demandes, par les autorités de contrôle, « *pour les données susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées*[181] ». Cette procédure devenait une nécessité juridique pour contrecarrer la diffusion massive et incontrôlée des données personnelles, notamment les données biométriques.

Lors de la transposition de la Directive par la loi du 6 août 2004, cette obligation s'est retrouvée énoncée à l'article 25 I 8° de la loi Informatique et libertés : « *sont mis en œuvre après autorisation de la commission nationale de l'informatique et des libertés, à l'exclusion de ceux qui sont mentionnés aux articles 26 (traitement Etat sécurité et infractions pénales) et 27 (traitements publics NIR, biométrie Etat, recensement, téléservices).*
8°) les traitements automatisés de données comportant des données biométriques nécessaires au contrôle de l'identité des personnes »
La procédure d'autorisation préalable, procédure de droit commun pour les traitements biométriques, est indiquée dans tous les cas où la CNIL n'a pas rendu une autorisation unique[182].

[181] Art. 20 de la Directive 95/46/CE du 24 oct. 1995 du Parlement européen et du Conseil, 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 n° L 281 du 23 nov. 1995 p. 0031 - 0050

[182] Infra n°147 et s.

146. La recevabilité de cette procédure est attachée à la satisfaction de formalités de déclaration (A). L'autorisation qui en découle ne prend effet qu'à compter de la notification qui en est faite par la CNIL (B). Dans les hypothèses de transfert des données personnelles hors Union européenne, les entreprises doivent s'acquitter de garanties supplémentaires de protection (C).

A. Les formalités d'autorisation préalable à l'installation de dispositifs biométriques

147. Le responsable du traitement des données biométriques ne peut effectuer directement la collecte des données puisqu'il doit préalablement obtenir l'accord de la Commission.

Il doit remplir un formulaire établi par la CNIL, disponible sur son site internet et fournir un certain nombre d'informations énumérées à l'article 30 de la loi, dans les termes suivants :

« ***I.*** *- Les déclarations, demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections 1 et 2 précisent :*

1° *L'identité et l'adresse du responsable du traitement ou, si celui-ci n'est établi ni sur le territoire national ni sur celui d'un autre État membre de la Communauté européenne, celle de son représentant et, le cas échéant, celle de la personne qui présente la demande ;*

2° *La ou les finalités du traitement, ainsi que, pour les traitements relevant des articles 25, 26 et 27, la description générale de ses fonctions ;*

3° *Le cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;*

4° *Les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;*

5° *La durée de conservation des informations traitées ;*

6° *Le ou les services chargés de mettre en œuvre le traitement ainsi que, pour les traitements relevant des articles 25, 26 et 27, les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;*

7° Les destinataires ou catégories de destinataires habilités à recevoir communication des données ;

8° *La fonction de la personne ou le service auprès duquel s'exerce le droit d'accès prévu à*

l'article 39, ainsi que les mesures relatives à l'exercice de ce droit ;
***9°** Les dispositions prises pour assurer la sécurité des traitements et des données et la garantie des secrets protégés par la loi et, le cas échéant, l'indication du recours à un sous-traitant ;*
***10°** Le cas échéant, les transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne, sous quelque forme que ce soit, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne au sens des dispositions du 2° du I de l'article 5.*
Les demandes d'avis portant sur les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe la liste de ces traitements et des informations que les demandes d'avis portant sur ces traitements doivent comporter au minimum.

***II.** - Le responsable d'un traitement déjà déclaré ou autorisé informe sans délai la Commission :*
- de tout changement affectant les informations mentionnées au I ;
- de toute suppression du traitement[183] ».

148. Ces informations ne sont pas dénuées d'intérêt dans la mesure où elles déterminent les objectifs du traitement (la déclaration de la finalité est l'une des mentions obligatoires) et permettent à la CNIL d'apprécier dans son ensemble la pertinence des données collectées.
Toutefois, les données traitées n'échappent pas au contrôle de la CNIL, même dans les hypothèses de modifications. Le fait d'obtenir un récépissé de déclaration ne donne pas droit, au responsable de traitement, de modifier les caractéristiques ou les finalités du traitement.
Afin d'éviter la sanction de détournement de finalités, il est recommandé au déclarant d'anticiper, lors de la phase déclarative, les éventuelles mutations de l'entreprise, notamment dans les hypothèses de cession où les données collectées peuvent être transférées vers un pays tiers qui n'assure pas le même seuil de protection[184].

[183] Art. 30 de la loi n° 78-17 du 6 janv. 1978 modifiée.
[184] Infra n° 161

149. L'article 8 du décret n° 2007-451 du 25 mars 2007[185], pris pour l'application de la loi Informatique et libertés de 1978 modifiée en 2004, précise les dispositions générales quant aux formalités : « *les déclarations, demandes d'avis et demandes d'autorisation sont présentées par le responsable du traitement ou par la personne ayant qualité pour le représenter. Lorsque le responsable du traitement est une personne physique ou un service, la personne morale ou l'autorité publique dont il relève doit être mentionnée. Les déclarations et demandes sont adressées à la commission :*
1° soit par lettre remise contre signature
2° soit par remise au secrétariat de la commission contre reçu ;
3° soit par voie électronique, avec accusé de réception qui peut être adressé par la même voie ».

Le responsable de traitement dispose de différents moyens de dépôt de sa demande. Notons qu'il a la faculté de faire usage des nouvelles technologies, en transmettant sa demande par voie électronique. La CNIL transmet, dès réception de la demande, un accusé de réception identique à cette dernière, dans ses formes.

150. En cas d'absence de déclaration, l'employeur s'expose à de lourdes sanctions pénales[186]. Par ailleurs, sa responsabilité patronale peut être engagée dès lors que les salariés fichés sans l'autorisation préalable de la CNIL peuvent demander la réparation du préjudice qu'ils ont subi[187].

151. Ces obligations de forme sont accompagnées de contraintes liées à la notification de la demande et soumises aux délais de réponse de la Commission nationale de l'informatique et des libertés (B).

---

[185] Décret n° 2007-451 du 25 mars 2007, JO du 28 mars 2007, p. 5782. Ce décret modifie le décret n° 2005-1309 du 20 oct. 2005 pris pour application de la loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés.
[186] C. pén. Art. 226-16 « *Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende.*
Est puni des mêmes peines le fait, y compris par négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues au 2° du I de l'article 45 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ».
[187] Agen, 1er oct. 1997, Petites affiches, 29 juil. 1998, n° 90, p. 30

B. La notification et les délais de réponse de la Commission nationale de l'informatique et des libertés

152. L'article 25 III de la loi Informatique et libertés, énonce que « *la Commission nationale de l'informatique et des libertés se prononce dans un délai de deux mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois sur décision motivée de son président. Lorsque la commission ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.* »

Le délai de deux mois est le délai habituellement employé par l'administration pour répondre à ses usagers. Ce délai nous paraît raisonnable pour l'étude des demandes d'autorisation.
Quant au régime de la décision, le silence de la Commission ne vaut pas acceptation de la demande contrairement à certaines dispositions du droit administratif[188], mais correspond à la décision opposée, comme le mentionne l'article 25 III ci-dessus. Cette disposition fait appel au bon sens puisqu'il est question de la protection des données personnelles des individus.

153. En ce qui concerne le point de départ du délai de deux mois, il est précisé dans l'article 8 in fine du décret n° 2007-451 du 25 mars 2007 que *« La date de l'avis de réception, du reçu ou de l'accusé électronique fixe le départ du délai de deux mois dont dispose la commission pour notifier ses avis et autorisations, en application du III de l'article 25 et de l'article 28 de la loi du 6 janvier 1978 susvisée. La décision par laquelle le président renouvelle le délai est notifiée au responsable du traitement par lettre remise contre signature. »*

La date de réception de la demande donne le point de départ du délai de deux mois, dans lequel la Commission doit se prononcer. Elle peut s'octroyer la possibilité de renouveler ce délai mais cette décision doit être motivée par le président. Cette contrainte de motivation du renouvellement du délai, nous amène à penser que la Commission conserve cette faculté dans des cas complexes, liés sans doute aux transferts de données hors de l'Union européenne.

[188] L'art. 22 de la loi n° 2000-321 du 12 avr. 2000 dispose que « *Le silence gardé pendant deux mois par l'autorité administrative sur une demande vaut décision d'acceptation dans les cas prévus par décrets en Conseil d'Etat.* »

154. Les transferts de données hors Union européenne doivent obligatoirement être déclarés et font l'objet d'une étude rigoureuse sur les pays concernés et les garanties associées à la sécurité du traitement (C).

C. Le transfert de données biométriques hors Union européenne dans le cadre de la procédure d'autorisation préalable

155. Le transfert des données hors Union européenne consiste, pour une entreprise généralement multinationale, à partager les fichiers contenant les données personnelles de ses salariés, à d'autres filiales du même groupe, situées dans des pays étrangers. Ces transferts sont inhérents à l'activité financière, économique ou sociale de ces entreprises (transferts de fonds, ressources humaines, banque, assurances etc.) Les législations sur la biométrie à travers le monde sont hétérogènes et n'accordent pas les mêmes garanties aux individus. En cas de détournement des données, les conséquences seraient irrémédiables.

156. Au sein de l'Union européenne, les Etats membres autorisent ces transferts, en principe, vers les pays qui garantissent le même seuil de protection (1°). A défaut, les entreprises peuvent quand même transférer leurs données si elles se conforment aux mécanismes juridiques existants (2°).

1°. Principe

157. L'article 68 de la loi Informatique et libertés modifiée précise les conditions dans lesquelles un transfert de données à caractère personnel peut intervenir dans un pays non membre de l'Union européenne. Le responsable de traitement ne peut pas, en principe, effectuer ce transfert sans l'accord de la CNIL, dans la mesure où le pays destinataire des données n'assure pas un seuil de protection suffisant de la vie privée et des libertés fondamentales des individus.

L'appréciation de la suffisance du seuil de protection se fait « *en fonction notamment des dispositions en vigueur dans cet Etat, des mesures de sécurité qui y sont appliquées, des*

caractéristiques propres du traitement, telles que ses fins et sa durée, ainsi que de la nature, de l'origine et de la destination des données traitées[189] ».

Le Conseil et le Parlement européens, ont donné le pouvoir à la Commission, sur la base de l'article 25 6° de la Directive de 1995, de déterminer les pays tiers assurant un niveau de protection adéquat. Dans les faits, cinq pays situés hors de l'Union européenne (Argentine[190], Canada[191], Guernesey[192], Ile de Man[193], Jersey[194], La Suisse[195]) et les entreprises américaines adhérant au Safe Harbor[196], ont été reconnus par la Commission, comme assurant un niveau de protection adéquat. Pour rendre ses décisions, elle s'est basée sur la correspondance entre les législations de protection des données des pays tiers et la Directive européenne.

158. Face à l'intensification des flux de données personnelles entre les Etats-Unis et l'Union européenne et aux disparités entre les législations et surtout, les fortes exigences de l'Union européenne en matière de protection des données personnelles, les Etats-Unis ont mis en place un dispositif, basé sur le volontariat et reposant intégralement sur l'autorégulation de l'entreprise plutôt que sur une intervention législative. Le ministère des Affaires américain (United States Department of Commerce) a voulu assurer un niveau de protection équivalent des données personnelles. Pour une entreprise américaine traitant des données personnelles des ressortissants européens, le dispositif Safe Harbor consiste à s'autocertifier adhérent à une série de principes protecteurs des données personnelles et de la vie privée, publiées par le ministre des Affaires des Etats-Unis. Il s'agit d'un système « *mélangeant les vertus de l'autorégulation et de l'autorité de la puissance publique*[197] ». Ce système est qualifié d' « *effective mix*[198] ». Les principes en vigueur portent notamment sur la finalité légitime ou le droit d'accès.

---

[189] Art. 68 al. 2 de la loi Informatique et libertés modifiée.
[190] Décision de la Commission C(2003)1731 du 30 juin 2003.
[191] Décision de la Commission 2002/2/EC du 20 déc. 2001.
[192] Décision de la Commission du 21 nov. 2003.
[193] Décision de la Commission 2004/411/CE du 28 avr. 2004.
[194] Décision de la Commission 2008/393/CE du 8 mai 2008.
[195] Décision de la Commission 2000/518/EC du 26 juil. 2000.
[196] Ce sont des principes de protection des données personnelles, issus d'une longue négociation entre les Etats-Unis d'Amérique (ministère du Commerce américain Déc. CE, JOCE 25 août 2000, n° L 215, p. 7) et la Commission européenne (Décision 2000/520/EC du 26 juil. 2000 reconnaissant le caractère adéquat de la protection assurée par les principes dits de la « sphère de sécurité »).
[197] Y. Poullet, « Les Safe Harbor Principles - une protection adéquate ? », 17 juin 2000, article disponible sur le site internet de Juriscom.net: http://www.juriscom.net/
[198] Voir les débats de l'OCDE tenus lors de la conférence de suivi d'Ottawa sur le commerce électronique (Paris, nov. 1999).

159. Les différentes décisions prises par la Commission sont pragmatiques. Elles tiennent compte, pour certaines entreprises, de la nécessité d'effectuer ces transferts de données personnelles. Les principes « Safe Harbor » ainsi que les décisions d'adéquation, soulagent les entreprises, de l'établissement de lourdes formalités. Elles doivent tout de même mentionner ce transfert, dans le cadre de la déclaration préalable de traitement de données auprès de la CNIL. Ainsi, en vertu de l'article 30 10° de la loi Informatique et libertés modifiée, la CNIL impose aux entreprises, de préciser tout transfert de données à destination d'un Etat non-membre de la Communauté européenne.

160. Devant la quantité importante de pays ne garantissant pas un seuil de protection des données satisfaisant, la Commission européenne a dû mettre en place des solutions alternatives. Lorsqu'un pays tiers ne dispose pas d'une protection suffisante, le transfert de données personnelles peut être autorisé par différents moyens. (2).

2°. Exceptions

161. Si le pays destinataire des données personnelles ne dispose pas d'un niveau de protection équivalent[199], l'article 69 de la loi Informatique et libertés modifiée, autorise les responsables de traitement à transférer les données personnelles vers ce pays tiers, si la personne concernée a donné son consentement ou si le transfert se fait dans le respect de certaines conditions[200].

---

[199] Art. 68 de la loi Informatique et libertés modifiée

[200] « *Toutefois, le responsable d'un traitement peut transférer des données à caractère personnel vers un État ne répondant pas aux conditions prévues à l'article 68 si la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes :*
***1°** A la sauvegarde de la vie de cette personne ;*
***2°** A la sauvegarde de l'intérêt public ;*
***3°** Au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;*
***4°** A la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;*
***5°** A l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci ;*
***6°** A la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers.*
Il peut également être fait exception à l'interdiction prévue à l'article 68, par décision de la Commission nationale de l'informatique et des libertés ou, s'il s'agit d'un traitement mentionné au I ou au II de l'article 26, par décret en Conseil d'État pris après avis motivé et publié de la commission, lorsque le traitement garantit un niveau de protection suffisant de la vie privée ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l'objet.

162. En ce qui concerne les entreprises désireuses d'échanger certaines données biométriques de leurs salariés, il est possible de régler ces difficultés de transferts entre la maison mère et sa filiale située dans un pays ne garantissant pas une protection adéquate. En premier lieu, les entreprises exportatrices et importatrices de données signent des clauses contractuelles (2.1), ou bien, en second lieu, elles adoptent des règles internes contraignantes appelées Binding Corporate Rules ou BCR (2.2). Ces deux solutions sont toutefois soumises à un contrôle préalable de la CNIL[201]. Ces deux solutions ont été considérées par le groupe de travail « Article 29[202] », comme offrant des garanties suffisantes de la protection des données personnelles[203].

Deux catégories de clauses contractuelles ont été validées par la Commission européenne (modèle 2001 et 2004). Elles couvrent deux hypothèses, l'une concerne deux responsables de traitement (2.1) et l'autre s'établit entre un responsable de traitement et un sous-traitant (2.2).

2.1 Les Clauses contractuelles types

163. Les clauses contractuelles types permettent aux entreprises d'effectuer des transferts de données, hors de l'Union européenne et surtout vers des pays qui ne garantissent pas le même seuil de protection. En pratique, ces clauses sont utiles s'il y a peu de transferts à effectuer.

La Commission européenne a établi un premier modèle en 2001[204]. Ce premier corps de règles a fait l'objet de nombreuses critiques, notamment de la part de la Chambre de commerce internationale. Cette dernière a créé un second corps de règles, à l'aide d'une

---

La Commission nationale de l'informatique et des libertés porte à la connaissance de la Commission des Communautés européennes et des autorités de contrôle des autres États membres de la Communauté européenne les décisions d'autorisation de transfert de données à caractère personnel qu'elle prend au titre de l'alinéa précédent. » Texte issu de l'art. 29 de la Directive du 25 oct. 1995.

[201] Article 69 in fine de la loi Informatique et libertés modifiée

[202] Le Groupe de travail « Article 29 » sur la protection des données est un groupe à caractère consultatif et permanent. Il est institué par l'art. 29 de la Directive européenne. Ce groupe se compose d'un membre des autorités de contrôle désignées par chaque Etat membre. Ses missions sont définies par l'art. 30 de la même Directive.

[203] Groupe de travail « Article 29 » sur la protection des données, Avis 8/2003 relatif au projet de clauses contractuelles types présenté par un groupe d'associations professionnelles ("le contrat type alternatif"), GT 84 11754/03/FR, adopté le 17 déc. 2003.

[204] Décision de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la Directive 95/46/CE du Parlement européen et du Conseil du 25 octobre 1995.

coalition d'associations professionnelles. Le groupe « Article 29 » a émis un avis favorable[205], mais aussi quelques réserves quant à l'exercice du droit d'accès au système de responsabilité, ainsi qu'au devoir de coopération avec les autorités de protection des données.

Ces règles ont été validées par la Commission le 27 décembre 2004[206]. Les deux modèles de clauses sont actuellement valables. Néanmoins, les responsables de traitement ne peuvent ni modifier les clauses ni combiner des clauses individuelles ou « les ensembles » des modèles de 2001 et 2004.

Les clauses types doivent comporter un certain nombre de renseignements tels que l'identification du responsable de traitement établi en France, les catégories de personnes concernées par le traitement, les finalités du transfert, les catégories de données transférées, le destinataire des données, la durée de conservation ainsi que les données sensibles traitées.

Les données biométriques peuvent donc faire l'objet d'un transfert, au titre de ces clauses. Néanmoins, nous nous questionnons sur le réel intérêt de prendre le risque de transférer ce type de données dès lors que l'identification biométrique s'effectue localement pour la plupart des finalités qui concernent la gestion des horaires, la restauration ou les ressources humaines. Cette problématique reste la même pour les BCR, nous la développerons de façon plus exhaustive[207].

Des clauses complémentaires peuvent être ajoutées, comme celles tendant à attribuer la compétence matérielle ou territoriale d'un tribunal en cas de litige ou le recours à l'arbitrage international.

164. Pour les entreprises internationales disposant de filiales dans le monde entier, il est préférable d'utiliser les règles contraignantes d'entreprise (Binding Corporate Rules) si elles transfèrent, dans des pays tiers, de nombreuses données personnelles (2.2).

[205]Groupe de travail « Article 29 », Avis 8/2003 précité.
[206] Commission des communautés européennes, décision 2004/915/CE du 27 déc. 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers, JOCE du 29 déc. 2004 L 385/74.
[207] Infra n° 167

2.2 Les règles contraignantes d'entreprises

165. Les BCR sont des règles qu'une entreprise multinationale peut adopter pour l'ensemble des filiales du groupe afin d'uniformiser les procédures de transferts internationaux de données personnelles. Elles sont utiles pour les entreprises qui doivent effectuer de nombreux transferts. Pour que ces règles soient considérées comme offrant des garanties suffisantes, elles doivent être autorisées par les autorités nationales de protection des données compétentes.

Les BCR visent toutes les entités d'un groupe de sociétés dont les filiales se situent dans des zones géographiques n'assurant pas un seuil de protection des données personnelles équivalent. Ces règles ont vocation à s'appliquer dans le monde entier au sein d'un même groupe. Ce sont des principes-clés qui permettent d'encadrer les transferts de données personnelles en provenance de l'Union européenne. Ce sont aussi des standards internes qui servent de guide informatif pour les salariés mais qui présentent également une garantie de protection des données personnelles, au niveau mondial, pour les clients de l'entreprise.

Le texte fondateur des BCR est l'article 26 de la Directive 95/46/CE qui prévoit « *qu'un État membre peut autoriser un transfert, ou un ensemble de transferts, de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat ... lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants* ».

166. Afin de faciliter l'adoption des BCR, règles trop souvent délaissées à cause du formalisme, dans un premier temps, le groupe « Article 29 », a établi des grilles d'analyses[208] ainsi que des trames[209], sortes de modèles, facilitant l'adoption de ces principes. Dans un second temps, les différentes autorités de protection des données ont décidé, à la fin de l'année 2008, d'accorder des mécanismes de reconnaissance mutuelle, concernant le travail

[208] Groupe de Travail « Article 29 » de protection des données, Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes, WP 153 1271-00/08/FR, adopté le 24 juin 2008.
[209] Groupe de Travail « Article 29 » de protection des données, Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes, WP 154 1271-00-01/08/FR, adopté le 24 juin 2008.

d'instruction de projets BCR. L'instruction opérée par l'un des pays, vaut instruction pour les autres, à charge pour les autorités concernées d'approuver officiellement les BCR visées.

Ces transferts font l'objet d'une grande vigilance de la part de toutes les commissions nationales informatique et libertés des pays de l'Union européenne, car certaines sociétés multinationales souhaiteraient transférer l'intégralité des données de leurs salariés, afin de centraliser les bases de données de « ressources humaines » de leur groupe.

167. La question reste entière de savoir s'il serait possible de transférer des données biométriques par le biais de BCR. Celles-ci peuvent être intégrées aux BCR, puisque les données sensibles peuvent faire l'objet du traitement, dans la mesure où la personne concernée a donné son consentement. Toutefois, selon nous, il ne serait pas judicieux de transférer des données biométriques ni par le biais des BCR ni par celui des clauses contractuelles types.

La biométrie est majoritairement utilisée, au sein des entreprises, pour un contrôle d'accès local sur un lieu déterminé et pour des finalités précises. Nous pensons que les données biométriques sont des données de proximité. Cela signifie que les finalités pour lesquelles elles sont prélevées, ont vocation à s'utiliser quotidiennement et sur le lieu de l'entreprise, par exemple, pour la gestion de l'accès aux locaux ou la restauration et pour des besoins déterminés, souvent différents d'un endroit à un autre. Dans ce cas précis, nous pensons qu'il n'est ni nécessaire, ni pertinent de transférer des données biométriques d'une filiale à une autre. Nous préconisons plutôt de procéder à une nouvelle capture des données biométriques sur le site d'affectation pour les hypothèses de mutation, en effaçant celles du site initial.

168. En conclusion, du point de vue international, de nombreuses solutions permettent aux entreprises de transférer leurs données personnelles, même à destination de pays qui ne garantissent pas un seuil adéquat de protection, à condition de se conformer aux règles établies par l'Union européenne. Du point de vue national, la procédure d'autorisation préalable permet au responsable de traitement, de soumettre la situation « informatique et libertés » de son entreprise à l'appréciation de la CNIL. Selon le choix de la technologie, de la finalité et des moyens employés pour garantir la sécurité des données et l'information des personnes, la CNIL sera encline ou non à donner son autorisation. Cette procédure laisse donc

planer de nombreuses incertitudes quant à son succès. En conséquence, elle est utilisée bien moins souvent ces dernières années, depuis qu'une « doctrine » a été mise en place par la CNIL, basée sur la procédure de déclaration de conformité à une autorisation unique. Cette procédure a pour objectif de simplifier la procédure de déclaration, mais surtout de permettre une collecte immédiate des données biométriques (sous section 2).

Sous section 2. La déclaration de conformité de l'usage de certains dispositifs biométriques

169. La loi Informatique et libertés, dans sa rédaction de 1978, prévoyait la possibilité d'édicter des normes, encadrant l'utilisation de certaines catégories de traitements courants, susceptibles de porter atteinte à la vie privée. Ceux-ci avaient pour finalité, la simplification des procédures déclaratives auprès de la Commission[210]. Depuis la modification opérée par la loi n° 2004-871 du 6 août 2004, les normes simplifiées sont disposées à l'article 24 et sont toujours intégrées au régime de déclaration auprès de la CNIL.

Quant aux traitements soumis au régime de l'autorisation de la CNIL, l'article 25 II de la loi Informatique et libertés énonce que « *Pour l'application du présent article, les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation*[211] ».

Les données biométriques, soumises au régime d'autorisation ont fait l'objet de décisions d'autorisation unique par la CNIL.
En 2006, à l'occasion de la publication d'un guide pédagogique de déclaration, la CNIL a précisé que la déclaration de conformité à une autorisation unique intervenait pour « *certains fichiers ou traitements de données personnelles sensibles ou à risques, qui visent une même*

[210] En ce qui concerne le milieu de l'entreprise, on peut citer la norme simplifiée n° 42 issue de la délibération n° 02-001 du 8 janv. 2002 visant les traitements automatisés d'informations nominatives mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration.
[211] Art. 25 II de la loi Informatique et libertés modifiée en 2004

finalité et des catégories de données et de destinataires identiques, sont autorisés par la CNIL au travers de décisions-cadre, appelées autorisations uniques[212] ».

170. Cette procédure de déclaration simplifiée doit suivre un certain formalisme même si ce dernier est moins contraignant que la procédure d'autorisation préalable
L'article 19 du décret n° 2007-451 du 25 mars 2007 dispose que « *L'engagement de conformité à une autorisation unique prise en application du II de l'article 25 de la loi du 6 janvier 1978 susvisée est adressé à la Commission dans les conditions prévues à l'article 8 du présent décret.* »

L'article 8 du décret n°2007-451 du 25 mars 2007 précise en outre, que « *les déclarations, demandes d'avis et demandes d'autorisation sont présentées par le responsable du traitement ou par la personne ayant qualité pour le représenter. Lorsque le responsable du traitement est une personne physique ou un service, la personne morale ou l'autorité publique dont il relève doit être mentionnée.*
Les déclarations et demandes sont adressées à la commission :
1° Soit par lettre remise contre signature;
2° Soit par remise au secrétariat de la commission contre reçu ;
3° Soit par voie électronique, avec accusé de réception qui peut être adressé par la même voie.
La date de l'avis de réception, du reçu ou de l'accusé de réception électronique fixe le point de départ du délai de deux mois dont dispose la commission pour notifier ses avis et autorisations, en application du III de l'article 25 et de l'article 28 de la loi du 6 janvier 1978 susvisée. La décision par laquelle le président renouvelle ce délai est notifiée au responsable du traitement par lettre remise contre signature. »

171. Devant la multiplicité des demandes d'autorisation en matière de biométrie, la CNIL a dû recourir au mécanisme des autorisations uniques. La majeure partie des demandes était faite par des entreprises désirant implanter des techniques biométriques, dans un objectif de meilleure gestion des contrôles d'accès, de restauration ou de gestion des horaires.

[212] Toutes ces définitions sont issues du Guide de déclaration téléchargeable sur le site internet de la CNIL au www.cnil.fr

Le 27 avril 2006, la Commission a établi trois autorisations uniques dont deux sont à destination des entreprises[213]. Plus récemment, le 7 mai 2009, elle a établi une autre autorisation unique destinée aux entreprises reposant sur la reconnaissance du réseau veineux du doigt de la main[214].

La procédure de déclaration de conformité à une autorisation unique soulève deux commentaires. Du point de vue formel, le responsable de traitement doit effectuer moins de formalités. De plus, elle s'adresse des dispositifs plébiscités par les entreprises qui ont fait l'objet de nombreuses demandes d'autorisation préalable. Elle a donc un réel sens pratique. Par ailleurs, contrairement à la procédure d'autorisation préalable, cette procédure a aussi un fort impact psychologique sur les responsables de traitement car elle a l'avantage de ne pas laisser subsister de doute quant à l'acceptation de la demande auprès de la CNIL. Du point de vue matériel, cette procédure ne nécessite pas de mobiliser, en principe, autant de personnel à la CNIL que les demandes d'autorisation préalable.

172. Pour qu'un responsable de traitement puisse obtenir une autorisation de mise en œuvre de traitement des données biométriques, il doit avoir satisfait aux conditions de forme précédemment étudiées mais aussi se conformer à certains grands principes. L'un d'entre eux, le principe de finalité, est essentiel dans la mesure où il détermine les motivations principales du traitement. Il fait l'objet d'une appréciation différente par la Commission selon qu'il intervient dans un processus d'authentification ou d'identification biométrique (Section 2).

[213] CNIL, Délibération n° 2006-101 du 27 avr. 2006 portant autorisation unique AU-007de mise en œuvre de dispositif biométrique reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail, J.O n° 138 du 16 juin 2006. CNIL, Délibération n° 2006-102 du 27 avr. 2006 portant autorisation unique AU-008 de mise en œuvre de dispositif biométrique reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail, J.O n° 138 du 16 juin 2006.

[214] Délibération n° 2009-316 du 7 mai 2009 portant autorisation unique AU-019 de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle d'accès aux locaux sur les lieux de travail, JO n° 0142 du 21 juin 2009.

Section 2. L'intégration des finalités d'authentification et d'identification biométriques en entreprise

173. En biométrie, le choix de la fonction biométrique d'authentification[215] ou d'identification[216] est intimement lié à la finalité pour laquelle le traitement est envisagé. Un traitement de données biométriques ne peut être effectué sans limitation ni contrôle, il doit se conformer au principe de finalité. Ce principe, qui constitue un élément essentiel du traitement, n'a pourtant jamais été défini. Plusieurs textes internationaux de protection des données personnelles évoquent ce principe mais aucun n'en a donné une définition exacte.

La Convention STE n°108, premier texte juridique international contraignant en matière de protection des données personnelles, qui émane du Conseil de l'Europe, énonce dans son article 5 b que « *Les données à caractère personnel faisant l'objet d'un traitement automatisé sont enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ses finalités*[217] ».

Les principes directeurs de l'Organisation des Nations unies du 14 décembre 1990[218] dans son principe 3 précise « *La finalité en vue de laquelle est créé un fichier et son utilisation en fonction de cette finalité devraient être* ***spécifiées***, ***justifiées*** *et, lors de sa mise en œuvre****, faire l'objet d'une mesure de publicité*** *ou être portées à la connaissance de la personne concernée, afin qu'il soit ultérieurement possible de vérifier:*
a) Si toutes les données personnelles collectées et enregistrées restent ***pertinentes*** *par rapport à la finalité poursuivie;*
b) Si aucune desdites données personnelles n'est utilisée ou divulguée, sauf accord de la personne concernée, à des fins incompatibles avec celles ainsi spécifiées;

---

[215] L'authentification biométrique (1 contre 1) consiste à comparer les données enrôlées d'une personne avec celles qu'il présente sur le lecteur afin d'être reconnu par le système. Les données sont stockées sur un support individuel.
[216] L'identification biométrique (1 contre N) consiste à comparer les données d'une personne à plusieurs autres échantillons de données déjà enregistrés. Pour effectuer cette fonction, les données sont généralement stockées au sein d'une base de données.
[217] Conseil de l'Europe, Convention STE n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janv. 1981
[218] Organisation des Nations unies, Principes pour la réglementation des fichiers informatisés contenant des données à caractère personnel, Adoptés le 14 décembre 1990 par l'Assemblée générale des Nations unies dans sa résolution 45/95 du 14 déc. 1990

c) Si la durée de conservation des données personnelles n'excède pas celle permettant d'atteindre la finalité pour laquelle elles ont été enregistrées. »

174. La loi n° 78-17 du 6 janvier 1978 se référait au principe de finalité[219] de façon incidente dans les dispositions relatives à l'obligation de déclaration (ancien article 19), dans laquelle devait figurer la finalité ainsi que les caractéristiques du traitement. Par ailleurs, l'ancien article 44 de cette même loi, devenu l'article 226-21 du Code pénal, sanctionnait le détournement de finalité.

La loi du 6 août 2004 qui a transposé la Directive de 1995, précise en son article 6, les conditions de licéité de la collecte et du traitement des données à caractère personnel dans les termes suivants :

« *Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :*

1° Les données sont collectées et traitées de manière loyale et licite ;

***2° Elles sont collectées pour des finalités déterminées, explicites et légitimes** et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'aux chapitres IX et X et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ;*

*3° **Elles sont adéquates**, **pertinentes et non excessives au regard des finalités** pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;*

4° Elles sont exactes, complètes et, si nécessaires, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effectuées ou rectifiées ;

5° Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées »

[219] Art. 19, 20, 22 de la loi de 1978

La finalité peut donc être définie comme l'objectif en vue duquel les données personnelles vont être collectées. C'est le but vers lequel tend le traitement, la raison pour laquelle il est nécessaire de collecter des données biométriques. Les principales finalités employées pour des traitements de données biométriques en entreprise seront le contrôle d'accès, physique ou logique, la gestion des horaires ou la restauration (ressources humaines).

175. Ce principe n'est pas apprécié de la même manière selon qu'il est question d'authentification (sous section 1) ou d'identification biométrique (sous section 2). En cas de non-respect de ce principe, le responsable de traitement encourt de lourdes sanctions (sous section 3).

Sous section 1. La finalité d'authentification biométrique intégrée à l'entreprise

176. Les nouvelles technologies intégrées au sein de l'entreprise ont permis, outre un accroissement de la productivité synonyme de rentabilité, un contrôle efficace du personnel. Pour une entreprise, toute nouvelle technologie représente à la fois un progrès mais peut entraîner de même, une régression pour les libertés des salariés. L'Internet donne la possibilité d'accroître la rentabilité et la rapidité des opérations, mais aussi de contrôler le courrier électronique des employés, tout comme l'effectivité du temps passé sur l'ordinateur. La géolocalisation contribue à la sécurité des personnes et des biens transportés, mais elle permet également de prendre connaissance de la position en temps réel des employés dans leur véhicule. La biométrie s'impose, lorsqu'il s'agit de sécuriser les locaux et de faciliter la gestion du personnel. Elle est toutefois en mesure d'aboutir à un « espionnage » des salariés.

Depuis quelques années, dans certaines entreprises, la présentation d'un badge[220] est obligatoire pour comptabiliser les heures de travail effectuées par le salarié. Cependant, si ce badge permet l'identification d'une personne, rien n'assure que le porteur de ce dernier en soit le détenteur légitime. Les nombreuses fraudes constatées ont poussé les chefs d'entreprise à s'équiper d'outils biométriques plus efficaces pour limiter, voire éradiquer ces fraudes.

[220] Dès son origine, en Angleterre, le « badge » était employé comme moyen d'identifier les chevaliers, d'où son emploi dans le langage commun comme un insigne d'appartenance à un groupe. Il sera employé au milieu du XXème siècle en France par le scoutisme sans doute sous l'influence américaine, lors de la campagne d'élection du général Eisenhower (1952 slogan « I like Ike »). Disponible sur le site internet de l'Analyse du Traitement informatique de la langue française : http://atilf.atilf.fr/

177. En biométrie, l'authentification ne peut se faire qu'en complément d'une autre technique de reconnaissance. Cela signifie que l'on n'utilise pas seulement la biométrie, mais qu'il est nécessaire d'avoir recours à une clé physique comme un badge. Ce complément va contenir un numéro identifiant fourni par l'employeur, qui sera comparé au signal biométrique de l'utilisateur, avec la donnée de référence du propriétaire légitime. Cette comparaison s'appelle « comparaison de 1 sur 1 ». Cela signifie concrètement que pour authentifier un individu, il ne sera pas nécessaire de constituer une base de données, plus intrusive. Le principe de finalité impose aux chefs d'entreprise de déterminer, préalablement à tout traitement de données à caractère personnel, les objectifs pour lesquels l'authentification biométrique est préférée.

178. Dès lors qu'un responsable de traitement souhaite implanter un dispositif biométrique, il doit, dans la demande d'autorisation, spécifier précisément la finalité du traitement. Néanmoins, cette dernière sera différemment appréciée par la Commission, selon le degré de traçabilité de la technologie choisie par l'employeur c'est-à-dire un dispositif de reconnaissance par empreinte digitale (A) ou bien d'autres techniques biométriques (B).

A. La spécification insuffisante des finalités au regard de la technique de reconnaissance par empreinte digitale

179. Au regard de la doctrine de la CNIL et en corrélation avec les délibérations rendues ces dernières années, si l'on se réfère à l'attribution des différentes autorisations uniques, nous constatons que le principe de finalité est reconnu comme l'objectif pour lequel une entité recourt à un outil biométrique, dans le but d'améliorer considérablement son domaine d'activité (la sécurité, la gestion…)

Bon nombre d'entreprises a trouvé dans la biométrie, non seulement une solution efficace pour lutter contre les fraudes, mais aussi un moyen de gestion et d'organisation des flux de personnes. Afin d'éviter que la biométrie soit détournée de ses objectifs et devienne le moyen le plus efficace « d'espionner » les salariés, la CNIL va être particulièrement vigilante tant à la finalité du traitement, qu'à ses caractères (explicite, légitime et déterminé).

L'usage de l'empreinte digitale, n'est pas anodin. C'est une technologie dite « à traces », dont les données récoltées sont « sensibles », car spécifiques. La CNIL considère que « *l'empreinte digitale est presque aussi redoutable que les traces d'ADN* » et qu'il « *pourrait presque être soutenu que l'empreinte digitale est aux autres données biométriques ce que le NIR*[221] *est aux autres données personnelles : une information particulière qui présente un risque réel de relâchement du principe de finalité des fichiers*[222]».

180. Les caractères d'unicité et d'immuabilité de l'empreinte digitale nécessitent de prendre certaines précautions. La finalité doit être déterminée, explicite et légitime comme l'énonce l'article 6 de la loi n°78-17 du 6 janvier 1978 modifiée. Ces caractères doivent être confrontés aux différentes finalités utilisées en biométrie soit pour les deux principales, la finalité de gestion des horaires (1°), soit pour celle du contrôle d'accès (2°).

1°. La finalité de gestion des horaires

181. Le contrôle des horaires des salariés est une des manifestations du pouvoir de direction de l'employeur qui exerce un lien de subordination par l'intermédiaire du contrat de travail. Ainsi, comme le relève très justement A. Supiot, « *le temps et le lieu du travail sont d'abord le temps et lieu de la subordination*[223] ». Le « *territoire* traditionnel *de l'entreprise* », lieu au sein duquel s'exerce le pouvoir règlementaire de l'employeur, « *son aire d'autorité*[224] », doit laisser s'exercer les libertés individuelles et collectives des salariés. Le contrat de travail est un contrat qui repose sur un lien de subordination entre l'employeur et le salarié[225].

---

[221] C'est un numéro d'inscription au répertoire, la gestion de ce répertoire est confiée à l'INSEE, il est constitué de 13 caractères comprenant le sexe, l'année, le mois, la commune de naissance suivi d'une clé de contrôle. Le NIR est unique, il est attribué à la naissance et ne change jamais.

[222] C. Cabal, Rapport de l'Office parlementaire d'évaluation des choix scientifiques et technologiques sur « Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre », 1ère partie, 16 juin 2003, p. 57

[223] A. Supiot, « Critique du droit du travail », PUF, 2007, p. 153

[224] « *La gestion administrative de la cantine, œuvre sociale, qui fut confiée au comité interentreprises, ne dispensait pas l'employeur d'exercer sa surveillance dans ce local placé dans son aire d'autorité* », Soc. 20 janv. 1977 n° 75-15.501, Bulletin des arrêts de la Cour de cassation.; n° 51, p. 40.

[225] Le lien de subordination a été défini dans le cadre d'un arrêt de la Cour de cassation du 13 nov. 1996 pourvoi n° 94-13.187, « *...le lien de subordination est caractérisé par l'exécution d'un travail sous l'autorité de l'employeur qui a le pouvoir de donner des ordres et des directives, d'en contrôler l'exécution et de sanctionner les manquements de son subordonné ; ... le travail au sein d'un service organisé peut constituer un indice du lien*

Pour l'employeur, ce lien se matérialise notamment par le pouvoir règlementaire de contrôler le temps de travail de ses salariés. L'employeur doit être en mesure, s'il subit un contrôle, de prouver qu'il s'est conformé aux dispositions légales.

182. La gestion des horaires des salariés par l'emploi de dispositifs biométriques a deux objectifs : la gestion administrative des horaires mais aussi la limitation des fraudes d'éventuels salariés. Dans ce dernier cas de figure, il est nécessaire d'être particulièrement vigilant sur les réelles intentions de l'emploi d'un tel système.

L'article 6 de la loi du 6 août 2004 rappelle que les données personnelles doivent être collectées pour des finalités « *déterminées, explicites et légitimes* ». Ces caractères regroupent l'idée de la spécification des finalités. Un traitement sans finalité est un traitement qui n'a aucune raison valable d'exister. La spécification de la finalité d'un traitement est une obligation légale sans laquelle le traitement ne peut être autorisé. L'article 30 2° de la loi Informatique et libertés soumet la validité de la déclaration, à la présence de mentions obligatoires, dont la finalité.

Ainsi, en matière de biométrie l'on peut considérer que la finalité est déterminée lorsqu'elle délimite précisément le nombre de personnes visées par le traitement des données personnelles ou qu'elle limite les zones d'accès.
La finalité est explicite lorsqu'elle est avouée, claire et précise. Ceci implique que l'entreprise intéressée par l'emploi de ces nouvelles technologies biométriques, va s'engager à donner les réelles motivations qui déterminent l'emploi de ce matériel. Pour obtenir l'autorisation d'installer un outil biométrique, le caractère loyal du traitement des données personnelles du salarié est sous-entendu et nécessaire.

C'est donc bien la question de la légitimité qui est donc la plus délicate et primordiale a appréhender et apprécier. On entend couramment par « légitime », ce qui est conforme à la justice, à l'équité[226]. La question reste donc entière, quant à l'appréciation de la légitimité d'une technologie, faute du recul nécessaire sur cette dernière. C'est la raison pour laquelle le principe de finalité est apprécié, compte tenu des évolutions scientifiques et des précautions,

---

de subordination lorsque l'employeur détermine unilatéralement les conditions d'exécution du travail » Bulletin 1996 V n° 386 p. 275.
[226] G. Cornu, Vocabulaire Juridique, PUF, 2003, p. 519

quelquefois excessives, qui sont prises. L'appréciation de la légitimité soulève de nombreuses interrogations, tant elle dépend des membres de la CNIL, en considération des connaissances techniques à une période donnée.

183. Les employeurs sont enclins à installer des dispositifs biométriques pour bon nombre de finalités. La gestion des horaires par l'utilisation de la biométrie a soulevé des réticences et fait l'objet d'une polémique en 2005, lorsque le tribunal de grande instance de Paris[227] a rendu son jugement. De nombreuses interrogations demeurent quant à la légitimité d'un tel dispositif, tant au regard des libertés individuelles (1-1), qu'à celui de l'éthique (1-2).

1-1 Le contrôle des horaires face aux libertés individuelles

184. L'entreprise est une entité économique au sein de laquelle doivent s'exercer des droits et des libertés. Par certains égards, l'enceinte de l'entreprise constitue un lieu de « contrainte », au sein duquel s'exerce le pouvoir de l'employeur. Cependant, les salariés disposent de libertés. La protection des droits fondamentaux est garantie dans ses sources, au niveau national et international[228], mais aussi dans la diversité que présentent les libertés, qu'elles soient individuelles ou collectives. En ce qui concerne les libertés individuelles, aucune liste n'a jamais été formellement établie, mais le plus souvent, celles remises en cause par le pouvoir de direction de l'employeur sont les plus courantes, à savoir, la liberté d'aller et venir, le droit au respect de la vie privée, le droit d'expression et d'opinion. Pour ce qui a trait au contrôle des horaires, seules les deux premières mentionnées ci-dessus seront concernées par nos développements.

185. Le pouvoir de direction de l'employeur s'arrête là où les libertés individuelles du salarié commencent, même si, selon le Code du travail, des restrictions à ces libertés peuvent intervenir si la nature de la tâche à accomplir l'exige[229]. Le droit au respect de la vie privée ne se limite pas au domicile du salarié mais s'étend à son lieu de travail. L'article 9 du Code civil français reconnaît à tout individu, y compris donc, au salarié, le droit au respect de sa vie

[227] Infra n° 194
[228] Art. 12 de la DUDH ; art. 17 du Pacte international des droits civils et politiques ; art. 7 de la Charte des droits fondamentaux de l'Union européenne
[229] C. trav., Art. 1121-1, infra n° 298

privée. La chambre sociale de la Cour de cassation a visé, à plusieurs reprises cet article, afin de préciser qu'« *il ne peut être procédé au licenciement d'un salarié pour une cause tirée de sa vie privée*[230] ».

Dans le célèbre arrêt Nikon, la Haute Cour a rappelé que le salarié a droit « *au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur*[231] ».

L'intégration de nouvelles technologies au sein de l'entreprise ne peut aboutir à l'espionnage des salariés qui ont droit au respect de leur vie privée dans son enceinte, pendant leurs heures de travail. Par ailleurs, il ne serait pas réaliste d'exiger un usage exclusivement professionnel d'un outil informatique dans une société de l'information et de la communication. L'outil informatique, attribué pour un usage exclusivement professionnel, peut être aussi employé raisonnablement à des fins privées (messagerie électronique privée, téléphone) à condition que cet usage reste « *proportionné*[232] ».

186. Pour contrôler le temps de travail d'un salarié, il existe différents moyens, qu'ils se dénomment pointeuse, badge ou fiche. Cette gestion des horaires au sein de l'entreprise, se fait dans l'intérêt des deux parties : le salarié peut valider le comptage de ses heures, tandis que l'employeur est en mesure de s'assurer de sa présence, de son efficacité et de la durée hebdomadaire de la tâche accomplie. Dans le cas où l'entreprise serait contrôlée par l'inspection du travail ou bien serait obligée d'argumenter devant un tribunal, l'employeur serait alors en mesure d'apporter la preuve du travail effectif de ses employés[233].

Un procédé de gestion des horaires n'est en rien incompatible avec le respect de la vie privée ou la liberté d'aller et venir, dans la mesure où ce dernier a satisfait aux obligations de

[230] Soc. 20 nov. 1991, n° 89-44.605, Bull. 1991 V n° 512, p. 318
[231] Soc. 2 oct. 2001, n° 99-42.942, Bull. 2001 V n° 291, p. 233; RTD Civ. 2002, p. 72.
[232] Soc. 11 mars 1998, n° 1375, RJS 4/1998, n° 415. L'appréciation de la proportionnalité peut se faire par exemple en se basant sur des relevés téléphoniques.
[233] Art. D. 3171-1 du Code du travail issu du décret n° 2008-1132 du 4 nov. 2008, JO n° 0258 du 5 nov. 2008 p. 16879.

déclaration auprès de la CNIL, de consultation des organes représentatifs du personnel[234], d'information du personnel[235], d'affichage[236].

187. Comme nous l'avons évoqué plus haut[237], avant la réforme opérée par la loi du 6 août 2004, les entreprises du secteur privé devaient simplement déclarer le traitement auprès de la CNIL, qui ne pouvait s'y opposer. Pour autant, en cas de défaut de déclaration, la Commission pouvait prendre des sanctions et les salariés s'opposer au traitement illicite. C'est ce qu'a fait un salarié de la société Allied, suite à son licenciement.

Dans cette affaire, la société Allied Signal Industrial Fibers, devenue Honeywell Longlaville en 1993, avait installé un système de badge géré par informatique qui s'appliquait à décompter les horaires des salariés. Pour ce faire, l'employeur avait prévenu ses salariés mais en mentionnant simplement ce dispositif dans le règlement intérieur de l'entreprise, sans avoir fait de déclaration à la CNIL. Devant l'opposition d'un des salariés à dix-neuf reprises de se soumettre à ce dispositif, l'employeur de la société Allied l'a licencié pour faute simple en 1998. En 2000, l'employeur a procédé à la déclaration du traitement. Néanmoins, la cour d'appel de Nancy a déclaré le licenciement sans cause réelle et sérieuse en raison du défaut de déclaration du dispositif auprès de la CNIL à l'époque des faits. La Cour de cassation, dans un arrêt du 6 avril 2004[238], a jugé sur ce point « *qu'à défaut de déclaration à la Commission Nationale de l'Informatique et des Libertés d'un traitement automatisé d'informations*

---

[234] C. trav. art. L. 2323-6, infra n° 382 et s.

[235] C. trav. art. L. 2323-32 « *Le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de celles-ci.*
Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci.
Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. »
C. trav. Art. L. 1222-4 énonce qu'« *Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.* »

[236] C. trav. Art. L. 1321-1 énonce que « *Le règlement intérieur est un document écrit par lequel l'employeur fixe exclusivement :*
1° Les mesures d'application de la réglementation en matière de santé et de sécurité dans l'entreprise ou l'établissement, notamment les instructions prévues à l'Article L4122-1 ;
2° Les conditions dans lesquelles les salariés peuvent être appelés à participer, à la demande de l'employeur, au rétablissement de conditions de travail protectrices de la santé et de la sécurité des salariés, dès lors qu'elles apparaîtraient compromises ;
3° Les règles générales et permanentes relatives à la discipline, notamment la nature et l'échelle des sanctions que peut prendre l'employeur. »

[237] Supra n° 145.

[238] Cass. Soc, 6 avr. 2004, pourvoi n°01-45.227, Société Allied Signal Industrial Fibers, devenue la société Honeywell Longlaville c/ M. Miguel Pacheco, FS- P+B+R+I, (n° lexabase : A8004DB3) ; D. 2004, p. 2736 note R. de Quenaudon.

nominatives concernant un salarié, son refus de déférer à une exigence de son employeur impliquant la mise en œuvre d'un tel traitement ne peut lui être reproché ; » Ainsi, « *le licenciement était sans cause réelle et sérieuse en raison du défaut de déclaration du traitement à la Commission Nationale de l'Informatique et des Libertés* »

Cette décision fait application stricte de la loi Informatique et libertés et soulève plusieurs commentaires et conclusions. Tout d'abord, l'information des salariés n'exonère pas le chef d'entreprise de toute procédure déclarative auprès de la CNIL, et ce, depuis la loi de 2004, évoquée précédemment et dans laquelle il est précisé que les entreprises doivent déclarer la majorité de leurs traitements. Lors de contrôles, la CNIL parvient encore à trouver des entreprises réfractaires aux règles « informatique et libertés ». Certains employeurs pensent pouvoir s'exonérer des procédures de déclaration. Néanmoins, le travail de communication, d'information et de sanction qu'elle opère, tend à rendre ces infractions plus rares.

Par ailleurs, cette décision met un frein aux dérives du pouvoir règlementaire de l'employeur. Le salarié a été licencié pour avoir refusé de se soumettre à un dispositif illégal pour lequel il n'a pas consenti. Il est important que tout employé de l'entreprise puisse exercer son droit de refus de se soumettre à un procédé illégal et qui, par conséquent, n'assure pas la protection de ses données personnelles. Enfin, il nous semble étonnant que les instances représentatives du personnel, généralement impliquées dans la défense des droits et libertés des salariés, aient laissé le salarié assurer seul sa défense.

188. Le contrôle des horaires exigé par la loi, n'a pas vocation à amoindrir la liberté d'aller et de venir, ni attenter à la vie privée du salarié. Différents procédés ont été employés ces dernières décennies, de la pointeuse de fiches en passant par le badge magnétique pour aujourd'hui aboutir à un badge biométrique. La CNIL autorise l'emploi de pointeuses biométriques, dès lors que la technologie employée comme, par exemple, le contour de la main, est conforme à l'autorisation unique AU-007[239]. L'emploi de l'empreinte digitale comme moyen de « pointer » les horaires des salariés est donc interdit, même si le stockage est opéré sur un support individuel. L'histoire de l'anthropologie en France[240] n'est pas sans lien avec cette réticence sans doute plus d'ordre éthique que sécuritaire (1-2).

[239] Cf. Annexe 6.
[240] Supra n° 7 et s.

1-2 Le contrôle des horaires biométrique sur support individuel évincé par l'éthique

189. En matière de gestion des horaires de travail, la CNIL est assez réservée quant à l'usage des empreintes digitales, même si elles sont stockées sur un support individuel qui assure à l'individu la maîtrise intégrale de ses données personnelles (a). Le jugement du tribunal de grande instance de Paris a été la première décision de justice à confirmer cette orientation et a interdit ce dispositif pour la finalité de contrôle des horaires (b). La CNIL n'est toutefois pas restée dans cette ligne jurisprudentielle puisque la délibération rendue pour la société Brisach laisse en suspend le devenir de cette technologie pour la finalité de gestion des horaires (c).

a. Le principe du support individuel

190. Dès l'année 2000, la CNIL a refusé à certaines collectivités locales, l'autorisation d'employer des systèmes de reconnaissance par empreinte digitale avec, pour finalité, le contrôle des horaires des salariés[241]. Une mairie du département de l'Hérault souhaitait gérer le temps de présence de ses salariés afin de limiter les fraudes et assurer une bonne gestion du service. La CNIL a refusé de donner son autorisation, car le stockage de ces données était envisagé dans une base centralisée. Il en a été de même pour la mairie de Goussainville[242] ou, plus récemment, dans le secteur privé, pour les sociétés SARL Brochage 3000[243], TAM Airlines[244] ou Famer Industrie Maintenance[245].

[241] CNIL, Délibération n° 00-057 du 16 nov. 2000 portant avis sur un projet d'arrêté présenté par le préfet de l'Hérault concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion du temps de travail des agents de la préfecture, disponible sur le site internet www.cnil.fr

[242] CNIL, Délibération n° 2006-005 du 23 avr. 2002 relative à la demande d'avis présentée par la mairie de Goussainville concernant la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion des horaires de travail des personnels communaux, disponible sur le site www.cnil.fr

[243] CNIL, Délibération n° 2008-058 du 6 mars 2008 refusant la mise en œuvre par la SARL Brochage 3000 d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des horaires, autorisation n° 1192992, disponible sur le site www.cnil.fr

[244] CNIL, Délibération n° 2008-395 du 6 nov. 2008 refusant la mise en œuvre par la société TAM Airlines d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des horaires, autorisation n° 1281379, disponible sur le site www.cnil.fr

[245] CNIL, Délibération n° 2009-025 du 29 janv. 2009 refusant la mise en œuvre par la société Famer Industrie Maintenance d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux et le contrôle des horaires, autorisation n° 1290116, disponible sur le site www.cnil.fr

191. Dans son 22ème rapport de l'année 2001 au chapitre 3, la CNIL précisait que « *1- Les technologies de reconnaissance biométrique ne reposant pas sur le stockage des gabarits dans une base de données* ***ne soulèvent pas de difficulté particulière en termes informatique et libertés, dès lors que le gabarit est conservé sur soi (carte à puce) ou sur un appareil dont on a l'usage exclusif (un téléphone portable, un ordinateur, etc.) et nulle part ailleurs****.*

2- En revanche, lorsqu'une base de données est constituée dans le cadre d'un dispositif d'identification biométrique, l'élément biométrique retenu peut avoir une incidence sur nos libertés et notre vie privée ; tel est le cas lorsque l'élément biométrique retenu laisse des traces dans notre vie quotidienne (ADN, empreintes digitales). Dans un tel cas le contrôle de finalité et de proportionnalité peut conduire à accepter la mise en œuvre de telles bases de données lorsqu'un impératif particulier de sécurité le justifie.

3- A défaut d'une telle justification particulière, et lorsqu'une base de données de gabarits est constituée, le choix d'un élément biométrique « ne laissant pas de traces, tel que le contour de la main, la rétine, la reconnaissance vocale, etc. devrait être préféré à la prolifération de fichiers ADN ou d'empreintes digitales[246] ».

192. Le stockage individuel ne pose pas de difficultés « informatique et libertés », dans la mesure où la donnée biométrique est uniquement conservée sur la carte à puce, sans qu'il existe de copie du gabarit. Seules, les bases de données d'empreintes digitales sont risquées car elles ne garantissent pas encore suffisamment de protection. Pour l'instant, les outils cryptographiques ne sont pas assez performants pour éviter les détournements de données.

La position de la CNIL est pertinente, dans la mesure où cette cohérence d'ensemble est conservée. Ceci n'est pas toujours le cas lorsqu'il s'agit d'apprécier la finalité de gestion des horaires puisque, même en l'absence de risque de détournement des données personnelles, elle persiste à refuser l'emploi de l'empreinte digitale.

[246] CNIL, 22ème rapport d'activité 2001, Doc. Fr. juill. 2002, p. 171, disponible sur le site internet www.ladocumentationfrancaise.fr

193. En 2005, le tribunal de grande instance de Paris a dû apprécier la pertinence de l'emploi d'un dispositif de reconnaissance par empreintes digitales aux fins de contrôle des horaires. Il s'agit du premier jugement concernant l'utilisation de la biométrie dans le secteur privé (b).

b. Le jugement du TGI de Paris

194. Quelques années après la communication de la CNIL, le tribunal de grande instance de Paris, en date du 19 avril 2005[247], s'est prononcé, pour la première fois, sur l'emploi d'un dispositif de reconnaissance par empreintes digitales ayant pour finalité la gestion des horaires[248]. La CNIL ne s'était pas prononcée sur le traitement, car avant 2004, elle n'avait pas le pouvoir de le faire. Par ailleurs, à cette date, elle n'avait pas encore délibéré sur la mise en place des autorisations uniques d'implantation de dispositifs biométriques.

195. L'inspection du travail avait relevé, lors d'un contrôle effectué dans l'enceinte de la société, la mauvaise tenue des feuilles d'émargement du personnel pour le contrôle obligatoire du temps de travail[249] par un système d'enregistrement automatique. La société Effia services, filiale de la SNCF, décide alors d'utiliser l'empreinte partielle stockée sur une carte individuelle, afin de contrôler « *la gestion des horaires et des temps de présence et la ventilation analytique des activités dans les centres de coûts.* » Cependant, le comité d'entreprise et le syndicat Sud Rail assignent la société devant le TGI de Paris.

Ce dispositif a été annulé par le jugement. Les arguments avancés par les juges, inspirés de la « doctrine de la CNIL », se sont portés dans un premier temps, sur le fondement de l'ancien article L. 120-1[250] du Code du travail avancé par le syndicat, disposant que « *nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions* ***qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché*** *».*

[247] Cf. Annexe 10
[248] TGI Paris, 19 avril 2005, disponible sur le site internet de legalis au www.legalis.net
[249] C. trav. art. L. 3171-4 al. 3 : « *Si le décompte des heures de travail accomplies par chaque salarié est assuré par un système d'enregistrement automatique, celui-ci doit être fiable et infalsifiable* ».
[250] C. trav. actuel art. L. 1121-1

Les magistrats ont estimé que ce procédé apportait aux salariés des restrictions à leurs libertés, manifestement injustifiées, car le procédé identifie les individus par leur empreinte. Le défaut de proportionnalité du dispositif a été soulevé. Néanmoins, cette décision fera l'objet d'un développement plus exhaustif sur ce sujet au sein du chapitre sur la proportionnalité[251].

196. La finalité du traitement des données biométriques a été brièvement évoquée dans cette affaire, mais de façon subjective. Cette finalité biométrique est considérée comme l'objectif indispensable lorsque d'autres techniques se sont révélées insuffisantes. Or, cette appréciation doit être objective, et en rapport avec les informations fournies par l'entreprise, c'est-à-dire, les éléments de faits et autres pièces versées au dossier comme une expertise d'un prestataire de dispositifs biométriques. Cette finalité doit réunir plusieurs conditions (déterminée, explicite et légitime), énoncées par l'article 6 de la loi Informatique et libertés, pour que le traitement soit considéré comme licite.

La finalité est déterminée dès l'instant où elle est circonscrite à un objectif précis, en l'espèce la gestion des fiches de paie et le contrôle des horaires des salariés. Elle est explicite dès lors qu'elle est énoncée clairement dans la déclaration de traitement auprès de la CNIL et qu'elle a fait l'objet de la même clarté au moment de l'information donnée aux salariés. Enfin, elle est légitime lorsqu'elle est « *établie par la loi, conforme à la règle*[252] ». C'est ce dernier point qui a fait débat.

La CNIL ne s'est pas prononcée sur cette déclaration. Elle n'en avait pas le pouvoir avant 2004. La légitimité a été appréciée souverainement par les juges du fond.

Si nous nous basons sur le 22ème rapport d'activité de la CNIL, précédemment cité, le traitement est légitime, dans la mesure où l'empreinte est stockée sur un support individualisé, par conséquent ce traitement aurait pu paraître légitime. Dans ce cas particulier, le tribunal a estimé que « *l'objectif poursuivi n'est pas de nature à justifier la constitution d'une base de données d'empreintes digitales…* ».

[251] Infra n° 295 et s.
[252] G. Cornu, Vocabulaire Juridique, PUF, p. 518

Or, l'objectif de la société Effia n'était pas de constituer une base de données, mais d'utiliser une solution efficace qui, de surcroît, permettait de se conformer aux exigences de l'inspection du travail. La société n'enregistrait que partiellement l'empreinte et uniquement dans une carte à puce détenue exclusivement par le salarié. Les données biométriques ne pouvaient pas être détournées. Il n'y avait donc pas de constitution de base de données. La finalité du traitement était l'utilisation d'un dispositif « *justifié par la nature de la tâche à accomplir* », en l'occurrence, la gestion des horaires de travail. Comme cette tâche ne pouvait être accomplie efficacement par le biais d'un système traditionnel, il convenait d'employer un programme de vérification[253] plus efficace, lequel programme ne contrevenait, ni à la vie privée, ni à la liberté d'aller et de venir des personnes qui s'y soumettaient.

Dans ce cas particulier, il s'agissait de vérifier l'identité du salarié, c'est à dire, de l'authentifier et non de l'identifier. La finalité avait été, au préalable, déterminée par l'emploi d'un dispositif de reconnaissance par empreintes digitales et assez explicite quant aux résultats attendus, c'est-à-dire « *la gestion des horaires et des temps de présence et la ventilation analytique des activités dans les centres de coûts* ». Donc, seule, la légitimité pouvait être sujette à débat.

Nous pensons que le débat sur la finalité a été détourné sur le plan éthique car en fait, la question importante était de juger, pour l'entreprise Effia services, le bien fondé de l'emploi de ce matériel biométrique, au regard de son projet de gestion des ressources humaines, en tenant compte de l'état des technologies à la date de la déclaration du dispositif. L'appréciation de l'éthique, « ce qui concerne la morale », est subjective.

A l'inverse, l'estimation de la finalité doit être objective, compte tenu des éléments de faits fournis par l'entreprise et des garanties qu'elle entraîne, notamment au sujet de l'information et du consentement des personnes. Il est préférable qu'une entreprise emploie ce type de dispositif biométrique, en admettant l'instaurer pour des finalités de gestion des horaires plutôt qu'elle ne l'emploie pour de fausses finalités sécuritaires ou même qu'elle ne conserve abusivement les historiques de passage des salariés afin de contrôler les temps de présence.

[253] Il est indispensable de bien distinguer la vérification (authentification) de l'identification biométrique. Dans ce cas, il s'agissait de vérifier l'identité du salarié, puisqu'il détient seul son empreinte partielle dans sa carte.

Les droits et libertés des salariés ne seraient pas mieux garantis si un dispositif, autre que biométrique, était envisagé. Les magistrats n'ont, en définitive, pas apprécié la finalité ou la proportionnalité du traitement et ont préféré, par réticence à cette nouvelle technologie, rejeter ce traitement, qui, pourtant, se conformait aux dispositions de la loi Informatique et libertés. C'est à ce propos que le professeur Frayssinet relève très justement que « *ce qui importe c'est l'organisation technique et juridique du traitement-système biométrique mis en place qui peut avoir des finalités variées, y compris positives pour les employés, dans un environnement pas forcément menacé, respecte la légalité pour ne pas précisément aboutir à une atteinte aux libertés des salariés*[254] ».

197. Postérieurement à cette décision en rapport avec les dispositifs de reconnaissance biométriques, la CNIL a établi plusieurs autorisations uniques ainsi que des délibérations, qui démontrent qu'elle n'a pas complètement suivi la position des magistrats (c).

c. L'autorisation postérieure accordée à la société Brisach

198. C'est ce que démontre la décision de la CNIL à propos de la société Brisach. La société Brisach a effectué une demande d'autorisation auprès de la CNIL, afin d'implanter un dispositif biométrique qui vise « *à renforcer l'identification des employés de cette société au moment des pointages et lors de l'accès aux locaux.* ***Le dispositif doit ainsi garantir qu'une tierce personne ne pourra se substituer au titulaire légitime du badge lors du contrôle des horaires.*** *Il permettra d'enregistrer les dates et heures d'entrée et de sortie des employés pour la gestion de leur temps de travail. Les traitements permettront de renforcer la sécurité des biens et des personnes, ainsi que des données traitées par la société Brisach s'agissant du contrôle d'accès à la salle informatique*[255] ». Quelques mois après le jugement rendu par le TGI de Paris, la CNIL a donné son autorisation, permettant l'usage de l'empreinte digitale avec stockage de données sur support individuel, dont la finalité est la

[254] J. Frayssinet, « La loi Informatique, fichiers et libertés cuvée 2004 et le droit du travail : constantes et nouveautés », Actes des journées prud'homales d'Aix-en-Provence, Centre de droit social, PUAM, 2005.
[255] CNIL, Délibération n° 2006-069 du 16 mars 2006 portant autorisation de la mise en œuvre par la société Brisach SAS d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalités le contrôle des horaires et le contrôle de l'accès aux locaux, disponible sur le site www.cnil.fr

gestion des horaires de travail. Cette position semble s'affranchir de la décision des magistrats.

199. Rappelons que la finalité doit être, selon l'article 6 de la loi 78-17 du 6 janvier 1978 « *déterminée, explicite et légitime* ». La finalité est déterminée et explicite lorsque le but de la collecte est défini de manière précise. Il s'agit, ici, du contrôle d'accès à la salle informatique qui est un lieu bien délimité. Quant à la gestion du temps de travail des salariés, le responsable de traitement doit se cantonner à ce seul et unique traitement. La finalité est-elle légitime ? La CNIL a été confrontée à la même interrogation que le tribunal de grande instance de Paris pour la société Effia services.

La légitimité repose sur des bases essentiellement d'ordre juridique. Le responsable de traitement doit concilier les intérêts légitimes de l'entreprise avec la protection des droits et libertés des salariés. Notre société actuelle permet de contrôler juridiquement le temps de travail des salariés dans le respect de leurs libertés individuelles. Dans le cadre de son pouvoir règlementaire, l'employeur peut mettre en place un dispositif de gestion des horaires, dans la mesure où ce dispositif ne vise pas à « espionner » ses salariés. Si les données personnelles sont exclusivement détenues par le salarié, le risque de divulgation des données est minime, voire inexistant. Il est donc permis de considérer cette finalité comme légitime puisqu'elle respecte non seulement le droit, mais au-delà, le salarié, qu'elle conforte dans ses droits. Les caractères qui permettent d'apprécier la finalité d'un traitement sont alors réunis.

La décision de la Commission, qui semblait être une avancée dans le développement de « sa doctrine », n'a cependant pas fait l'objet d'une autorisation unique. La CNIL, nous semble-t-il, n'a pas souhaité « officialiser » sa position concernant la finalité de la gestion biométrique des horaires de travail par système de reconnaissance d'empreintes digitales stockées sur un support individuel. Les autorisations uniques, accordées un mois plus tard en sont peut être la démonstration.

Le 27 avril 2006, la CNIL a publié une série de délibérations au sujet des autorisations uniques de traitement des données biométriques[256]. L'une d'entre elles, l'autorisation unique

[256] Supra n° 169 et s.

AU-008, vise le traitement des données personnelles par empreintes digitales[257]. Elle est accordée pour le stockage des données biométriques sur support individuel, mais seulement pour la finalité du contrôle d'accès aux locaux, sur le lieu de travail[258]. Elle exclut donc, par là même, toute finalité de gestion des horaires par ce type de procédé. La CNIL entend réserver l'emploi de l'empreinte digitale pour des finalités sécuritaires, ce qui est sans doute regrettable puisque cette technologie permet un contrôle efficace des horaires, tout en garantissant la protection des données personnelles des salariés.

200. Dans ce cas particulier, il apparaît clairement que la finalité principale invoquée par la société Brisach, était d'empêcher les fraudes à l'identité liées aux badges, en les remplaçant par un contrôle utilisant l'empreinte digitale. Pourtant, le contrôle d'accès à la salle informatique de l'entreprise, dans le but de renforcer la sécurité des biens et des personnes n'est évoqué qu'au second plan. Cette autorisation est la seule en la matière, qui permette à un organisme de traiter les données biométriques issues des empreintes digitales pour une finalité de gestion des horaires. Devant cette décision, surprenante, nous pensons que l'autorisation a été accordée à la société Brisach, parce que la demande touchait deux finalités, et non une seule, portant uniquement sur la gestion des horaires[259].

Nous nous interrogeons sur les raisons qui animent le refus catégorique du stockage des empreintes digitales sur un support individuel pour la finalité de gestion des horaires. La CNIL a pour mission essentielle de veiller à ce que l'informatique soit au service du citoyen et que son développement ne portent pas atteinte « *à l'identité humaine, aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*[260] ».

En l'absence de risque de détournement, lorsque l'entreprise garantit la sécurité des données par un stockage individuel dont seul, le propriétaire a la détention, nous pensons que rien n'empêche l'emploi d'un système de reconnaissance par empreinte digitale pour la gestion des horaires de travail. Rappelons qu'en authentification, le gabarit biométrique n'est pas stocké au sein d'une base de données. Il est nécessaire d'associer la technologie biométrique à une autre donnée de référence, par exemple un numéro.

---

[257] Cf. Annexe 7
[258] Infra n° 202 et s.
[259] Nous ne pouvons donner que des hypothèses, car nous avons été dans l'impossibilité d'obtenir le rapport de séance de cette délibération auprès de la CNIL.
[260] Art. 1er de la loi Informatique et libertés modifiée.

Lorsqu'une entité souhaite avoir recours à une technique de reconnaissance par empreinte digitale, avec stockage sur une base de données utilisant la méthode de l'identification, elle doit justifier son choix par l'existence d'un fort impératif de sécurité, ce qui paraît normal au regard des dangers que comporte ce mode de stockage. Or, en matière d'authentification avec une finalité de contrôle d'accès, les entreprises n'ont pas à prouver un fort impératif de sécurité mais simplement un besoin général de sécurisation, qui se justifie plutôt facilement[261].

Cette position de la CNIL peut conduire les entreprises à avancer de fausses finalités sécuritaires pour obtenir les autorisations demandées ? C'est ce qui apparaît en premier lieu, car en plus de la « sécurité » déclarée, elles obtiennent aussi, un contrôle biométrique des horaires de travail des salariés. Les entreprises disposent aujourd'hui de salles informatiques dont elles veulent protéger le matériel et les informations consignées. Pour leur protection, la CNIL propose l'emploi d'autres technologies comme la reconnaissance du contour de la main qui, par ailleurs, s'avère peu performante, ou bien la reconnaissance du réseau veineux des doigts, mais pour celle-ci, l'installation du matériel est plus coûteuse que la mise en place d'un dispositif de reconnaissance par empreintes digitales en authentification. Aucune de ces deux solutions n'est totalement satisfaisante.

201. Dans une économie mondialisée, les entreprises sont en compétition permanente pour protéger leurs locaux, leur savoir, leurs biens et leurs installations. La biométrie est perçue comme un moyen efficace de sécuriser le patrimoine de l'entreprise. La finalité de gestion des contrôles d'accès est régulièrement avancée (2°).

[261] Infra n° 227.

2°. La finalité de gestion du contrôle d'accès

202. Le marché du contrôle d'accès, comme nous l'avons étudié précédemment, est l'un des piliers de l'utilisation de la biométrie. Il vise à contrôler les personnes, entrant ou sortant dans une zone sécurisée. Ce contrôle d'accès intéresse, bien sûr, les particuliers, pour la sécurisation de leurs biens personnels mais surtout les entreprises, pour la sécurisation de leur patrimoine (droits réels, personnels ou intellectuels).

203. Pour cette finalité, les applications biométriques sont diverses. Le contrôle d'accès peut être d'ordre physique, lorsqu'il s'agit d'accéder à un bâtiment ou à une salle d'accès restreint. Il peut, aussi, être d'ordre logique, lorsqu'il convient d'accéder à un poste informatique en particulier, un serveur partagé ou une clé USB, faisant office de disque dur externe. Il s'agit de l'alliance entre la sécurité des données biométriques et un stockage, gage de liberté pour le salarié (2-1). Cette finalité, plébiscitée par les entreprises est en pleine expansion (2-2).

2-1. Une finalité de contrôle d'accès associée à un processus sécurisé

204. Pour qu'une technique biométrique fonctionne, il est nécessaire qu'elle soit acceptée par les individus qui sont appelés à s'y soumettre. La biométrie est de mieux en mieux acceptée par la population car elle touche les différentes sphères de la vie de l'individu (privée ou professionnelle), ou celle du citoyen avec le passeport biométrique. Parmi toutes les techniques biométriques d'identification existantes, c'est l'emploi de l'empreinte digitale qui est préféré car c'est une technique à la fois fiable et connue des individus.
En phase d'authentification et pour la seule finalité du contrôle d'accès, la CNIL n'est pas défavorable à l'emploi d'une technique de reconnaissance par empreintes digitales, mais seulement dans le cas où le gabarit de celle-ci est enregistré sur un support individuel et conservé par la personne qui aura ainsi une entière liberté pour utiliser ses données personnelles. En revanche, le propriétaire, détenteur de ce support est entièrement responsable de la perte ou du vol de ses propres données biométriques.

Pour ce type de technologie, il faut se conformer à l'autorisation AU-008 de la CNIL[262]. Il y est bien précisé que la finalité du traitement par empreinte digitale, ne concerne que le contrôle de l'accès aux locaux sur le lieu de travail, ce qui, exclut du champ d'autorisation, tout dispositif visant la gestion des horaires de travail et la restauration en entreprise. Le traitement envisagé doit se conformer à quelques caractéristiques techniques : « *seul le gabarit de l'empreinte digitale, clé biométrique résultat du traitement des mesures par un algorithme, est enregistré sur le support individuel et non une image ou une photographie de l'empreinte digitale ;*

on entend par support individuel tout support de stockage ***dont la personne concernée a un contrôle exclusif,*** *tel qu'une carte à puce ou magnétique ;*

le gabarit de l'empreinte digitale de la personne concernée est exclusivement enregistré sur un support individuel détenu par elle seule et dont le contenu ne peut être lu à son insu ;

lors de l'enrôlement, un enregistrement temporaire du gabarit de l'empreinte digitale peut être effectué sur le poste informatique servant à l'enrôlement pour les stricts besoins de son inscription dans la mémoire du support individuel et sous réserve qu'il soit effacé à l'issue de cette phase qui ne saurait excéder quelques secondes ;

le contrôle d'accès s'effectue par une comparaison entre le doigt apposé sur le lecteur et le gabarit de l'empreinte digitale enregistré sur le support individuel ***sans qu'aucune copie de ce gabarit, même temporaire****, ne soit effectuée ;*

à l'exclusion des gabarits des empreintes digitales, certaines données nécessaires à l'identification de la personne et à la réalisation des contrôles relatifs à la validité du badge peuvent être enregistrées dans un serveur dédié au contrôle des accès. »

Ces caractéristiques techniques tendent à garantir la sécurité des données lors des différentes étapes du traitement de l'empreinte digitale. La CNIL rappelle que le contrôle d'accès en authentification s'effectue par la comparaison entre le doigt du salarié apposé sur le lecteur et

[262] CNIL, Délibération n° 2006-102 du 27 avr. 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale, exclusivement enregistrée sur un support individuel, détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail, disponible sur le site www.cnil.fr

le gabarit contenu dans le support individuel. Concrètement, l'individu pose son empreinte sur le lecteur mais détient son gabarit dans sa clé USB. Le support par clé USB est sa propriété, ce qui signifie qu'il a la maîtrise de ses données personnelles.

En ce qui concerne le côté technique, il faut distinguer ce dispositif de l'enrôlement du gabarit pour constituer une base de données correspondant alors à une identification biométrique. En cas de perte ou de vol, cette clé ne pourrait être utilisée par le fraudeur pour plusieurs raisons.

D'abord parce que le leurre de l'empreinte digitale du propriétaire est extrêmement difficile à mettre en œuvre[263], cela nécessite d'avoir une excellente capture de l'empreinte permettant une reproduction à l'identique. Pour cet exercice, le fraudeur doit posséder un matériel relativement sophistiqué.

Ensuite, le seul gabarit enregistré sur le support individuel ne permet pas de remonter à son propriétaire. La raison est d'ordre technique. Chaque logiciel crypte le gabarit d'une façon différente et par sécurité, il ne conserve pas l'image initiale de l'empreinte digitale. Pour obtenir ce même gabarit, le fraudeur doit nécessairement disposer d'une machine et d'un programme de cryptage identiques sans garantie de succès.

Enfin, cette hypothèse, redoutée par la Commission, ne tient pas compte de l'existence actuelle de capteurs nommés « *liveness detection* » qui détectent de faux doigts. De nouveaux dispositifs biométriques, intègrent cette technologie encore coûteuse, qui mesure la vascularisation des doigts. En conséquence, un fraudeur, muni d'un faux gabarit ou même, à l'extrême, du doigt coupé du détenteur de l'accès, ne pourrait faire fonctionner le système, en l'absence de l'afflux sanguin.

205. La finalité de contrôle d'accès est plébiscitée par les entreprises. Cette expansion s'explique d'une part par la simplification de la procédure et d'autre part par la faculté d'intégrer au contrôle d'accès, un logiciel de gestion de la restauration ou des ressources humaines (2-2).

[263] J.-F., Mainguet, « Fake detection », Encyclopedia of Biometrics in Fingerprint, pp. 458

2-2. La finalité du contrôle d'accès en expansion

206. Dès l'année 2005, la CNIL a constaté un accroissement des demandes des entreprises, désireuses d'employer l'empreinte digitale comme outil visant à garantir la sécurité des locaux[264]. Dans une délibération n° 2005-001 du 13 janvier 2005, antérieure à l'autorisation préalable AU-008, la société TF1 a été autorisée à mettre en œuvre un traitement automatisé de données à caractère personnel, dont la finalité est la gestion des contrôles d'accès par badge. La gestion de contrôle d'accès à ses locaux les plus sensibles a nécessité la mise en place d'un accès restreint. Pour se faire, le système de reconnaissance biométrique par empreintes digitales a été choisi. Ce traitement avait pour finalité accessoire, l'accès simplifié au restaurant d'entreprise, ainsi que le paiement des consommations.

La CNIL a donné son avis favorable, dans la mesure où les données biométriques étaient stockées dans un support individuel, détenu par la personne concernée, qui en a, seule, la responsabilité. Les normes de sécurité en matière de chiffrement des données étaient respectées, la CNIL peut donc accepter l'emploi d'un système de reconnaissance par empreintes digitales. De nombreuses délibérations dans ce domaine ont été prises. Le contrôle d'accès suit la vogue de « l'identification gadget », de telle sorte que cette technique touche plusieurs autres domaines notamment la gestion de la restauration d'entreprise, la gestion des ressources humaines et bientôt la gestion des stocks.

207. Tout comme le secteur industriel, le secteur bancaire est un secteur sensible et compétitif, pour lequel il est nécessaire d'avoir recours à des techniques de sécurité, à la fois sophistiquées et rapides. Dans une délibération n° 97-0044 du 10 juin 1997, la Banque de France a procédé à une demande d'avis auprès de la CNIL, concernant la gestion des contrôles d'accès des agents, des zones sécurisées aux zones classées hautement sécurisées. C'est la première demande d'avis, dans le secteur bancaire, qui touche à la fois, à la sécurité et au contrôle d'accès.
Le traitement était mis en œuvre dans un sas de passage à unicité d'enrôlement dans lequel l'empreinte était enregistrée, associée à un code personnel. On a constaté que le dispositif technique ne permettait pas de procéder à l'impression des empreintes enregistrées. La CNIL

[264] CNIL, Rapport d'activité 2006, Doc. Fr. juin 2007, p.13 et s, disponible sur le site www.ladocumentationfrancaise.fr

a souligné qu'il n'était pas possible, avec ce système, d'identifier l'individu et a ainsi donné un avis favorable à cette finalité qui a pour but la sécurisation des zones sensibles.

Depuis lors, dans le domaine bancaire, cette pratique tend à se développer et à s'étendre non plus seulement au contrôle d'accès physique que représentent les accès à des bâtiments, et aux salles réservées à un personnel restreint, mais aussi au contrôle d'accès logique c'est-à-dire au poste de travail. La délibération n° 2006-136 du 9 mai 2006 en est la preuve.
La banque Finama a mis en place un système de reconnaissance par empreintes digitales dont la finalité est le contrôle d'accès logique au poste de travail. Ce système permet de « *remplacer le système d'identification actuel reposant sur la saisie d'un mot de passe et d'un identifiant par un dispositif de reconnaissance de l'empreinte digitale associé à une carte à puce personnelle. Un tel dispositif a pour avantage essentiel de remédier aux difficultés inhérentes à la gestion des mots de passe et à leur confidentialité.* »

208. Cette technologie ne fait pas toujours l'unanimité des salariés, même en matière d'authentification où les risques de falsification sont moindres voire inexistants. Préférée par les entreprises, du fait de son accessibilité et de son faible coût, la technique de reconnaissance biométrique par empreintes digitales reste dangereuse pour la Commission, du seul fait de sa traçabilité et ne doit pas être implantée par facilité. Néanmoins, les entreprises n'éprouvent plus de difficultés à justifier la licéité du traitement par des finalités sécuritaires.

Nous craignons que la justification du contrôle d'accès ne se résolve en une finalité de « complaisance », qu'il devient indispensable d'invoquer, pour avoir une chance d'obtenir de la Commission, l'autorisation d'implanter un système de reconnaissance par empreintes digitales. Au-delà des objectifs pour lesquels la biométrie est sollicitée, la finalité doit permettre d'établir l'existence ou non « *d'un détournement d'usage* »[265]. Il ne faut pas qu'elle soit détournée de son objectif initial, de même que le contrôle d'accès ne doit pas conduire à la surveillance des salariés.

209. La technologie de reconnaissance par empreintes digitales est pour l'heure cantonnée essentiellement au contrôle d'accès. En revanche, les autres dispositifs

[265] Expression empruntée à l'OCDE dans un rapport intitulé « Technologies fondées sur la biométrie », Groupe de travail sur la sécurité de l'information et de la vie privée, Direction de la science, de la technologie et de l'industrie. Comité de la politique d'information, de l'informatique et des communications, 10 juin 2005, p. 7.

biométriques sont autorisés par la CNIL sans grande difficulté, dans la mesure où ils garantissent la sécurité des données (B).

B. L'appréciation de la finalité au regard des autres techniques de reconnaissance biométrique

210. Devant la multiplication des demandes d'autorisation de traitement des données personnelles, la CNIL a établi des autorisations uniques dans différents domaines : marketing, déplacement, assurance, banque, etc. Ces autorisations uniques visent une même finalité, des catégories de données et de destinataires identiques. Ainsi, les organismes qui possèdent un traitement conforme à l'une de ces autorisations, peuvent faire cette déclaration de conformité[266].

211. La CNIL reçoit de plus en plus de demandes d'autorisation pour l'utilisation de systèmes biométriques, correspondant à une multitude de techniques. C'est pourquoi elle a élaboré des autorisations uniques à partir desquelles il est possible de réfléchir sur le contrôle de finalité des dispositifs de reconnaissance du contour de la main (1°), du réseau veineux des doigts de la main (2°) ainsi que les autres dispositifs qui tendent à se développer (3°).

1°. Au regard de la technique de la reconnaissance du contour de la main

212. La technique de reconnaissance du contour de la main, nommée aussi géométrie de la main, est l'une des techniques les plus répandues car elle est réputée sans traces et son seuil d'acceptabilité par les individus est plutôt bon. Les dispositifs de reconnaissance du contour de la main peuvent être indifféremment employés, pour des finalités de contrôle d'accès, de gestion des horaires ou de gestion de la restauration (1-1) dans la mesure où ils concernent les seuls salariés de l'entreprise, ce qui exclut, sauf autorisation, les clients de cette dernière (1-2).

[266] Supra n° 169 et s.

1-1. Les finalités de contrôle d'accès, de gestion des horaires et de la restauration sur le lieu de travail

213. Tout employeur désirant installer un procédé biométrique de reconnaissance du contour de la main doit faire une déclaration de conformité qui respecte les dispositions de la délibération n° 2006-101 du 27 avril 2006, portant autorisation unique AU-007[267]. Ce dispositif relève de l'article 25-8° de la loi de 2004.

Cette autorisation unique énonce limitativement, dans son article 1er intitulé « *Finalités et Caractéristiques techniques du traitement* », les finalités pour lesquelles le traitement de données biométriques par géométrie de la main peut intervenir.
Il s'agit du :
« - *contrôle des accès à l'entrée et dans les locaux limitativement identifiés de l'organisme faisant l'objet d'une restriction de circulation ;*

- *La gestion des horaires et des temps de présence ;*

- *le contrôle de l'accès au restaurant d'entreprise ou administratif et la gestion de la restauration ainsi que la mise en place d'un système de paiement associé ;*

- *le contrôle d'accès des visiteurs.* »

Le dispositif employé est un dispositif dit « sans traces ». La CNIL est donc plus encline à élargir les finalités du traitement. Toutefois, les caractéristiques techniques n'en sont pas pour autant amoindries puisque :
« *aucune photographie de la main des personnes concernées n'est conservée ;*

les éléments pris en compte reposent exclusivement sur la géométrie de la main ;

[267] CNIL, Délibération n° 2006-101 27 avr. 2006 de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail, Cf. Annexe 6

seul le gabarit du contour de la main, résultat du traitement des mesures par un algorithme, est enregistré dans une base de données où il peut être associé à un numéro d'authentification de la personne ;

lorsque la finalité poursuivie est le contrôle des horaires des employés, le dispositif de reconnaissance du contour de la main peut être interconnecté avec une application de gestion des horaires et des temps de présence ;

lorsque la finalité poursuivie est le contrôle de l'accès au restaurant d'entreprise ou administratif, le dispositif de reconnaissance du contour de la main peut être interconnecté avec une application de gestion de la restauration ainsi qu'avec un système de paiement associé. »

214. Seule, l'image de la géométrie de la main doit être capturée et tout comme l'empreinte digitale, elle ne doit pas être gardée. Le gabarit informatique uniquement, peut être conservé. Le risque de détournement d'une donnée est accru lorsque le responsable du traitement sauvegarde l'image initiale à partir de laquelle est issu le gabarit informatique. Procéder à l'effacement de cette image, dès que la capture a été faite, limite considérablement les risques de détournement des données.

La technologie de reconnaissance de la géométrie de la main n'est pas réputée « à traces », pourtant, un programme informatique pirate peut dérober l'image initiale si cette dernière est maintenue dans une base de données. Cependant, si, à partir d'une image, un fraudeur peut générer un gabarit informatique, il lui est parfaitement impossible, à partir du gabarit, de reconstituer l'image initiale. Le stockage est autorisé au sein d'une base de données, car en authentification, pour reconnaître le salarié, il est nécessaire d'associer un code en plus de la donnée biométrique.
Par ailleurs, la délibération prévoit que la base de données peut être interconnectée[268] avec d'autres applications. Cependant les interconnexions sont ciblées par chaque domaine

[268] L'interconnexion constitue « *la liaison physique et logique des réseaux de communications publics utilisés par la même entreprise ou une entreprise différente, afin de permettre aux utilisateurs d'une entreprise de communiquer avec les utilisateurs de la même entreprise ou d'une autre, ou bien d'accéder aux services fournis par une autre entreprise. Les services peuvent être fournis par les parties concernées ou par d'autres parties qui ont accès au réseau. L'interconnexion constitue un type particulier d'accès mis en œuvre entre opérateurs de*

d'activités. La CNIL a précisé des interconnexions différentes, pour le contrôle d'accès et pour la gestion des horaires des salariés. Il s'agit là d'une manière de ne pas étendre, de façon illimitée, les « passerelles » entre les données.

La finalité est toujours appréciée par la CNIL au regard du concept de traçabilité, même si les techniques employées ne laissent pas de traces visibles. La traçabilité peut être informatique et pas simplement physique comme l'empreinte digitale laissée sur un verre par exemple. En l'absence de traces, les techniques biométriques sont admissibles, qui plus est lorsque le stockage de ces données se fait sur un support individuel détenu exclusivement par la personne. Au Québec, cette technologie est employée dans les salles de sport aux fins d'authentification des abonnés. C'est aussi le cas en France pour le Centre de culture physique d'Aquitaine[269], qui utilise un traitement de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité le contrôle d'accès à la salle de sport.

215. En entreprise, l'usage d'un système de reconnaissance du contour de la main pose bien moins de difficultés que l'empreinte digitale. C'est pourquoi la CNIL a sans doute voulu officialiser cette technologie en simplifiant la procédure d'autorisation.

Les systèmes de reconnaissance du contour de la main ont vocation à s'étendre tant leurs atouts « informatique et libertés » sont nombreux. Toutefois, les performances de ces systèmes sont moins bonnes que les systèmes de reconnaissance par empreinte digitale, les taux d'erreurs sont plus élevés, ce qui peut être un frein à son utilisation en matière de contrôle d'accès. La multiplication des taux d'erreur apporte de grandes difficultés aux responsables de traitement mais aussi aux responsables de la sécurité des systèmes informatiques. Le temps d'attente s'allonge si un problème d'authentification survient dans la journée, lors du pointage des horaires ou de l'accès à la salle informatique.

---

réseaux publics. » Art. 2 de la Directive n° 2002/19/CE du 7 mars 2002 relative à l'accès au réseau de télécommunication électronique ainsi qu'à leur interconnexion (directive dite « Accès »).

[269] CNIL, Délibération n° 2009-311 du 7 mai 2009 autorisant la mise en œuvre par le Centre de culture physique d'Aquitaine d'un traitement de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité la gestion de l'accès à la salle de sport, autorisation n°1309515, disponible sur le site www.cnil.fr

216. En entreprise, ce dispositif ne peut être utilisé que dans la limite de l'autorisation unique. Pour toute autre utilisation, comme son usage sur les clients de l'entreprise, il est nécessaire d'obtenir une nouvelle autorisation préalable de traitement (1-2).

1-2. La finalité de contrôle d'accès des clients de l'entreprise

217. L'autorisation unique AU-007 ne vise pas le contrôle d'accès des clients. Il est nécessaire de procéder à une demande d'autorisation préalable selon les articles 25 et 64 de la loi n° 78-17 du 6 janvier 1978 modifiée. Aucune déclaration de conformité ne peut être établie pour ce type de traitement de données personnelles. Il s'agit, dans ce cas, de contrôler l'accès à des personnes étrangères qui n'appartiennent pas à l'entreprise, d'où la nécessité de les protéger plus strictement. Comme le chef d'entreprise ne peut se prévaloir de son pouvoir règlementaire pour imposer ce dispositif d'authentification à des clients, il doit procéder à une demande d'autorisation préalable. Même si ce sont des relations d'affaires, il ne peut leur imposer les mêmes conditions d'authentification qu'à ses salariés. En pratique, nous n'avons pas encore relevé de demande d'autorisation préalable mais nous pourrions imaginer qu'une entreprise procède à une demande d'autorisation de cette façon, pour cette finalité dès lors, par exemple, qu'il existe un fort impératif de sécurité à identifier et non plus authentifier les clients.

218. Un autre dispositif s'étend, en parallèle des systèmes de reconnaissance du contour de la main : celui de la reconnaissance du réseau veineux des doigts de la main, développé par la société Hitachi et dont les finalités sont vastes (2°)

2°. Au regard de la technique de reconnaissance du réseau veineux des doigts de la main

219. Depuis la fin de l'année 2007 et l'autorisation donnée à la société Hitachi de traiter des données biométriques par le système de reconnaissance du réseau veineux des doigts de la main[270], la CNIL a constaté une multiplication des demandes tendant à mettre en place ce type de dispositif[271].

Le réseau veineux des doigts de la main est unique pour chaque individu. Il s'attache à reconnaître une personne, par l'entrelacement des vaisseaux sanguins des doigts de la main. Ce dispositif a pour avantage de ne pas laisser de traces, puisque les vaisseaux sanguins sont dissimulés sous la peau. Après expertise, la CNIL a estimé, qu'en l'état des connaissances actuelles, ce dispositif présentait les mêmes garanties d'identification que l'empreinte digitale, sans les risques de détournement existants. L'inconvénient reste le coût d'installation de ce procédé et le manque de recul sur cette technologie.

La société Hitachi, précurseur dans le domaine, souhaitait mettre en place en 2007 ce dispositif biométrique, en vue de sécuriser plusieurs sites répartis sur le territoire français.

Le dispositif a pour finalité la sécurisation des accès, sur différents sites en France, au cours d'opérations de maintenance et de résolution de problèmes techniques. Le dispositif fonctionne en authentification, c'est-à-dire qu'aucune base de données biométriques n'est constituée et qu'il est nécessaire pour le salarié d'utiliser en complément un numéro identifiant.

La CNIL s'est prononcée favorablement à l'égard de cette technologie qu'elle considère, en l'état actuel de la technique, comme une biométrie sans trace « *dont l'enregistrement sur un serveur aux fins de contrôler les accès à un système d'information ne comporte pas de risques particuliers pour les libertés et les droits fondamentaux des personnes. A cet égard, en l'état*

[270] CNIL, Délibération n° 2007-339 du 8 nov. 2007 autorisant la mise en œuvre par la société Hitachi Data Systems d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès au système d'information, autorisation n° 1248197, disponible sur le site www.cnil.fr

[271] CNIL, De nouvelles technologies expertisées, article du 14 janv. 2008, disponible sur le site internet de la CNIL

actuel des techniques, la biométrie par reconnaissance du réseau veineux n'est pas susceptible d'être capturée à l'insu des personnes[272] ».

220. Devant le succès de cette technologie biométrique, réputée sans traces, près de deux ans plus tard, la Commission a trouvé opportun de lui dédier une autorisation unique, lui conférant ainsi une reconnaissance « officielle[273] ».
La finalité de cette technologie est, pour l'heure, réduite au contrôle d'accès. Néanmoins, son seuil de dangerosité est réputé faible, car au regard des connaissances actuelles, il paraît impossible de falsifier ce type de données. Nous ne serions pas surpris que certaines applications basées sur cette technologie, soient employées pour une finalité d'organisation ou de gestion de l'entreprise. Il apparaît, au fil des délibérations, que le principe de finalité permet de déterminer la pertinence de l'emploi de la biométrie. Ensuite, la traçabilité va intervenir dans l'appréciation du principe de proportionnalité, elle est encore et toujours la clé de voûte déterminant l'avenir, prometteur ou non, d'une nouvelle technologie biométrique.

En effet, si la technique est dite « sans traces » c'est qu'elle minimise les risques de détournement des données personnelles. Les finalités pour lesquelles le dispositif est sollicité seront donc étendues au contrôle d'accès, à la gestion des horaires et de la restauration.
Les constructeurs de dispositifs biométriques ont trouvé, dans cette technologie sans traces, une des solutions « informatique et libertés » permettant l'usage efficace de la biométrie tout en respectant les données personnelles des individus. Cette technologie est-elle toutefois dénuée de risques ? A l'heure actuelle et compte tenu des connaissances acquises en la matière il ne semble pas y avoir de risque de détournement des données personnelles, mais elle a un coût financier non négligeable pour les entreprises qui désirent l'implanter.

221. D'autres techniques biométriques existent, mais elles n'ont pas eu un franc succès au sein des entreprises. Si elles ont l'avantage de ne pas laisser de traces, elles ne sont pas forcément acceptées par les salariés ou sont coûteuses à mettre en œuvre, elles doivent néanmoins être citées (3°).

---

[272] Voir la délibération précitée.
[273] CNIL, Délibération n° 2009-316 du 7 mai 2009 portant autorisation unique n°AU-019 de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle d'accès aux locaux sur les lieux de travail, JO n° 0142 du 21 juin 2009
De l'année 2007 à l'année 2009 cette technologie a totalisé près de quatre-vingt-dix délibérations de la CNIL sur le site internet Legifrance.

3°. Au regard des autres techniques

222. Nous faisons entrer dans cette catégorie, les dispositifs biométriques de reconnaissance faciale, de l'iris ou de la voix, ainsi que d'autres techniques en cours de développement, dont la fiabilité n'est pas assurée. Pour l'heure, en France, ces techniques ne sont employées que pour la recherche ou à des fins policières.
Aucune autorisation unique ne peut être effectuée, faute de recul sur ces technologies. Toutefois, ce propos doit être tempéré, car le développement croissant d'une technique face à une autre, dépend avant tout de la culture d'un pays.

Ainsi, en Allemagne, l'iris est préféré à l'empreinte digitale. En Angleterre ou aux Etats-Unis, la reconnaissance faciale est pratiquée plus couramment, quelquefois au détriment des individus. C'est le cas de la vidéosurveillance, associée à un système de reconnaissance faciale.[274] Ces considérations sont faites en tenant compte du développement technologique et du recul vis-à-vis de ces techniques, au moment des déclarations de conformité.
En authentification, les risques resteront tout de même moindres qu'en identification. La finalité sera appréciée, à nouveau, en fonction des bénéfices envisagés et des risques encourus pour les libertés.

223. En 2007, la CNIL a eu l'occasion, pour la première fois, d'examiner, pour la société Michelin[275], un système de reconnaissance vocale qui avait pour objet de sécuriser et de faciliter la gestion et la réinitialisation automatique des mots de passe. Ce système a été favorablement accueilli par la CNIL, même s'il convenait d'enregistrer et de conserver une base de données d'empreintes vocales. Ce système sera plus développé ci-dessous, dans ce qui concerne les finalités d'identification et la constitution de bases de données biométriques (sous section 2).

[274] C. Cabal, Rapport de l'Office parlementaire d'évaluation des choix scientifiques et technologiques, Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre, 1ère partie, 16 juin 2003, p. 13.
[275] CNIL, Délibération n° 2007-248 du 13 sept. 2007 autorisant la mise en œuvre par la Manufacture française des pneumatiques Michelin d'un traitement automatisé de données à caractère personnel reposant sur un procédé de reconnaissance vocale et ayant pour finalité la gestion des mots de passe, disponible sur le site www.cnil.fr

Sous Section 2. La finalité d'identification biométrique avec constitution de bases de données

224. Depuis les attentats terroristes du 11 septembre 2001 et sous l'impulsion des Etats-Unis d'Amérique, l'Union européenne s'est engagée à établir, avec les passeports des citoyens, une base de données biométriques[276]. La collecte massive de données est considérée comme le moyen le plus fiable de garantir l'identification des personnes. Par ailleurs, l'existence d'une base centralisée minimise les coûts de production d'un support (badge). L'identification biométrique, accompagnée de la constitution d'une base de données est donc une association rentable qui a vocation à s'étendre dans d'autres domaines que la simple identification policière.

Fortes de ce constat, les entreprises tentent d'intégrer des dispositifs biométriques dans leur architecture de sécurité. La biométrie est devenue une des solutions « *pour gérer les incertitudes de la modernité contemporaine*[277] ». Elle fait partie des technologies que l'on croit « d'anticipation des menaces » mais qui, dans les faits, n'est pas prouvée. Personne ne peut prétendre que les attentats du 11 septembre 2001 aux Etats-Unis auraient été évités grâce à l'emploi de la biométrie dans les aéroports. La mise en réseau des données constitue un risque moderne d'un nouveau genre que la biométrie ne peut régler.

L'identification biométrique permet, en pratique, de comparer une donnée à une multitude d'autres données précédemment enrôlées. Cette identification ne peut se faire qu'à partir d'une base de données biométriques. Cette dernière peut intervenir de deux manières :

- soit les données stockées dans la base, sont reliées à un réseau (les données ne sont pas anonymes, dans ce cas le risque de détournement est plus grand puisqu'un réseau ouvert offre plus de possibilités de piratage informatique.
- soit les données stockées dans la base ne sont pas rattachées à un réseau, elles sont alors appelées bases anonymes de données. Les échanges de données s'effectuent par transit sur des supports physiques, sans accès au réseau. Ce

[276] La base de données est définie 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 par tout autre moyen.* » Loi n° 98-6536, 1er juil. 1998, CPI. art. 112-3 al. 2, JO 2 juillet 1998, p. 10075.

[277] A. Ceyhan, « La biométrie : une technologie pour gérer les incertitudes de la modernité contemporaine. Applications américaines », in Pierre Piazza (dir.), Police et identification. Enjeux, pratiques, techniques, Les Cahiers de l'INHES, n° 56, premier semestre 2005.

sont ces dernières qui garantissent le mieux la protection des données personnelles.

Cela signifie qu'en matière d'identification, une personne déjà enregistrée dans une base, est en mesure de comparer sa donnée biométrique à l'ensemble de la base. Selon les finalités de celle-ci, la capacité des éléments contenus sera plus ou moins importante. Ainsi, pour une base de données constituée pour une finalité de contrôle d'accès, la taille de cette dernière est au maximum de mille empreintes. En revanche, pour des applications policières, elle peut contenir des millions de données.

225. Dans les deux cas, il est nécessaire d'obtenir l'autorisation préalable de la CNIL et de justifier sa demande d'un fort impératif de sécurité dès lors qu'il est envisagé un dispositif reposant sur la reconnaissance de l'empreinte digitale (A). Dans le cas des autres techniques qui ne laissent pas de traces, il est nécessaire de motiver la finalité de traitement consistant à avancer un besoin général de sécurisation (B).

A. La constitution de bases de données d'empreintes digitales

226. Les réticences concernant la biométrie sont liées à la collecte massive des éléments du corps humain au sein d'une base de données centralisée alors que les outils cryptographiques servant à préserver la sécurité de ces bases ne sont pas fiables à 100%. Plusieurs auteurs se sont érigés contre ces technologies de la peur et de la surveillance permanente[278].

Lorsqu'il s'agit d'un organisme public ou privé (exception faite des traitements pour le compte de l'Etat)[279], la constitution de bases de données d'empreintes digitales ou d'autres données biométriques est soumise, en France, à l'autorisation préalable de la CNIL. Ces

[278] D. Duclos, « Ces industries florissantes de la peur permanente », Le Monde diplomatique, Août 2005, p. 16 et 17
A. Weber, J.-R. Lecerf, « Faut-il avoir peur de la biométrie ? », L'Express, 5 sept. 2005, p. 2-3
G. Agamben, « Non à la biométrie », Le Monde, 6 déc. 2005, p. 25

[279] L'Etat français dispose de règles qui lui sont propres en matière de biométrie. La loi n° 78-17 du 6 janvier 1978 modifiée distingue les traitements biométriques pour le compte de l'Etat (articles 26 et 27) des autres traitements biométriques (article 25).

autorisations sont émises en matière d'identification, au cas par cas et font l'objet d'une étude précise de la finalité pour laquelle la base de données est constituée.

227. La CNIL a rappelé, que la constitution d'une base de données biométriques ne doit pas être anodine et doit correspondre à un fort impératif sécuritaire. « *Confier ses données biométriques à un tiers, lui permettre de les enregistrer et de les conserver* ***n'est donc jamais un acte anodin*** *: cela doit répondre à* ***une nécessité a priori exceptionnelle, justifiée*** *et être* ***entourée de garanties sérieuses***[280] ».

C'est pourquoi, à de nombreuses reprises, la Commission a refusé la constitution de bases de données biométriques, pour l'accès aux cantines des collèges[281] ou pour la surveillance du temps de travail des salariés[282]. Le contrôle d'accès répond le plus souvent, à un « *besoin général de sécurisation* ». Ce terme, souvent employé par la CNIL lors de ses délibérations[283], se distingue du « *fort impératif de sécurité*[284] », dans la mesure où il répond à un besoin quotidien courant de sécurisation. Il est utilisé par la CNIL, notamment pour refuser les autorisations visant à implanter des dispositifs de reconnaissance par empreintes digitales qui ne seraient pas justifiées par cet impératif de sécurité.

Nous proposons comme définition du besoin général de sécurisation, la réelle nécessité pour une entreprise, d'avoir recours à des dispositifs biométriques qui lui permettent de pérenniser son droit de propriété, tout en sécurisant ses biens[285], ses informations et installations dans un intérêt purement personnel et ne pouvant avoir de conséquences sur la société civile.

---

[280] CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, 27 nov. 2007, site internet www.cnil.fr

[281] CNIL, « La CNIL dit non aux empreintes digitales pour la biométrie dans les écoles », Fiches pratiques, 25 septembre 2008, disponible sur le site internet au www.cnil.fr

[282] Voir notamment la délibération n° 2006-005 du 12 janvier 2006 portant refus d'autorisation de la mise en œuvre par la clinique de Goussonville d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle des horaires des employés, disponible au www.legifrance.gouv.fr

[283] CNIL, Délibération n° 2008-233 du 17 juil. 2008 refusant la mise en œuvre par la société Histoire et patrimoine d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des accès aux locaux, autorisation n°1296677, disponible sur le site www.legifrance.gouv.fr

CNIL, Délibération n° 2009-024 du 29 janv. 2009 refusant la mise en œuvre par la société Rexel France Ouest d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, autorisation n°1291947, disponible sur le site au www.legifrance.gouv.fr

[284] Infra n° 229.

[285] Biens au sens large comprenant les biens matériels comme immatériels d'une entreprise.

De ce fait, le fort impératif de sécurité est, à l'inverse, un impératif qui vise à protéger « l'intérêt public », entendu comme l'intérêt de la société civile, qui doit dépasser le strict intérêt de l'entreprise. Le défaut de protection de ces entreprises à fort « risque » potentiel aurait des répercussions sur la société prise dans son ensemble.

228. A titre d'exemple, dans une délibération n° 00-057 du 16 novembre 2000, la préfecture du département de l'Hérault a saisi la CNIL, afin de mettre en œuvre un traitement automatisé de données nominatives, destiné à permettre l'authentification des agents territoriaux et de gérer le temps de travail avec un système de reconnaissance par empreintes digitales. Ce traitement aboutissait à la constitution d'une base de données biométriques avec le stockage d'empreintes digitales. La préfecture faisait valoir comme finalité que « *le badge d'accès, dont l'utilisation permet de conserver la trace des heures d'entrées et de sorties du personnel afin de calculer le temps de travail des agents territoriaux soumis à des horaires variables, ne doit pas pouvoir être utilisé frauduleusement par un agent territorial souhaitant dissimuler l'absence ou le retard d'un de ses collègues. C'est la raison pour laquelle la Préfecture souhaite, grâce à un dispositif de reconnaissance des empreintes digitales associé à l'utilisation des badges d'accès, éviter toute utilisation d'un badge par une personne autre que son titulaire*[286] ». Pour ce faire, la préfecture souhaitait constituer une base de données biométriques centralisée. La CNIL a estimé qu'une telle finalité était incompatible et disproportionnée avec la création d'une base de données centralisée.

229. Le contrôle de la finalité en matière d'identification biométrique est bien plus contraignant et doit « *être limitée* ***au contrôle de l'accès d'un nombre limité de personnes*** *à* ***une zone bien déterminée*** *représentant ou contenant* ***un enjeu majeur dépassant l'intérêt strict de l'organisme*** ***et*** *ayant trait à la* ***protection de l'intégrité physique des personnes*** *ou* ***à celle des biens*** *et* ***des installations*** *ou à* ***celles de certaines informations***[287] ». La finalité sécuritaire dépend d'un enjeu majeur. Le seuil de dangerosité d'un site (bâtiments nucléaires ou de la défense nationale) implique de protéger l'accès à certaines zones, en réduisant l'entrée aux seules personnes compétentes pour agir en cas de sinistre.

[286] CNIL, Délibération n° 00-057 du 16 nov. 2000 portant avis sur un projet d'arrêté présenté par le préfet de l'Hérault concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion du temps de travail des agents de la préfecture, disponible sur le site internet www.cnil.fr

[287] CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, 27 nov. 2007, site internet www.cnil.fr

L'enjeu majeur va consister à éviter la survenance d'un péril qui ferait courir un risque pour les personnes, les biens, les installations, ou les informations. Il doit être déterminé de façon stricte de sorte à ne pas élargir son application à d'autres finalités que celle de sécuriser. La CNIL précise que cet enjeu majeur « *doit dépasser l'intérêt strict de l'organisme* ». Il vise la protection de l'intégrité physique des personnes (1°), la protection des biens et des installations (2°), la protection de certaines informations (3°) et les missions de recherche scientifique (4°).

1°. L'enjeu majeur de la protection de l'intégrité physique des personnes

230. Tout être humain a un droit intangible à la protection de l'intégrité physique de son corps. Il s'agit d'une garantie fondamentale des droits de l'Homme, énoncée par différentes normes tant nationales qu'internationales[288], « *au-dessus de tout prix et n'admet nul équivalent, n'ayant pas une valeur relative, mais une valeur absolue*[289] ». En France, la protection de l'intégrité physique des personnes est un principe à valeur constitutionnelle[290].
Ainsi, respecter la dignité humaine revient à appliquer la maxime d'Emmanuel Kant : « *Agis de façon telle que tu traites l'humanité, aussi bien dans ta personne que dans la personne de tout autre, toujours en même temps comme fin, jamais simplement comme moyen*[291] ».

231. De plus en plus d'entreprises optent, dans le cadre du contrôle d'accès à leurs locaux, pour des systèmes biométriques aux fins d'identification de leurs salariés.
Un procédé d'identification biométrique ne peut être autorisé que dans la mesure où la finalité est exclusivement liée au contrôle d'accès, ce qui élimine explicitement la restauration et la gestion des horaires. Ainsi, l'intérêt pour lequel ce dispositif est mis en place, est supérieur aux intérêts propres à l'entreprise.

Certaines entreprises exercent une activité dangereuse telle que le traitement de déchets radioactifs ou le traitement d'échantillons biologiques, c'est pourquoi il est nécessaire « *de*

[288] Art. 1er de la Déclaration universelle des droits de l'Homme, articles 16 et 16-1 du code civil français, article 3 de la CEDH etc.
[289] T. de Koninck, « De la dignité humaine », Essai, PUF, Quadrige, 2002
[290] Ce concept a eu une reconnaissance officielle par la décision du Conseil constitutionnel du 27 juillet 1994 : D. 1995. 237, note Mathieu.
[291] I. Kant, « Fondements de la métaphysique des mœurs », éd. LGF, 1993, traduction de Victor Delbos.

protéger des installations comportant un risque élevé d'explosion ou de diffusion de matières dangereuses ou de détournement de celles-ci par des tiers non autorisés ;
Assurer la protection des personnes exposées à des risques particuliers en raison de leurs activités[292] ».

En pratique, pour ces entreprises particulières, la CNIL a autorisé différents traitements biométriques, qui consistent à l'enregistrement des empreintes digitales avec stockage dans un lecteur-comparaison ou sur un serveur. La liste qui suit n'est pas exhaustive mais relate des cas où l'intégrité physique des personnes pourrait être mise en cause.

- Bâtiments de stockage de plutonium de la COGEMA à La Hague[293].
- Zones de fabrication de principes actifs pour l'industrie pharmaceutique[294].
- Contrôle d'accès à une zone d'appontement pétrolier et gazier relié à deux sites classés « SEVESO II » [295].
- Contrôle d'accès à une zone de traitement de produits dangereux[296].

232. La CNIL, dans la délibération n° 2006-158 précitée, avait autorisé l'entreprise à collecter et traiter les données biométriques sur un support individuel. Cependant, l'entreprise était soumise à des obligations légales de sécurité et selon ses dires, elle était dans l'impossibilité de les satisfaire avec le précédent mode de stockage des données. C'est pourquoi elle a souhaité en changer au profit d'une base de données biométriques. La raison invoquée réside dans le fait que « *Le dispositif reposant sur l'utilisation d'une carte à puce s'est avéré inadapté aux contraintes liées au fait que le site dont elle souhaite contrôler les*

[292] CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, 27 nov. 2007, site internet www.cnil.fr
[293] En 2000, les entreprises n'étaient pas soumises à déclaration, il n'y a donc pas de références de déclaration mais simplement un récépissé de déclaration du 17 novembre 2000.
[294] CNIL, Délibération n° 2006-158 du 30 mai 2006 portant autorisation de la mise en œuvre par la société La Mesta Chimie Fine SAS d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, disponible au www.cnil.fr
[295] CNIL, Délibération n° 2007-056 du 21 mars 2007 autorisant la mise en œuvre par le port autonome de Bordeaux d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès à un appontement pétrolier et gazier, disponible sur le site www.cnil.fr
[296] CNIL, Délibération n° 2007-051 du 21 mars 2007 autorisant la mise en œuvre par Millenium Chemicals Thann SAS d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles, disponible sur le site au www.cnil.fr

accès relève de la réglementation sur les installations classées pour la protection de l'environnement (ICPE) soumis à une autorisation d'exploiter préfectorale.
S'agissant d'un site classé de type "SEVESO seuil bas" dans lequel sont stockés simultanément des produits dangereux, la société La Mesta Chimie Fine SAS a obligation de mettre en œuvre un Plan d'Opération Interne (POI) dans lequel sont définis les mesures d'organisation et les moyens à mobiliser pour protéger le personnel, la population et l'environnement en cas d'accident. A ce titre, la société La Mesta Chimie Fine SAS doit être en mesure de fournir, en cas d'exercice d'évacuation ou d'accident, la liste exacte des personnes présentes sur le site.
Or, le recours à un support individuel de stockage des empreintes digitales ne permet pas de savoir quelles sont les personnes présentes sur les lieux en cas d'oubli, de perte, de vol ou d'endommagement des cartes. Dès lors, afin d'assurer le suivi exhaustif des personnes accédant au site et de garantir la fiabilité de l'historique de leurs passages, la modification du dispositif apparaît nécessaire[297] ».

233. Le contrôle de la finalité d'identification avec constitution d'une base de données biométriques ne s'établit pas uniquement sur les caractères énoncés à l'article 6 de la loi Informatique et libertés[298] mais tient compte du risque lié à l'activité de l'entreprise et de son impact sur l'intégrité physique des personnes. La finalité doit être appréciée au regard des éléments objectifs présentés par l'entreprise, c'est-à-dire l'environnement dans lequel l'entreprise évolue ou les obligations légales en matière de sécurité auxquelles elles doivent se conformer. La finalité était déterminée, explicite et légitime en ce que l'entreprise a des obligations légales de sécurité qui ne sont pas incompatibles avec la création d'une base de données.

Au sujet des données enregistrées, elles ne sont pas excessives, il s'agit des : nom, prénom, gabarit biométrique et historique de passage de l'employé. Les données relatives à l'historique de passage sont conservées durant un mois. Les autres données personnelles seront conservées pendant toute la durée du contrat de travail. Par ailleurs, le salarié a la faculté de consulter, en

[297] CNIL, Délibération n° 2006-071 du 16 mars 2006 portant autorisation de la mise en œuvre par la société La Mesta Chimie Fine SAS d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, disponible sur le site www.cnil.fr
[298] « *Les données sont collectées pour des finalités déterminées, explicites et légitimes.* »

ligne, son dossier ainsi que son historique de passage, après saisie d'un mot de passe et d'un nom d'utilisateur. Les personnes habilitées à accéder aux données sont au nombre de deux.

Les mesures prises semblent raisonnables et conformes au minimum de données à collecter pour le bon fonctionnement d'une base de données personnelles.
Le mode de stockage est un serveur interne, dénué de communication avec l'extérieur, ce qui permet de minimiser les risques d'intrusion et de vol des données personnelles.

234. Malgré les impératifs de préservation de l'intégrité physique, il est nécessaire de rappeler que dans ces cas précis, la collecte des données personnelles dans une carte à puce serait envisageable et permettrait, tout aussi efficacement, d'atteindre le même objectif sans passer par une collecte massive des données personnelles. Simplement, il en va d'une question d'efficacité en cas d'accidents ou d'attentats terroristes. Il est nécessaire de pouvoir réagir rapidement et efficacement sur les lieux. Les personnes dont la présence est sollicitée peuvent avoir oublié ou perdu leur badge. C'est pour éviter ces contraintes techniques que les bases de données centralisées sont mises en place.

Dans ce cas de figure, la biométrie détient sa fonction première, de technologie au service de l'homme et non une technologie qui l'asservit. Elle a pour réelle fonction de protéger les produits chimiques contenus dans le bâtiment et par là même l'intégrité physique de la société civile dans son ensemble, s'il s'agit de bâtiments nucléaires[299].

235. Une difficulté subsiste : en ce qui concerne l'enjeu majeur, aucun cadre précis n'a été défini. Malgré la définition que l'on peut en donner sur l'état de dangerosité, son périmètre n'est pas déterminé. Faut-il élargir la notion d'enjeu majeur, afin d'y intégrer toutes les entreprises classées (ICPE, SEVESO etc.), même si leur seuil de risque est bas, comme pour la société Mesta Chimie ? Ou bien faut-il encore restreindre l'accès aux seuls bâtiments reconnus comme réellement dangereux, de par les produits qu'ils contiennent, soit qu'ils les fabriquent, soit qu'ils les stockent ?
Une classification doit être effectuée, de façon à ce que les bases de données d'empreintes digitales ne se propagent pas. Dans la procédure d'autorisation préalable, il y a un effet

[299] Il s'agit ici d'une « Privacy Enhancing Technology » (P.E.T), une technologie protectrice de la vie privée.

« pervers » non négligeable : les autorisations sont données au cas par cas, sans une réelle vue d'ensemble.

La constitution d'une base de données biométriques s'apprécie en fonction de la nécessité de préserver l'intégrité de la personne. Collecter massivement des données personnelles, pour le Comité consultatif national d'éthique (CCNE), contrevient au respect de la dignité humaine[300].

Cette difficulté ne touche pas uniquement la France. Au Canada, pour la mise en œuvre d'un dispositif biométrique, les entreprises peuvent avancer la balance des intérêts entre la protection de la vie privée et la nécessité, pour l'employeur, de préserver les besoins de l'entreprise.[301] Ainsi, dans cette affaire, l'employeur a pu implanter un dispositif de reconnaissance vocale permettant de réinitialiser les mots de passe des postes informatiques. Le syndicat des salariés n'a pas obtenu gain de cause[302].

236. Une base de données biométriques peut aussi être constituée, dès lors qu'une entreprise fait valoir un enjeu majeur à protéger ses biens et installations (2).

2°. L'enjeu majeur de la protection des biens et des installations

237. Selon la communication de la CNIL du 27 novembre 2007, les hypothèses justifiant la constitution d'une base de données, peuvent aussi viser les dommages de grande ampleur et irréversibles, qui risquent d'être portés aux biens et installations d'un organisme ou d'une collectivité. L'opportunité de la constitution d'une base de données biométriques doit être envisagée dans la mesure où « *le fonctionnement de services essentiels à la collectivité peut être menacé par l'intrusion de personnes non autorisées dans telle ou telle*

[300] CCNE, Avis consultatif n° 260/98 Biométrie, données identifiantes et droits de l'Homme, 19 mars 2008, disponible sur le site internet http://www.ccne-ethique.fr/
[301] Privacy Commissioner of Canada, PIPEDA Case Summary 281, disponible sur le site au: http://www.privcom.gc.ca/cfdc/2004/cf-dc_040903_e.asp
[302] Affaire anonymisée, PIPEDE Case summary 281, issue de l'article de Gary T. Clarke « Biometrics in the workplace – Where to draw the line?" Personal Information Protection Act Conference 2006, April 26 and 27, Calgary, Alberta (Canada), p. 9.

partie d'un organisme[303] ». Les exemples donnés par la Commission visent notamment le contrôle d'accès :

« *- à certaines zones d'une entreprise travaillant pour la Défense nationale ;*

- au centre de contrôle et de sécurité d'une grande entreprise de messageries ;

- aux zones sensibles d'un centre départemental d'incendie et de secours[304] *;*

- aux zones sensibles d'une imprimerie fiduciaire soumise à des règles de sécurité nationales et internationales[305] ».

238. Ainsi, dans une délibération n° 2006-070 du 16 mars 2006, la société Sagem Défense Sécurité a été autorisée, en vue d'un contrôle d'accès plus fiable à ses locaux, à implanter un système de reconnaissance des empreintes digitales avec constitution d'une base de données biométriques[306]. La finalité invoquée est le contrôle d'accès à des zones sensibles contenant des informations ou des biens classés « secret défense », il s'agit de protéger les biens matériels ou immatériels des dommages irréversibles que ces zones pourraient subir ou des conséquences qu'occasionnerait leur disparition pour la Nation. La protection de ces biens est, par conséquent, supérieure à la préservation du droit de propriété de l'entreprise. Mais nous nous interrogeons sur la portée et les conséquences de cette classification.

Le procédé de classification « secret défense » vise les procédés, les objets, les documents, les informations, les réseaux informatiques ou données et fichiers informatisés intéressant la Défense nationale. Il a pour objectif de protéger les éléments qui peuvent nuire ou conduire à la découverte d'un secret de la Défense nationale s'ils tombaient entre de mauvaises mains[307]. On peut se demander quelle influence une telle classification pourrait avoir sur les décisions de la CNIL. Cette dernière n'a aucun regard sur cette classification décidée en Conseil d'Etat

[303] CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, 27 nov. 2007, p. 8, disponible sur le site internet www.cnil.fr

[304] CNIL, Délibération n° 2009-026 du 29 janv. 2009 autorisant la mise en œuvre par le Service Départemental d'Incendie et de Secours de l'Isère (SDIS) d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, autorisation n° 1303760, disponible sur le site www.legifrance.gouv.fr

[305] CNIL, Délibération n° 2007-050 du 21 mars 2007 autorisant la mise en œuvre par François Charles Oberthur Fiduciaire d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles, disponible sur le site www.legifrance.gouv.fr

[306] CNIL, Délibération n° 2006-070 du 16 mars 2006 portant autorisation de la mise en œuvre par la société Sagem Défense Sécurité d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, disponible sur le site www.legifrance.gouv.fr

[307] C. pen. Art. 413-9 modifié par la loi n° 2009-928 du 29 juil. 2009 (art. 12), JO n° 0175 du 31 juil. 2009, p. 12713.

[308] et ne fait sans doute pas l'objet d'une décision d'habilitation pour consulter le contenu du dossier. En effet, l'article R. 2311-7 du Code de la défense, précise sur ce point que « *Nul n'est qualifié pour connaître des informations ou supports protégés s'il n'a fait au préalable l'objet d'une décision d'habilitation et s'il n'a besoin de les connaître pour l'accomplissement de sa fonction ou de sa mission*[309] ». Mais nous supposons que la CNIL dispose de la preuve de cette dernière, pour juger de la pertinence du mode de stockage, en l'absence de renseignements précis sur les informations classées. Nous postulons en faveur du fait que la seule classification « secret défense » ouvre droit à la possibilité de constituer une base de données biométriques d'empreintes digitales.

239. La constitution d'une base de données biométriques est aussi envisagée dès lors qu'il convient de protéger des informations d'une nature si particulière qu'elle justifie la collecte des empreintes digitales (3°).

[308] La procédure de classification est disposée aux articles L. 2312-1 et suivants du Code de la défense.
[309] Code de la défense Art. R. 2311-7 créé par décret n° 2009-254 du 4 mars 2009.

3°. L'enjeu majeur de la protection des informations

240. Certaines informations, de par leur nature ou leur confidentialité, nécessitent de restreindre efficacement leur accès aux seules personnes habilitées à en avoir connaissance.
Selon la CNIL[310], il s'agit « *des informations ou des données devant faire l'objet d'une protection particulière en raison des conséquences que leur divulgation, leur détournement à d'autres fins ou leur destruction auraient pour les personnes concernées par l'activité de l'entreprise, de l'institution ou de l'organisme.* »
Les exemples donnés par la CNIL sont « *l'accès aux locaux d'une entreprise classée ICPE développant des procédés et matériels sensibles faisant l'objet de restrictions à l'exportation ;*
- à la salle sécurisée contenant des informations de clients de niveau « confidentiel défense » d'une entreprise spécialisée dans les systèmes d'information de grandes entités et dans leurs problématiques de sécurité;
- aux locaux d'un cabinet-conseil en matière de propriété intellectuelle et industrielle, habilité à gérer des dossiers sensibles (confidentiel ou secret défense, etc.)[311] *;*
- au bâtiment d'un service de l'Education nationale contenant les sujets d'examens et concours[312] ».
Cette catégorie de données reste extensive car bon nombre d'entreprises a pour intérêt de conserver un « secret industriel » dans le but de préserver leur compétitivité sur la scène économique internationale, ou un « secret professionnel » qui touche des professions règlementées. Apparaissent à nouveau les informations classées « confidentiel défense[313] » dont la nature des informations n'est peut être pas fournie[314].
Dans ces hypothèses, le critère de finalité, à lui seul, ne permet pas une évaluation objective des avantages prodigués par rapport aux risques encourus. Les finalités sont déterminées,

[310] CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, 27 nov. 2007, p. 8 in fine, site internet www.cnil.fr
[311] CNIL, Délibération n° 2007-054 du 21 mars 2007 autorisant la mise en œuvre par la société Brevalex d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, disponible sur le site www.legifrance.gouv.fr
[312] CNIL, Délibération n°00-056 du 16 novembre 2000 portant avis sur un projet d'arrêté présenté par le ministre de l'Education nationale concernant un traitement automatisé d'informations nominatives ayant pour finalité le contrôle d'accès par la reconnaissance des empreintes digitales de certains personnels de l'Education nationale, pour certains locaux de la cité académique de Lille, disponible sur le site www.legifrance.gouv.fr
[313] En vertu de l'article R. 2311-2 du Code de la défense, la classification comporte trois niveaux, 1° Très secret-défense, 2° Secret-défense 3° Confidentiel-défense.
[314] Supra n° 237 et s.

explicites et légitimes mais dans ces cas, le principe de proportionnalité doit être observé pour s'assurer de la pertinence de tels traitements[315].

En ce qui concerne les locaux de l'Education nationale, d'autres procédés peuvent être utilisés, comme l'a décidé la CNIL, pour le Graduate Management Admission Council (GMAC)[316]. Pour cet examen de renommée internationale, on a demandé à la Commission un recours pour installer un dispositif de reconnaissance du réseau veineux des doigts de la main, dont les éléments sont stockés dans une base de données. Des substituts à l'usage de l'empreinte digitale peuvent donc être trouvés comme par exemple la technologie de reconnaissance du réseau veineux de la main qui, bien que coûteuse, a de bons résultats d'authentification.

241. Les dispositifs biométriques ne peuvent se développer que s'ils font l'objet d'expérimentation. La CNIL a reconnu ces missions de recherche scientifique comme un enjeu majeur qui justifie la constitution d'une base de données (4°).

4°. L'enjeu majeur des missions de recherche scientifique

242. Les autorisations de constitution de base de données visent aussi le cadre de missions de recherche et de développement, dans le domaine de la biométrie et sur une durée déterminée.

Depuis l'année 2007, pas moins de dix initiatives ont été autorisées par la Commission. Ces autorisations concernent entre autres :

- la mise en œuvre par l'université d'Evry-Val d'Essonne d'un traitement automatisé de données à caractère personnel ayant pour finalité principale l'évaluation d'algorithmes de reconnaissance du visage et de l'iris[317].
- la mise en œuvre par le Groupe des Ecoles des Télécommunications (GET) d'un traitement automatisé de données à caractère personnel ayant pour

[315] Infra n° 269.

[316] CNIL, Délibération n° 2009-360 du 18 juin 2009 autorisant la mise en œuvre par le Graduate Management Admission Council (GMAC) représenté par Pearson Education France d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux de la paume de la main et ayant pour finalité de contrôler l'accès à des salles d'examen et d'empêcher la substitution de candidat à l'examen GMAT, demande d'autorisation n°1323460, disponible sur le site www.legifrance.gouv.fr

[317] CNIL, Délibération n° 2007-006 du 18 janv. 2007 autorisant la mise en œuvre par l'université d'Evry-Val d'Essonne d'un traitement automatisé de données à caractère personnel ayant pour finalité principale l'évaluation d'algorithmes de reconnaissance du visage et de l'iris, disponible sur le site www.legifrance.gouv.fr

finalité principale l'évaluation d'algorithmes de reconnaissance de diverses données biométriques[318].

- la mise en œuvre par l'Ecole nationale supérieure d'ingénieurs de Caen (ENSICAEN) d'un traitement de données à caractère personnel ayant pour finalité la création d'une plate-forme de tests biométriques[319].

243. Par exemple, la société Thales Security System a initié un projet nommé Vérification d'identité numérique Sécurisée itinérante (VINSI) dont l'objectif était « *de tester et d'améliorer les processus de capture, de reconnaissance, de comparaison et de visualisation des données biométriques ainsi que de concevoir une plate-forme de vérification d'identité numérique reposant sur un terminal mobile sécurisé capable d'effectuer de la reconnaissance d'empreintes digitales et de visages de personnes*[320] ».

La CNIL a donné son avis favorable à la constitution d'une base de données d'empreintes digitales et de photographies du visage d'employés volontaires de la société. La CNIL précise que « *son autorisation ne porte que sur un programme de recherche et ne saurait être interprétée comme l'acceptation tacite de futures demandes relatives à l'utilisation d'une plate-forme de vérification d'identité numérique reposant sur un terminal mobile ;*
La demande présentée par la société Thales sur la mise en œuvre du dispositif projeté à des fins de recherche ne saurait avoir valeur de labellisation de la technologie présentée ».

La CNIL a déterminé que « *dans la mesure où seules les données biométriques des personnes volontaires seront traitées et ce, dans le seul but de procéder à des travaux de recherche destinés à tester et améliorer les processus de capture, de reconnaissance, de comparaison et de visualisation des données biométriques et à concevoir une plate-forme de vérification*

[318] CNIL, Délibération n° 2007-296 du 4 oct. 2007 autorisant la mise en œuvre par le Groupe des Ecoles des Télécommunications (GET) d'un traitement automatisé de données à caractère personnel ayant pour finalité principale l'évaluation d'algorithmes de reconnaissance de diverses données biométriques, demande d'autorisation n° 1226906, disponible sur le site www.legifrance.gouv.fr
[319] CNIL, Délibération n° 2008-098 du 10 avr. 2008 autorisant la mise en œuvre par l'Ecole nationale supérieure d'ingénieurs de Caen (ENSICAEN) d'un traitement de données à caractère personnel ayant pour finalité la création d'une plate-forme de tests biométriques, autorisation n° 1198593, disponible sur le site internet www.legifrance.gouv.fr
[320] CNIL, Délibération n° 2008-084 du 27 mars 2008 autorisant la mise en œuvre par la société Thales Security Systems d'un traitement automatisé comportant des données biométriques nécessaires au contrôle de l'identité des personnes, autorisation n° 1239796, disponible sur le site internet www.legifrance.fr

d'identité numérique, les traitements soumis à la Commission sont adaptés et proportionnés à la finalité assignée au dispositif au regard de la protection des données personnelles ».

244. La CNIL a pris la même décision à propos d'une demande d'autorisation établie par le Groupe des Ecoles des Télécommunications dont la finalité est l'évaluation d'algorithmes de reconnaissance de diverses données biométriques pour le projet BioSecure. Dans la délibération n° 2007-296 du 4 octobre 2007 la CNIL a autorisé un traitement de données biométriques à des fins de recherche, dans la mesure où les données des volontaires resteraient confidentielles. Techniquement, « *les données biométriques stockées sur ce poste informatique seront indexées par un code identifiant. La correspondance entre l'identité des personnes (nom, prénom et coordonnées) et le code identifiant figurant dans la base de données biométriques s'effectuera grâce à un fichier distinct qui sera sauvegardé sur un CD-ROM et conservé dans un coffre fort sous le contrôle de la personne responsable du projet. Il en ira de même pour les formulaires remplis par les participants à la campagne d'acquisition des données*[321] ».

Lorsqu'il s'agit de missions de recherche, les autorisations sont concédées pour améliorer des technologies existantes ou en tester de nouvelles. Les traitements n'ont pas vocation à perdurer dans le temps. Par ailleurs, les données sont collectées sur des personnes volontaires et pour une durée déterminée. Ainsi, à propos de l'autorisation donnée au Groupe des Ecoles des Télécommunications, la sauvegarde des données s'effectue sur un CD-ROM. Cette précaution garantit une base différente pour les données biométriques et les identifiants. La donnée biométrique à elle seule n'ouvre pas d'accès dans le code identifiant correspondant.

245. Les bases de données constituées dans le cadre de ces missions sont contrôlées et ne servent qu'à améliorer les technologies testées et la sécurité des données enregistrées.

Ces missions de recherche sont fondamentales quant au devenir de la biométrie, mais restent encore confidentielles. Elles permettent d'évaluer, dans une durée raisonnable, les avantages

[321] CNIL, Délibération n° 2007-296 du 4 oct. 2007 autorisant la mise en œuvre par le Groupe des Ecoles des Télécommunications (GET) d'un traitement automatisé de données à caractère personnel ayant pour finalité principale l'évaluation d'algorithmes de reconnaissance de diverses données biométriques, disponible sur le site internet www.legifrance.fr

ou les inconvénients de l'usage de la biométrie, de perfectionner les moyens de sécurité (cryptographie, signature électronique) etc.

Le rapport présenté par Christian Cabal, le 16 juin 2003 proposait déjà à ce sujet comme quatrième recommandation, « *la mise en place d'un organisme associant des partenaires publics et privés et doté des moyens de financement nécessaires pour faire réaliser par des laboratoires indépendants des travaux d'évaluation scientifiques et techniques, recueillir l'avis d'experts ou d'universitaires sur la fiabilité des travaux menés par d'autres organismes et diffuser les résultats des études conduites en son sein*[322] ». Nous sommes favorables à cette recommandation. Il serait judicieux que les entreprises françaises, en association avec d'autres acteurs de différents milieux (universitaire, experts) du secteur public comme privé, développent en commun les techniques biométriques. A ce jour, à notre connaissance, cette recommandation n'a pas été suivie d'effets alors même que la France doit rester compétitive dans le domaine de la recherche face aux Etats-Unis, au Japon et à la Chine déjà bien avancés !

246. Devant les craintes soulevées par la constitution de bases de données d'empreintes digitales, d'autres technologies ont émergé. Ces dernières ont des bases fiables, car les données collectées « ne laissent pas de traces », pour reprendre les termes de la CNIL. (B)

[322] C. Cabal, Rapport de l'Office parlementaire des choix scientifiques et technologiques sur « les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mises en œuvre », Partie 3, p. 13, disponible sur le site de l'Assemblée nationale au lien suivant : http://www.assemblee-nationale.fr/12/rap-off/i0938.asp

B. La constitution de bases de données issues d'autres techniques biométriques

247. Entre 1970 et 1995, plusieurs publications scientifiques ont vu le jour sur les technologies de reconnaissance du visage, dont la plus célèbre, en 1991, démontre l'existence d'un algorithme révolutionnaire, nommé « eigenfaces », qui permet de créer des dispositifs de reconnaissance du visage.[323] Cette découverte a donné une nouvelle impulsion au marché américain de l'identification avec la mise en œuvre, par le ministère de la Défense américain, du programme FERET (Face Recognition Technology).

Parallèlement au développement matériel de cette technologie, les autorités de protection des données personnelles se sont interrogées sur la qualification juridique qu'il fallait donner aux données issues de la voix et de l'image (qui comprend le visage mais aussi les applications numériques qui en découlent comme la vidéosurveillance).

A travers la définition des données à caractère personnel[324], la CNIL a estimé que la voix et l'image d'une personne doivent être considérées comme des données qui permettent d'identifier ou de rendre identifiable un individu car « *si la photographie, de face et/ou de profil, permet déjà d'identifier une personne et de détecter des usurpations d'identité, (c'est le cas de l'utilisation de cartes d'identité perdues ou volées), l'image vidéo ou l'image animée le permettent mieux encore*[325] ».

La reconnaissance de ces données, comme des données à caractère personnel, a permis de les placer sous le régime de la loi Informatique et libertés afin de les protéger et d'en contrôler

---

[323] Notamment les articles suivants: T. Kanade, « Picture processing by computer complex and recognition of human faces », Kyoto University, November, 1973; Turk, M., and Pentland, A., (1991) Eigenfaces for Recognition, Journal of Cognitive Neuroscience, Vol. 3, No. 1, pp. 71-86.

[324] Art. 2 de la Directive 95/46/CE du Parlement européen et du Conseil, 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 n° L 281 du 23 nov. 1995 p. 0031 – 0050. Il s'agit de « *toute information concernant une personne identifiée ou identifiable* » ; le texte poursuit : « *est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale* ».
Art. 2 de la Convention STE 108 du Conseil de l'Europe pour la protection des personnes à l'égard des traitements automatisés des données à caractère personnel, Strasbourg, 28 janv. 1981 « *Aux fins de la présente convention : a) Données à caractère personnel signifie : toute information concernant la personne physique identifiée ou identifiable ...* ».

[325] CNIL, Délibération n° 94-095 du 15 nov. 1994 relative à la proposition modifiée de directive du Conseil de l'Union européenne relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel et à la libre circulation de ces données, disponible sur le site internet www.legifrance.gouv.fr

leur utilisation au sein de bases de données. Les applications biométriques basées sur la reconnaissance faciale sont, pour l'heure, essentiellement employées pour la sécurité aéroportuaire ou la sécurité nationale.
Ce procédé a été évalué en premier lieu à titre expérimental[326], pour être employé désormais par les entreprises, comme moyen de sécuriser l'accès à certaines zones (salles informatiques par exemple) [327]. La constitution d'une base de données d'images issues de ce dispositif n'a pas encore été autorisée par la CNIL, faute de recul nécessaire sur cette technologie. C'est pour cette raison que nous n'avons pas davantage développé ce sujet. En revanche, deux technologies font l'objet d'un réel engouement par les entreprises, il s'agit de la technologie de reconnaissance vocale et celle du réseau veineux des doigts de la main.

248. La CNIL a donné l'autorisation, à certaines entreprises, de constituer des bases de données biométriques d'empreintes vocales, comme ce fut le cas pour la société Michelin, ou du réseau veineux de la paume de la main, pour la GMAC. Ces systèmes que nous venons de citer, sont des techniques dites « sans traces ». En conséquence, ces demandes sont soumises au régime de la déclaration préalable mais ne font pas l'objet de la même méfiance, par la Commission.

Dans son 22ème rapport d'activité, la CNIL précisait que « *s'agissant des dispositifs reposant sur la constitution de bases de données, il paraît très significatif que la Commission* ***ait donné systématiquement des avis favorables ou n'ait pas formulé de réserve lorsque la base de données était constituée de gabarits du contour de la main****, élément biométrique qui,* ***à la différence des empreintes digitales, ne laisse pas de trace complète ou repérable sur les objets qui nous entourent***[328] » Cela signifie, par extension, que si la technologie employée « *ne laisse pas de trace complète ou repérable sur les objets qui nous entourent* » la

[326] Se référer notamment aux délibérations de la CNIL n° 2007-006 du 18 janv. 2007 autorisant la mise en œuvre par l'université d'Evry-Val d'Essonne d'un traitement automatisé de données à caractère personnel ayant pour finalité principale l'évaluation d'algorithmes de reconnaissance du visage et de l'iris. Disponible sur le site internet de Légifrance au www.legifrance.fr
CNIL, Délibération n° 2007-296 du 4 oct. 2007 autorisant la mise en œuvre par le Groupe des Ecoles des Télécommunications (GET) d'un traitement automatisé de données à caractère personnel ayant pour finalité principale l'évaluation d'algorithmes de reconnaissance de diverses données biométriques. Disponible sur le site internet de Légifrance au www.legifrance.fr
[327] CNIL, délibération n° 2009-314 du 7 mai 2009 autorisant la mise en œuvre par la société Novadis d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des visages et ayant pour finalité le contrôle de l'accès aux locaux. Disponible sur le site internet de Légifrance au www.legifrance.fr
[328] CNIL, Extrait du 22ème rapport d'activité 2001, Chapitre 3, p. 170, disponible sur le site internet de la documentation française au http://www.ladocumentationfrancaise.fr/ ou sur le site internet de la CNIL au www.cnil.fr

constitution d'une base de données biométriques n'est pas conditionnée au fort impératif de sécurité. Les entreprises font valoir plutôt « *un besoin général de sécurisation*[329] » en vertu duquel l'entreprise doit garantir la sécurité de ses locaux, biens et informations en restreignant l'accès à certaines zones de l'entreprise, pour ses propres intérêts.

249. Nous nous interrogeons toutefois, sur les risques liés à la constitution de ces bases de données. Les exemples de la société Michelin (1°) à propos de la voix et du GMAC (2°) à propos du réseau veineux des doigts de la main sont intéressants sur ces questions.

1°. La technique de reconnaissance de la voix

250. La voix émane de l'être humain, elle contribue, sans machine, à identifier des personnes qui nous sont familières. Le dispositif biométrique de reconnaissance de la voix consiste à distinguer une personne et à l'identifier à l'aide de sa voix. Néanmoins, la voix est mouvante, peut changer en cas de maladie, de vieillesse. Ce dispositif n'est donc pas particulièrement fiable même en l'absence de traces.

La société Michelin a fait une demande d'autorisation de traitement de données à caractère personnel, reposant sur un procédé de reconnaissance vocale. La délibération du 13 septembre 2007 a autorisé cette société à constituer une base de données d'empreintes vocales. Le dispositif a pour finalité « *de sécuriser et de faciliter la gestion et la réinitialisation des mots de passe utilisés pour accéder au système d'information de la société Michelin. Il s'agit de mettre à la disposition des employés un dispositif permettant de générer et de réinitialiser automatiquement les mots de passe*[330] ».

Du point de vue technique, lors de l'enrôlement, l'employé enregistre son gabarit vocal en répétant plusieurs couples de prénoms choisis aléatoirement parmi 4000 combinaisons possibles. Lorsque le salarié souhaite réinitialiser son mot de passe, le dispositif compare les

[329] Supra n° 227.
[330] CNIL, Délibération n° 2007-248 du 13 sept. 2007 autorisant la mise en œuvre par la Manufacture française des pneumatiques Michelin d'un traitement automatisé de données à caractère personnel reposant sur un procédé de reconnaissance vocale et ayant pour finalité la gestion des mots de passe, disponible sur le site internet www.legifrance.gouv.fr

mots répétés avec ceux contenus dans la base de données et précédemment enrôlés. Une fois l'identification effectuée, le mot de passe est réinitialisé et communiqué au salarié.
La CNIL a donné un avis favorable à la constitution de cette base de données d'empreintes vocales car elle observe « *que les caractéristiques techniques du dispositif, telles qu'elles lui ont été soumises, permettent de considérer qu'en l'état des connaissances sur la technologie utilisée,* ***le gabarit de l'empreinte vocale de la personne ne constitue pas une donnée biométrique qui "laisse des traces" pouvant être utilisées à des fins d'identification des personnes.***
En outre, compte tenu des modalités de mise en œuvre du dispositif et notamment des moyens utilisés pour garantir la sécurité des données et prévenir tout risque d'usurpation d'identité ou d'utilisation des données pour d'autres finalités, le recours à la constitution d'une base de données de gabarit d'empreintes vocales aux fins de gérer les mots de passe informatiques est adapté et proportionné à la finalité assignée au dispositif, au regard de la protection des données personnelles. »

Les informations collectées sont quantitativement raisonnables puisque, seules, les informations minimales d'identification sont collectées. Les données sont conservées, la plupart du temps, pendant toute la durée du contrat de travail, période pendant laquelle le salarié garde son compte informatique. Seul, le responsable du système a accès aux renseignements. La base de données contient des empreintes vocales, néanmoins, ces éléments seuls ne suffisent pas à identifier le salarié mais à réinitialiser un mot de passe. Une affaire similaire a été jugée au Canada.

Au Canada, en 2004, dans l'affaire Turner v. Telus Communications Inc.[331], plusieurs employés de la société se sont plaints du fait que leur employeur les obligeait à consentir à l'emploi d'un système de reconnaissance de la voix afin de réinitialiser les mots de passe. Du côté de l'employeur la justification du procédé était que cette technique lui permettait de garantir protection efficacité et rentabilité. La Commissaire adjointe à la protection des

[331] Lien vers le site internet de référence : http://www.privacylawyer.ca/blog/2005/12/federal-court-on-biometric-voice.html
Commentaires de l'affaire par la commissaire à la protection de la vie privée du Canada : http://www.priv.gc.ca/cf-dc/2004/cf-dc_040903_f.cfm

données du Canada a convenu, suite à un rapport effectué par son commissariat, que la collecte de l'empreinte vocale était moins attentatoire à la vie privée que d'autres techniques biométriques, tant qu'elle se conformait à la finalité assignée au traitement. Dans le contexte de la plainte, il n'est pas apparu que cette empreinte dévoilait des informations sur la personne. De plus, elle a rappelé qu'il était nécessaire de trouver un juste équilibre entre le droit à la protection des renseignements personnels et la nécessité d'organisation et de gestion de l'entreprise. De son côté, l'entreprise a apporté des garanties de protection des données personnelles. L'accès à la base de données est situé dans un endroit sécurisé et le nombre de personnes pouvant y accéder est restreint. Les données sont stockées pour une durée limitée à quelques mois suivant l'autorisation d'accès de l'employé concerné. Par ailleurs, le procédé garantit l'impossible reproduction de la voix à des fins frauduleuses. La collecte a été jugée raisonnable au regard des circonstances présentées. La plainte a été déclarée non fondée et l'affaire résolue.

La CNIL a estimé qu'il était préférable de collecter les données biométriques aux fins d'identification, lorsque la technologie ne laisse pas de traces, position qui pourrait avoir, pour conséquence, la multiplication des demandes, afin de constituer des bases de données. A cet effet, dans ses rapports annuels, la CNIL a conscience de l'importance de sa tache, mais dit ne disposer ni des moyens de ses ambitions, ni d'un personnel conséquent, pour contrôler toutes les entreprises détentrices de bases de données biométriques.

251. En 2007, la société Hitachi, développeur de la technologie de reconnaissance du réseau veineux de la main a obtenu l'autorisation de la CNIL de collecter ces données personnelles aux fins du contrôle d'accès[332]. Dès 2009, cette technologie a fait l'objet d'une autorisation unique, qui a contribué à son développement au sein des entreprises[333]. Fort de ce succès, un organisme américain a souhaité l'employer, en France, pour lutter contre la fraude

[332] CNIL, Délibération n° 2007-339 du 8 nov. 2007 autorisant la mise en œuvre par la société Hitachi Data Systems d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès au système d'information (autorisation n° 1248197), www.legifrance.fr

[333] CNIL, Autorisation unique AU-019, délibération n° 2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail, JO n°0142 du 21 juin 2009, disponible sur le site internet www.cnil.fr

à un examen international qu'il organise chaque année. L'autorisation donnée par la CNIL permet à cet organisme la constitution d'une base de données biométriques (2°).

2°. La technique de reconnaissance du réseau veineux des doigts de la main

252. Les industriels et chercheurs dans le domaine de la biométrie, ont découvert que le réseau veineux de la paume de la main était unique, d'un individu à l'autre. Cette découverte, a donné lieu à des applications biométriques d'authentification et plus récemment d'identification.

En effet, jusqu'en 2009, cette technologie était employée en authentification dans les entreprises, pour le contrôle d'accès des employés. Elle a pour avantage de ne pas « laisser de traces » donc de diminuer les risques de détournement.

Suite à une multiplication de fraudes à l'examen international du Graduate Management Admission Test (GMAT), l'association organisatrice a décidé de mettre en place un dispositif biométrique de reconnaissance du réseau veineux des doigts de la main. Cependant, le nombre de candidats ne permettait pas une authentification de ces derniers sur un support individuel. L'association a donc fait une demande tendant à stocker les données au sein d'une base centralisée. La CNIL a été amenée à se prononcer sur la pertinence de la constitution d'une base de données biométriques à l'égard de la protection des données personnelles des participants au concours.

253. Le GMAT est organisé par une association américaine à but non lucratif, nommée le Graduate Management Admission Council (GMAC). L'examen concerné permet d'évaluer des compétences dans différentes matières, afin d'intégrer un « Master of Business Administration » diplôme d'affaires de renommée internationale.

Cet organisme a souhaité mettre en œuvre ce dispositif à la suite de nombreuses fraudes. La finalité avancée est de deux sortes : « *La première sera de permettre de* ***vérifier qu'un candidat qui passe l'examen plusieurs fois sous la même identité, est bien le même individu***. *A cet effet, lorsqu'un candidat repasse l'examen, son gabarit biométrique sera préalablement transféré au poste de contrôle du centre d'examen depuis la base centrale, afin de permettre une vérification biométrique en début de session. La deuxième finalité sera de* ***vérifier, par***

comparaison des gabarits biométriques entre eux au sein de la base centrale, qu'une même personne ne s'est pas présentée sous deux identités distinctes au GMAT[334] ».

Du point de vue technique, il s'agit d'une identification biométrique, puisque les gabarits enregistrés ont vocation à être comparés au sein de la base de données. C'est une comparaison appelée « 1 contre N » qui vise à vérifier les identités mais aussi à déceler les identités multiples. Il y a donc une collecte massive de données stockées sur un serveur (sans doute relié au réseau). Le stockage de ces données sera hébergé par le prestataire Pearson Vue situé aux Etats-Unis.

Du point de vue juridique, la CNIL a estimé « *que le recours à la reconnaissance du réseau veineux de la paume de la main répond à* ***une finalité légitime*** *et* ***n'est pas excessif*** *au regard de cette finalité*[335] ».

Contrairement aux bases de données d'empreintes digitales, elle a eu à se prononcer sur le fort impératif de sécurité. En revanche, elle a apprécié, conformément à l'article 6 de la loi Informatique et libertés modifiée, que la finalité soit déterminée, explicite et légitime.
Il est vrai que la finalité est déterminée puisqu'elle précise les personnes visées par la mesure, c'est-à-dire, les candidats aux différentes épreuves. Elle est explicite car elle est avouée, claire et précise. Il s'agit d'éradiquer les fraudes à l'identité, qui ont, les années précédentes porté préjudice à la réputation de l'examen.

Quant à la question de la légitimité, le traitement nous paraît légitime, dans la mesure où il est question d'un examen à valeur et reconnaissance internationale. Il serait matériellement difficile, vu le grand nombre de candidats, d'appliquer à ce type d'examen un stockage sur support individuel. Cette technologie « *peut ainsi, lorsque le recours à un tel dispositif est* ***justifié par des raisons sérieuses*** *et* ***entouré de garanties appropriées****, être employée en matière de lutte contre la fraude à l'identité.* »

[334] CNIL, Délibération n° 2009-360 du 18 juin 2009 autorisant la mise en œuvre par le Graduate Management Admission Council (GMAC) représenté par Pearson Education France d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux de la paume de la main et ayant pour finalité de contrôler l'accès à des salles d'examen et d'empêcher la substitution de candidat à l'examen GMAT, demande d'autorisation n°1323460, disponible sur le site internet au www.cnil.fr
[335] Ibid.

La CNIL n'a pas précisé ce qu'il convenait d'entendre par la justification de « raisons sérieuses » mais nous supposons qu'il s'agit d'enjeux supérieurs comme le caractère international de l'examen et de sa reconnaissance à travers de nombreux pays.

En ce qui concerne les garanties appropriées, elles touchent aussi bien les sécurités avancées pour certifier un stockage fiable des données que l'hébergement des données à l'étranger.
L'hébergeur des données se situe aux Etats-Unis, pourtant, il devra se conformer à la loi Informatique et libertés en vertu de l'article 5 I 2° de la loi[336]. Ce dernier a signé une convention de clauses contractuelles types, qui permet à la CNIL d'avoir un contrôle sur les données (conservation, effacement), en plus d'un engagement des grands principes « informatiques et libertés ». La CNIL a estimé que ce procédé ne présentait pas de risques pour les droits et libertés fondamentaux mais exige que les candidats ne soient pas discriminés pour l'examen en cas de faux rejet. Elle a, en conséquence, donné son autorisation pour ce type de traitement.

254. Cette autorisation soulève plusieurs commentaires : les garanties prises par la CNIL semblent suffisantes, si elle peut s'assurer effectivement du respect des principes « informatique et libertés » lors de contrôles. Cette tâche sera sans doute délicate si elle doit se rendre aux Etats-Unis afin de vérifier si la convention a été suivie à la lettre et si les données ont été effectivement effacées.
Les données collectées sont nombreuses : le gabarit du réseau veineux de la paume de la main, des renseignements d'identification comme le nom, le prénom, le sexe, la date et le lieu de naissance, le numéro de téléphone, l'adresse électronique, la langue maternelle, le numéro d'inscription GMAT. Cependant, il serait impératif de s'assurer, qu'elles ne feront pas l'objet d'une utilisation frauduleuse sur le territoire américain.
Il s'agit d'une collecte massive de données biométriques au sein d'une base. Cette collecte, tout en étant justifiée, doit rester exceptionnelle. La CNIL n'a pas semblé dégager, contrairement aux bases de données d'empreintes digitales, de critères d'admissibilité sur les bases d'autres données biométriques sans doute parce que cette décision n'a pas vocation à s'étendre. Elle a précisé, au sein d'un article sur son site internet, le caractère exceptionnel de

[336] « *I- Sont soumis à la présente loi les traitements de données à caractère personnel :*
2°) Dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre Etat membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français, à l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre Etat membre de la Communauté européenne ».

cette autorisation et a insisté « *sur le fait que l'autorisation accordée à GMAC ne signifie pas qu'elle est, de façon générale, favorable à l'utilisation systématique de bases biométriques centralisées pour empêcher la fraude à tous les concours et examens nationaux*[337] »
Néanmoins, elle devra tôt ou tard, établir un document d'orientation comme elle l'a fait pour les empreintes digitales stockées au sein d'une base de données.

255. La première fonction du principe de finalité est de déterminer l'objectif pour lequel le traitement est mis en œuvre. Dès que cet objectif est déterminé et que l'autorisation est donnée par la CNIL de mettre en œuvre le traitement de données biométriques, l'entreprise doit se conformer aux exigences mentionnées dans l'autorisation. Si l'entreprise prend la liberté d'outrepasser cette finalité, elle commet un délit de détournement de finalités sujet à sanctions (sous section 3).

Sous section 3. Les sanctions du détournement de la finalité du traitement de données biométriques

256. Le principe de spécification de la finalité a pour vocation première de restreindre l'étendue du traitement. Une entreprise qui établit une demande d'autorisation doit justifier les raisons pour lesquelles elle souhaite collecter et traiter les données personnelles de ses salariés. Une fois l'autorisation donnée par la CNIL, l'entreprise ne doit pas outrepasser l'autorisation mais seulement traiter les données personnelles conformément à cette finalité.
L'article 6 de la loi Informatique et libertés précise que la finalité doit être « *adéquate, pertinente et non excessive* ». Elle doit donc avoir un objectif précis (gestion des horaires, contrôle d'accès par exemple).

Pour une entreprise, est délictueux, le fait de détourner les données personnelles des salariés, pour un autre objectif que celui assigné au traitement déclaré à la CNIL. Lorsque la CNIL constate, lors de ses contrôles, un manquement sérieux à ce principe, elle a le pouvoir de prononcer des sanctions administratives ou financières. Selon la gravité du manquement, elle a la faculté d'avertir, d'envoyer une lettre de mise en demeure, assortie d'un délai pouvant s'échelonner de dix jours à trois mois, d'ordonner des sanctions pécuniaires, de procéder à des

[337] CNIL, « La CNIL autorise le recours à la biométrie pour lutter contre la fraude à un concours mondial organisé par des grandes écoles de commerce », article du 15 juil. 2009, disponible sur le site www.cnil.fr

injonctions de cesser le traitement et même de retirer une autorisation accordée en application de l'article 25 de la loi. Elle peut, par ailleurs, dénoncer le détournement de finalités qu'elle a constaté auprès du procureur de la République[338].

257. Le délit de détournement de finalité est une des sanctions pénales envisageables en matière de biométrie. Il en existe d'autres, comme la sanction du défaut d'information, la durée de conservation excessive des données, la divulgation d'informations et le manquement à la sécurité des fichiers.
Le délit de détournement de finalité est mentionné à l'article 226-21 du Code pénal lequel dispose que « *le fait pour toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, règlementaire ou la décision de la commission nationale informatique et libertés autorisant le traitement automatisé ou par des déclarations préalables à la mise en œuvre de ce traitement, est puni de 5 ans d'emprisonnement et de 300 000 euros d'amende* ».

L'article 52 de la loi Informatique et libertés modifiée en 2004 a introduit un mécanisme d'information par lequel « *le Procureur de la République avise le Président de la Commission nationale informatique et libertés de toutes poursuites relatives aux infractions aux dispositions de la section 5 du chapitre VI du titre II du livre II du code pénal et, le cas échéant, des suites qui leur sont données.* » Le procureur de la République informe le président de la CNIL de la date et de l'objet de l'audience, par lettre recommandée adressée au moins dix jours avant la date. Ce dernier pourra être appelé « *à déposer des observations ou à les développer oralement à l'audience* ». Ce dispositif, assez inédit, n'était pas prévu initialement par la Directive de 1995. Toutefois, la CNIL a exprimé cette recommandation, suivie dans la modification de la loi en 2004, dans son avis portant sur le projet de loi.

258. Enfin, il faut préciser qu'en vertu de l'article 226-22-1 du Code pénal, le juge pénal dispose d'un pouvoir d'effacement des données qui font l'objet du traitement ayant donné lieu à infraction. La CNIL a le pouvoir de constater l'effectivité de cet effacement.
Le rapport d'activité de la CNIL a établi pour l'année 2007[339] que 18 % des dossiers de la formation contentieuse étaient relatifs à la biométrie.

[338] Art. 45 et s. de la loi n° 78-17 du 6 janv. 1978 modifiée.

En mars 2010, la CNIL a sanctionné une société, pour avoir utilisé frauduleusement des dispositifs biométriques alors qu'elle en avait refusé l'utilisation quelques années plus tôt. Elle a ordonné à la société de cesser tout traitement sans néanmoins prendre de sanctions pénales ou pécuniaires. Elle n'a pas relevé de détournement de finalités mais dans les faits, ce détournement peut intervenir lorsque l'entreprise a pour finalité initiale le contrôle d'accès aux locaux et qu'elle contrôle par là même les horaires des salariés à l'aide des historiques de passage. Ces derniers doivent en principe être régulièrement effacés. La CNIL a constaté leur effacement lors du contrôle, mais elle n'a pas pu déterminer s'il s'agissait d'une coïncidence ou du respect partiel de la loi Informatique et libertés.
Nous n'avons pas d'exemples, à ce jour, de détournement de finalité de données biométriques, mais nous pouvons raisonner par analogie sur la base d'exemples, dans d'autres domaines.

Entre les deux tours des élections présidentielles de 2002, une société a adressé un courrier électronique à des internautes, sous la forme d'un sondage politique, présenté comme anonyme. Lors d'un contrôle, la CNIL a constaté que la société avait constitué un fichier unique comportant les données personnelles des internautes[340]. Elle a dénoncé ces agissements au parquet de Nanterre qui a condamné la société à 5 000 euros d'amende. La sanction pécuniaire n'est pas élevée au regard de la peine encourue et se veut sans doute plus éducative que punitive. Par ailleurs, la publicité consécutive à la publication du jugement et de la mention de cette affaire sur le site internet de la CNIL a eu sans doute plus de répercussions que la sanction financière même si l'on peut regretter qu'il n'existe pas de publication obligatoire du jugement sur le site internet de l'entreprise, comme c'est le cas pour les sociétés de presse en matière de droit à l'image.

259. A titre de conclusion, le principe de finalité a deux vocations :
La première, tend à déterminer les réelles intentions de l'emploi de la biométrie. Il s'agit du principe de spécification de la finalité rappelé notamment par l'OCDE. En faisant de la biométrie une technologie qu'il est nécessaire d'avancer essentiellement pour des finalités

[339] CNIL, Schéma de la typologie des dossiers présentés en formation contentieuse, 28ème Rapport d'activité 2007, p. 48, disponible sur le site www.cnil.fr

[340] CNIL, « Condamnation définitive d'une société qui, à travers un sondage prétendument anonyme, avait collecté des données personnelles sensibles », article du 30 mai 2006, disponible sur le site internet de la CNIL au www.cnil.fr

sécuritaires, les entreprises invoquent de manière presque systématique le besoin de sécurité pour justifier le recours à la biométrie. Cette première vocation ne suffit pas, à elle seule, à garantir la protection des données personnelles, même si elle constitue une antériorité nécessaire qui ne peut faire l'objet d'une économie. En l'état actuel, les formulaires d'autorisation préalable au traitement de données biométriques, demandent d'énoncer la finalité pour laquelle le traitement est sollicité et de justifier le choix du dispositif (document nommé annexe dispositifs biométriques). Nous pensons que les formulaires sont complets de ce point de vue et qu'il ne serait pas pertinent d'alourdir les formalités. Seuls, les contrôles sur place permettraient de veiller au respect du principe de finalité et là encore, le manque de moyens humains et financiers est souvent soulevé par la Commission.

La seconde vocation du principe de finalité est la sanction. Le détournement de finalités est passible de poursuites pénales. C'est cette dernière qui semble particulièrement intéressante mais là encore, les entreprises ont la possibilité de dissimuler ce détournement. Une entreprise est capable d'implanter un dispositif biométrique en ayant déclaré une finalité de contrôle d'accès et dans le même temps, contrôler les horaires des salariés à travers les historiques de passage. La difficulté liée au principe de finalité réside dans le fait que tout traitement biométrique peut être justifié par une finalité invoquant la sécurité ou une meilleure gestion des horaires de travail ou de l'accès au restaurant de l'entreprise. Pour s'en convaincre il s'agit de consulter les multiples demandes d'autorisation auprès de la CNIL, elles sont pour la plupart fondées sur les mêmes finalités et la majeure partie des autorisations sont favorables, dès lors que la technologie de reconnaissance par empreintes digitales n'est pas sollicitée.

D'autres pays suivent un cheminement juridique similaire à la CNIL (finalité, proportionnalité, sécurité, information, responsabilité), comme le Canada ou l'Australie, sans toutefois disposer de procédure d'autorisation préalable puisque, pour la plupart, seule une déclaration du traitement suffit.

En conséquence, nous nous apercevons que le principe de finalité n'est pas garant à lui seul de la protection des données personnelles, il doit s'accompagner aussi du respect du principe de proportionnalité.

260. Si la plupart des techniques ont une finalité déterminée, explicite et légitime, à l'inverse, toutes les techniques biométriques ne sont pas proportionnelles aux finalités avouées. Le principe de proportionnalité est complémentaire à celui de la finalité dans la mesure où il conditionne, lui aussi, la licéité du traitement (Chapitre 2).

Chapitre 2. La sujétion du traitement des données biométriques au principe de proportionnalité

« *L'homme n'existe qu'autant qu'il risque,*
qu'autant qu'il parie, qu'il choisit arbitrairement ;
(...) quelle action n'est pas aveugle,
et quelle science n'est pas constituée à base de pari ?
Le sort de l'homme est de tâtonner[341] »

261. Le rapport rendu par Gérard Lyon-Caen sur « les *libertés publiques et l'emploi*[342] », a contribué à la prise de conscience des dangers que pouvait causer l'usage des nouvelles technologies dans l'entreprise et de la reconnaissance de l'existence de la sphère privée du salarié, au sein d'une entreprise, pendant ses heures de travail. Il relève d'ailleurs, que « *le salarié n'est pas seulement un être de travail. Son identité intime doit être respectée*[343] ». L'article 9 al. 1 du Code civil rappelle en effet que « *chacun a droit au respect de sa vie privée* », y compris le salarié sur son lieu de travail.

Or, il y a, depuis quelques années, une progression des libertés dans le milieu professionnel, notamment dans l'utilisation raisonnable de l'Internet sur le poste de travail du salarié qui lui permet, en concomitance, d'effectuer les tâches de l'entreprise, mais aussi de consulter une messagerie électronique d'ordre privé. Les réseaux sociaux, les jeux et paris en ligne sont les nouveaux « divertissements » qui mettent en péril l'exécution du contrat de travail. L'employeur peut alors être poussé à surveiller l'activité effective du salarié alors que seul ce dernier peut déterminer « *l'étendue de sa sphère d'intimité*[344] ».

La Cour de cassation a récemment jugé, sous le visa de l'article 9 du Code civil, que « *les fichiers créés par le salarié à l'aide de l'outil informatique mis à sa disposition par*

[341] M. Villey, « Réflexion sur la philosophie et le droit », Les carnets de Michel Villey, préparés et indexés par M. Frison-Roche et Ch. Jamin, préface B. Kriegel et F. Terre, PUF, 1995, Livre II, n° 92 p. 57.
[342] G. Lyon-Caen, Les libertés publiques et l'emploi, Rapp. min. Travail, Emploi et Formation professionnelle : La Documentation française, Paris, 1992.
[343] G. Lyon-Caen, Les libertés publiques et l'emploi, Rapp. min. Travail, Emploi et Formation professionnelle : La Documentation française, Paris, 1992, p.158.
[344] B. Bossu, « Un huissier peut accéder aux fichiers non personnels d'un salarié », JCP S 2008. 1582

l'employeur pour les besoins de son travail sont présumés avoir un caractère professionnel, sauf si le salarié les identifie comme étant personnels, en sorte que l'employeur est en droit de les ouvrir hors la présence de l'intéressé[345] ». Les fichiers et les dossiers créés par le salarié sont présumés professionnels à défaut de mentions contraires.

Il en va de même en ce qui concerne la connexion internet, elle est présumée professionnelle dès lors que le salarié l'utilise depuis son poste de travail, durant ses heures de travail[346]. De nombreuses jurisprudences sur les messageries électroniques, ont rappelé à l'employeur qu'il ne pouvait consulter le contenu et le flux (nombre d'envois et de réceptions) des messages électroniques sans l'accord préalable du salarié[347] exception faite de la survenance d'un évènement ou d'un risque particulier[348].

En somme, l'existence d'une vie privée au travail, même si elle est reconnue et protégée « *ne saurait créer une zone d'immunité ou d'impunité pour des fautes commises à l'encontre de son propre employeur ou de tiers*[349] ». Il a été nécessaire de rappeler aux chefs d'entreprise qu'il existe une vie privée à respecter, au sein de l'activité professionnelle, tout en précisant aux salariés qu'ils ont un devoir de loyauté, impliquant de respecter le contrat de travail passé avec l'employeur. Les juges rappellent régulièrement que l'employeur est en droit d'attendre raisonnablement du salarié, le respect de l'obligation générale de loyauté[350]. Les salariés ont des droits individuels (respect de la vie privée, protection des données personnelles, liberté d'aller et de venir, droit à l'emploi), des droits collectifs (liberté de manifestation et de réunion), mais aussi des devoirs (devoir de loyauté envers l'employeur, respect du contrat de travail).

Sur le lieu de travail, les nouvelles technologies bouleversent quelque peu ces schémas traditionnels, de telle sorte que certains employeurs ont recours aux chartes informatiques, pour rendre opposables aux salariés, les règles de bonne conduite informatique et se

[345] Cass. soc., 18 oct. 2006: Juris Data n° 2006-035418; Comm. com. électr. 2007, comm. 61, note A. Lepage ; Cass. soc., 21 oct. 2009, pourvoi n° 07-43.877, Bull. 2009. V, n° 226, disponible sur le site au www.legifrance.gouv.fr
[346] Cass. soc., 9 juill. 2008, n° 06-45.800 : Juris Data n° 2008-044801
[347] Cass. soc., 2 oct. 2001, Arrêt Nikon, pourvoi n° 99-42.942, Bull. 2001. V n° 291, p. 233, RTD Civ. 2002, p. 72, note de J. Hauser.
[348] Cass. soc., 17 juin 2009, Comm. com. électr. 2009, comm. 106, note É.-A. Caprioli.; Revue de droit du travail 2009 p. 591, comm. L. Marino.
[349] CA Aix-en-Provence, 1er ch. A, 25 novembre 2003, n°2003/798.
[350] Cass. soc.; 16 juin 1998 : D. 1998. IR. 177

constituer, ainsi, des moyens de preuve en cas de litiges. Plusieurs sociétés ont souhaité préciser les limites à l'usage des nouvelles technologies mais aussi les droits que les salariés peuvent attendre de cette même entreprise (protection des données personnelles). Ainsi, les entreprises Canon ou Air France BlueLink ont signé cette charte avec leurs employés et ont constaté une nette amélioration de leurs rapports face à ces nouvelles technologies (l'Internet, la géolocalisation, vidéosurveillance)[351].

Dans un rapport sur la cybersurveillance des salariés, la CNIL a rappelé que ces chartes avaient vocation à « *assurer une parfaite information des utilisateurs, de sensibiliser les salariés ou les agents publics aux exigences de sécurité, d'appeler leur attention sur certains comportements de nature à porter atteinte à l'intérêt collectif de l'entreprise ou de l'administration*[352] ». Les chartes informatiques disposent d'une reconnaissance juridique[353] et sont une première initiative mais elles ont un contenu trop variable quant à l'équilibre entre devoirs et libertés. Elles contiennent souvent des affirmations péremptoires et de nombreux interdits qui peuvent les rendre inopérantes en cas de litige.

262. Les chefs d'entreprise ont trouvé, en la biométrie, un fabuleux outil qui associe rentabilité et amélioration de la productivité. Cependant, dans un même temps, cet outil peut être détourné pour un usage de surveillance et avoir pour conséquence d'entraver le respect de la vie privée du salarié sur son lieu de travail. L'usage de la biométrie ne doit pas être une régression pour les libertés mais doit contribuer au développement des activités de l'entreprise dans le respect des personnes.

L'article L. 1121-1 du Code du travail énonce que « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché*. »

Le principe de finalité, comme étudié précédemment peut être une première piste d'évaluation de l'objectif visé par l'employeur dans l'usage de la biométrie. C'est un principe qui permet aussi de prendre des sanctions en cas de détournement d'usage. Toutefois, il n'est pas

[351] V. Leblanc, « Des salariés en libertés surveillées », in Entreprises et Carrières, n° 961, du 30 juin au 6 juil. 2009, p. 12 à 23.
[352] CNIL, « La cybersurveillance sur les lieux de travail », Rapport présenté par H. Bouchet, 5 fév. 2002, p. 4, disponible sur le site internet de la CNIL, www.cnil.fr
[353] Cass. Soc., 21 déc. 2006, n° 05-41.165, commenté dans la Gazette du Palais, 7 août 2007, n° 219, p. 22

suffisant à lui seul[354]. Le principe de proportionnalité a vocation à s'interroger plus fortement sur l'appréciation du « bon usage » d'une technique biométrique dans son sens large, c'est-à-dire, en prenant en compte, tant la technologie employée que les mesures qui tendent à garantir la protection des données personnelles. Il ne peut être circonscrit à la technique mais va s'étendre aussi à l'appréciation du mode de stockage. Il permet de mesurer le plus équitablement possible, la pertinence de l'emploi d'une technique biométrique au regard de l'objectif visé initialement. Le principe de proportionnalité comprend donc, non seulement l'appréciation du choix du dispositif biométrique envisagé, mais aussi du choix du mode de stockage de la donnée qui en découle. Il est entendu par la CNIL, comme le fait de déterminer l'outil biométrique le mieux adapté à la finalité du traitement envisagé[355]. Les questions de proportionnalité sont souvent liées à celle de la sécurité employée pour garantir l'anonymat et la non-divulgation des données issues du traitement.

Ce principe permet d'évaluer la pertinence de l'emploi de la biométrie et des moyens alloués pour la protection des données personnelles dans la prise en considération des intérêts mutuels des parties en présence. Il importe d'évaluer si ce principe parvient à l'encadrement de la maîtrise collective de l'usage de la biométrie en entreprise.

263. Le principe de proportionnalité tend à concilier les intérêts de tous les acteurs de l'entreprise, employeur et salariés. Ce principe s'attache donc à apprécier les réelles motivations de l'emploi de la biométrie et les garanties que les chefs d'entreprise sont prêts à avancer, comme l'emploi de la cryptographie, pour la protection des données personnelles (Section 1). Dès lors que les chefs d'entreprise font usage des bonnes pratiques « informatique et libertés » en s'interrogeant sur l'opportunité de l'emploi de la biométrie, la CNIL a pour mission, d'évaluer la proportionnalité de l'usage des techniques biométriques au regard du critère de traçabilité (Section 2).

[354] Supra n° 256.
[355] CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, 27 nov. 2007, p. 9 in fine, disponible sur le site internet www.cnil.fr

Section 1. L'appréciation de la balance des intérêts collectifs en entreprise

264. Le terme proportionnalité n'apparaît pas de façon explicite dans la plupart des textes fondateurs sur la protection des données personnelles. Pourtant il est reconnu comme étant un principe majeur.

La Convention 108[356], premier instrument international juridique contraignant dans le domaine de la protection des données personnelles, précise dans son article 5 sur la qualité des données, qu'elles doivent être « c- ***adéquates***, ***pertinentes*** *et* ***non excessives*** *par rapport aux finalités pour lesquelles elles sont enregistrées;* ». Cet article est intégré au sein d'un Chapitre 2 intitulé « *Principes de base pour la protection des données* ».

Cette formule a été reprise, mot pour mot, par la Directive européenne de 1995 « *la collecte de données biométrique doit être adéquate, pertinente et non excessive au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement*[357] ».

La loi du 6 août 2004 reprend les mêmes termes en son article 6 3°) qui dispose que « *Les données sont* ***adéquates***, ***pertinentes*** *et* ***non excessives*** *au regard des finalités pour lesquelles elles sont collectées et* ***de leur traitement ultérieurs***[358] ». Aucun texte n'a expressément évoqué le principe de proportionnalité, même si dans l'évaluation de la CNIL, le principe de finalité doit être apprécié avec son corollaire, le principe de proportionnalité[359]. Il s'agit de déterminer le juste équilibre entre les moyens techniques mis en œuvre et la finalité pour laquelle le traitement est requis.

Le Comité consultatif national d'éthique mentionne explicitement, quant à lui, le critère de proportionnalité et l'élève en critère majeur : « *la notion de proportionnalité des moyens* ***est en effet essentielle à prendre en considération puisque intégrer des données personnelles au-delà de ce qui est nécessaire à la finalité déclarée ne saurait en aucun cas être considéré***

[356] Convention STE n°108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Conseil de l'Europe, 28 janv. 1981.
[357] Art. 6 C de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO n° L 281 du 23 nov. 1995 p. 0031 – 0050.
[358] Loi n° 2004-801du 6 août 2004, art. 6 3° de la loi, JO 1er août 2004
[359] CNIL, 22ième Rapport d'Activité 2001, Doc. Fr. 2002, Chap. 3 « Un siècle de Biométrie », p. 167

comme éthique. *Cette asymétrie des buts et des moyens met en relief les enjeux réels qui sont ceux d'une surveillance accrue des conduites humaines au nom de leur protection*[360] ».

265. Le principe de proportionnalité associé à l'usage de la biométrie en entreprise conduit les responsables de traitement à poser les questions suivantes : l'usage de la technique biométrique choisie est-il raisonnable pour l'objectif assigné au traitement ? Ne peut-on pas recourir à un autre système de sécurité tout aussi efficace et moins contraignant pour les personnes qui s'y soumettent ? L'emploi de l'empreinte digitale est-il raisonnable pour contrôler le temps de travail d'un salarié ou pour contrôler l'accès à un site ?

Le choix du dispositif est raisonnable lorsqu'il tient compte des répercussions ultérieures du traitement, sur l'anonymat et la fiabilité de l'identité des personnes en cas de détournement.
En Suisse, le Préposé fédéral à la protection des données précise, à propos du principe de proportionnalité qu' « *on recourra en particulier à la biométrie, que s'il n'y a pas de moyens moins intrusifs d'atteindre l'objectif visé ou si celle-ci est un élément de protection et/ou sécurité des données*[361] ».

266. Le principe de proportionnalité, permet à la CNIL d'exiger du responsable du traitement, la preuve qu'il n'est pas possible de recourir à une autre méthode d'identification, que la biométrie ne dissimule pas l'intention d'épier les salariés d'une entreprise. La CNIL adopte cette grille d'appréciation, et comme d'autres commissions de protection des données personnelles dans le monde, il importe d'en dresser un aperçu lors des développements ultérieurs. Le principe de proportionnalité peut être apprécié par rapport à la qualité des données (A) mais aussi, en tenant compte de l'évaluation des risques ainsi que de la traçabilité de la technologie employée pour ce traitement (B).

[360] CCNE, Avis n° 98, « Biométrie, données identifiantes et droits de l'homme », 20 juin 2007, disponible sur le site internet du CCNE au http://www.ccne-ethique.fr/
[361] Préposé fédéral suisse à la protection des données, Guide relatif aux systèmes de reconnaissance biométrique, Version 1.0, Sept. 2009, consultable sur le site internet au
http://www.edoeb.admin.ch/

A. La qualité des données appréciée au regard du principe de proportionnalité

267. L'article 6 3° de la loi n°78-17 du 6 janvier 1978 modifiée énonce que les données traitées sont « *adéquates, pertinentes, et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs* ». Il énonce ainsi que le principe de proportionnalité suppose que le responsable de traitement soit particulièrement vigilant aux données qu'il va collecter à l'égard de la finalité du traitement. Ce principe a donc vocation à réguler la collecte des données personnelles.

D'autres pays, aux législations avancées en matière de protection des données personnelles comme l'Australie[362], la Nouvelle-Zélande[363] ou le Canada[364] (Provinces de l'Alberta, du Québec et du Saskatchewan), utilisent le principe de proportionnalité comme un principe « régulateur » de la collecte des données personnelles, tant pour le secteur public que pour le secteur privé, au niveau fédéral et provincial. Le droit comparé apporte un regard croisé sur l'appréciation des différents principes, en confrontant leurs législations « informatique et libertés ». Le terme « proportionnalité » n'est pas évoqué explicitement, mais dans les grands principes de ces législations, deux éléments reviennent, celui d'une collecte en adéquation avec la finalité pour laquelle les données sont collectées et celui d'une collecte raisonnable des données.

---

[362] Part 3- Section 14, "*Principle 1 Manner and purpose of collection of personal information;*

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:

(a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and

(b) the collection of the information is ***necessary for or directly related to that purpose****.*

2. Personal information shall not be collected by a collector ***by unlawful or unfair means****.*"

The Privacy Act, 1988, http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/

[363] Part 2 - Section 6- Information Privacy Principles- Principle 1 Purpose of collection of personal information, "*Personal information shall not be collected by any agency unless—*

- *(a) The information is collected for a lawful purpose connected with a function or activity of the agency; and*
- *(b) The collection of the information* ***is necessary for that purpose****.*"

The Privacy Act, 1993, http://www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html

[364] Partie 1- Section 1- Protection des renseignements personnels- l'article 5-1 fait référence à l'obligation de respecter les grands principes de l'Annexe 1 Principe 2 sur la détermination des fins de la collecte de renseignements 4.2.2 « *Le fait de préciser les fins de la collecte de renseignements personnels avant celle-ci ou au moment de celle-ci permet à l'organisation de déterminer les renseignements dont elle a besoin pour réaliser les fins mentionnées. Suivant le principe de la limitation en matière de collecte (article 4.4), l'organisation ne doit recueillir que les renseignements nécessaires aux fins mentionnées.* » Loi sur les renseignements personnels et les documents électroniques, 2000 ch5, http://lois.justice.gc.ca/fr/

268. En France, au sens de la loi Informatique et libertés modifiée[365], le principe de proportionnalité implique que les données soient traitées de manière « *adéquate, pertinence et non excessive* (1°) » et de façon conforme au traitement ultérieur (2°).

1°. Données adéquates, pertinentes et non excessives

269. Selon le dictionnaire Larousse, l'adéquation est la « *conformité à l'objet, au but qu'on se propose*[366] ». Une donnée adéquate est une donnée qui est conforme à la finalité pour laquelle elle est collectée. Il en a été jugé ainsi par la CNIL, à propos du Centre d'aide au travail de Thionville[367], à la suite d'une demande tendant au traitement de données à caractère personnel, qui repose sur la reconnaissance du réseau veineux et dont la finalité est le contrôle de la présence des travailleurs handicapés.

La Commission a considéré que la collecte des nom et prénom, de l'adresse, du gabarit du réseau veineux du doigt, du numéro identifiant et des coordonnées de la personne à prévenir en cas de problèmes étaient des données adéquates par rapport à la finalité qui consiste à s'assurer de la présence des travailleurs handicapés. Les données collectées par le Centre ont pour but de s'assurer de la présence des individus. Pour cet établissement, cela implique la possibilité, au minimum, de faire des comparaisons entre l'identité de la personne, son numéro identifiant à l'intérieur des locaux et son gabarit biométrique. Pour ce qui est des coordonnées de la personne à prévenir en cas de problème, cette information personnelle paraît conforme à l'objet principal du Centre qui est de veiller au bon déroulement des activités des travailleurs handicapés. Les données collectées sont en adéquation avec la finalité du traitement.

270. La pertinence des données personnelles est prouvée lorsque la collecte est en relation directe avec l'objet du traitement. Ce qui implique de ne recueillir, que les renseignements nécessaires à celui-ci. La récolte de ces données se justifie par la liaison

[365] Art. 6. 3° de la loi n° 78-17 du 6 janv. 1978 modifiée, JO 7 août 2004.
[366] Dictionnaire Larousse en ligne, disponible sur le site http://www.larousse.fr/
[367] CNIL, Délibération n° 2008-038 du 7 fév. 2008 autorisant la mise en œuvre par le Centre d'aide au travail - « le Vert Coteau » de Thionville d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux et ayant pour finalité le contrôle de la présence des travailleurs handicapés (autorisation n° 1238037), disponible sur le site www.legifrance.gouv.fr

étroite entre elles et la finalité du traitement. Cette relation explique le fait que les données ne doivent pas être collectées de manière excessive. Si elles sont pertinentes et raisonnables (non excessives), elles se rapprochent au plus juste de la finalité du traitement. Prenons l'exemple concret d'une entreprise qui désire avoir recours à la biométrie pour le contrôle d'accès à ses locaux. Elle devra seulement récolter les données d'identité en stricte relation avec l'objectif de sécurité des lieux : les nom et prénom, gabarit biométrique, numéro identifiant du salarié, sa fonction au sein de l'entreprise et l'historique des passages. Ces informations ne devront, en aucune façon, être associées à d'autres renseignements personnels inutiles dans ce cas, comme le régime matrimonial, d'assurance ou les coordonnées bancaires, données de santé, etc.

Ces caractères sont déterminants car ils permettent de ne pas collecter excessivement des données réputées inutiles pour le traitement envisagé. En cas de détournement du gabarit biométrique collecté associé à d'autres données personnelles, ce qui représente une crainte majeure en matière de biométrie, seule une faible quantité de données seraient concernée.

271. Les prescriptions du législateur ne s'arrêtent pas à la collecte. La licéité du traitement des données est conditionnée à un traitement ultérieur des données personnelles, compatible à la finalité déclarée (2°).

2°. Le traitement ultérieur compatible des données

272. Le temps qui passe, fait courir un risque important de dégradation ou de détournement des données personnelles. Même si la plupart de ces dernières sont protégées par des solutions cryptographiques, les systèmes informatiques se heurtent à des problèmes croissants de dysfonctionnement ou des risques d'intrusion. L'article 6 3° in fine de la loi Informatique et libertés interdit toute collecte ultérieure des données qui serait incompatible avec la finalité. Il importe donc, de s'assurer de la pérennité et de l'absence de divulgation ou de détérioration des données biométriques.

Le principe de proportionnalité tient compte de la technique utilisée par rapport à la finalité envisagée mais aussi de la durée de la conservation des données. Si elles sont collectées pour

la durée du contrat de travail du salarié, l'entreprise doit maintenir les données adéquates pertinentes et non excessives, mais aussi ne pas les conserver au-delà de ce contrat par mesure de sécurité. Tout traitement ultérieur à cette date est un traitement excessif des données personnelles, susceptible d'être sanctionné.

273. Ces règles se résument par la nécessité de ne traiter que les données pertinentes, en relation avec la finalité du traitement. Il doit être raisonnable dans sa quête, et s'il est en droit de collecter le numéro de sécurité sociale de son salarié pour la gestion des fiches de paie et la gestion du personnel[368], en revanche, ce ne sera pas le cas de la déclaration d'impôts pour laquelle on considère qu'elle contient des informations à caractère privé.

Les conditions de licéité du traitement se retrouvent dans un bon nombre de délibérations des homologues de la CNIL à l'étranger. En matière de biométrie, l'Australie, par exemple, a établi dès 2001, un Code de la vie privée sur l'usage des données biométriques[369] qui précise, en substance, les précautions et attitudes à avoir, dès lors qu'une entreprise recourt à la biométrie. Il ressort de la section F 1-1 de ce même Code intitulée « *Biometric Institute Privacy Principles* » qu'un contractant doit collecter uniquement les informations personnelles qui lui sont strictement nécessaires à la conduite de son activité[370]. Cette collecte doit être raisonnable et se dérouler conformément à la loi.

274. On peut considérer qu'un traitement de données biométriques est proportionnel dès lors que seules, les données nécessaires à la conduite de l'activité sont collectées. Cela implique d'avoir préalablement réfléchi aux critères de pondération de l'usage de la biométrie en entreprise (B).

[368] Décret n° 91-1404, du 27 déc. 1991 – Art. R. 115-1 et R. 115-2 du Code de la sécurité sociale.
[369] Approval of the biometrics institute privacy code, disponible sur le site internet www.biometricprivacy.org
[370] "*A Code Subscriber must not collect personal information unless the information is necessary for one or more of its functions or activities.*"

B. La « pondération » des intérêts de l'entreprise

275. Le principe de proportionnalité commande la plupart des avis de la CNIL sur la biométrie. Si un dispositif biométrique est employé de façon mesurée entre la technologie choisie et la finalité pour laquelle elle est requise, rien ne s'oppose à son implantation. Nous parlons ici de pondération comme « *quelqu'un qui agit avec réflexion et modération*[371] ». En entreprise, le responsable de traitement est la personne chargée de veiller à l'équilibre de la balance entre les intérêts légitimes de l'entreprise et la protection des données personnelles des salariés.

En premier lieu, le principe de proportionnalité est évalué par la CNIL en fonction de la technologie choisie par l'employeur, qu'il s'agisse de l'emploi d'un simple badge ou de puces RFID. En second lieu, une fois la technologie déterminée, la CNIL apprécie la pertinence du mode de stockage (authentification ou d'identification[372]).

276. L'Irlande[373], soumise à la même directive européenne que la France, propose aux chefs d'entreprise désireux d'implanter des dispositifs biométriques, une grille de réflexion sur leurs réelles intentions quant à l'emploi de ce dispositif. Cette méthodologie très pertinente, équivaut à une auto-évaluation « informatique et libertés » de l'entreprise, sur la réalisation de la politique de sécurité. Elle consiste à évaluer la nécessité de l'utilité d'une technique biométrique dans l'environnement de l'entreprise (1°), à estimer la fiabilité du dispositif (2°) ainsi qu'à mesurer l'usage raisonnable du dispositif par rapport aux finalités du traitement (3°).

[371] Dictionnaire Larousse, disponible sur le site internet www.larousse.fr
[372] Supra n° 224.
[373] Commissaire irlandais à la protection des données, Guide à l'attention des employeurs, disponible sur le site internet http://www.dataprotection.ie/viewdoc.asp?m=m&fn=/documents/guidance/bio.htm

1°. L'usage nécessaire de techniques biométriques dans l'entreprise

277. Une entreprise qui désire recourir à la biométrie doit évaluer les avantages et les inconvénients de ce choix sur la vie privée des salariés. Au préalable, le responsable de traitement doit prendre en considération l'existence de solutions alternatives si l'emploi de la biométrie n'est pas nécessaire. Ainsi, selon le Conseil de l'Europe, « *la biométrie ne devrait pas être choisie parce qu'elle est pratique à utiliser (...) Il faut prendre en compte les aspects socioculturels et les réticences possibles à l'égard de l'utilisation instrumentale du corps humain*[374] ». Elle ne devrait être employée que si l'employeur « ne peut pas s'en passer[375] ».

Toutefois, le principe de subsidiarité, bien que pertinent, ne peut pas toujours être totalement appliqué pour plusieurs raisons. Les nouvelles technologies sont nombreuses et toujours plus performantes, de telle sorte que les méthodes traditionnelles de sécurité ne peuvent plus rivaliser. De ce fait, les entreprises avancent les performances de la biométrie pour privilégier, par exemple, l'emploi d'une technique biométrique de reconnaissance du contour de la main plutôt que le traditionnel badge, pour contrôler les horaires ou l'accès à l'entreprise. Elles se tournent progressivement vers l'emploi de la biométrie, notamment pour son aspect pratique et son moindre coût, alors qu'elles disposent déjà d'un système de sécurité (d'ordre humain - et/ou - informatique).

Ce constat est le même outre-Manche puisque l'Office du commissaire à la protection des données irlandais a précisé, dans une communication adressée aux employeurs, qu'ils devaient toujours rechercher une solution de sécurité moins intrusive pour les libertés que la biométrie[376].

Il importe cependant de privilégier les dispositifs qui font appel à l'authentification biométrique plutôt qu'à l'identification. Le principe de subsidiarité ne sera donc plus

[374] Conseil de l'Europe, Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, 2005, p. 24, disponible sur le site internet du Conseil de l'Europe http://www.coe.int/

[375] La nécessité est le caractère de ce qui est nécessaire, de ce dont on ne peut se passer. Définition du Dictionnaire Larousse en ligne, http://www.larousse.fr/

[376] Office de protection des données personnelles irlandais, Guide à l'attention des employeurs sur le site internet du commissaire à la protection des données irlandais : http://www.dataprotection.ie/viewdoc.asp?m=m&fn=/documents/guidance/bio.htm

simplement le fait de chercher une technologie autre que la biométrie, mais plutôt la mise en place d'un dispositif biométrique sans constitution de base de données.

La CNIL a fait application du principe de subsidiarité, dans une série de délibérations où elle a notamment refusé l'autorisation à la société Nigay SA, spécialisée dans la fabrication de produits alimentaires (caramels aromatiques, caramels colorants) l'emploi d'un dispositif de reconnaissance d'empreintes digitales avec stockage dans une base de données[377].

La société Nigay SA, a fait valoir qu'elle ne pouvait avoir recours aux autres technologies (le dispositif de reconnaissance du contour de la main et le dispositif de reconnaissance du réseau veineux des doigts de la main) pour des raisons d'hygiène ou de dysfonctionnements possibles du dispositif causés par des « *doigts salis par [du] caramel ou [du] noir de cambouis* ». La CNIL a refusé les motifs invoqués par la société et a estimé que cette dernière pouvait employer des solutions subsidiaires moins intrusives pour les libertés. L'année suivante, la société Nigay SA a effectué une nouvelle demande d'autorisation pour la même finalité, mais a opté pour un dispositif de reconnaissance du réseau veineux des doigts de la main[378]. Ce dispositif a été autorisé par la CNIL.

278. Pour qu'un dispositif biométrique soit considéré comme proportionnel, il doit pouvoir être intégré dans l'architecture de sécurité de l'entreprise et garantir la fiabilité du système envisagé (2°).

[377] CNIL, Délibération n° 2008-447 du 20 nov. 2008 refusant la mise en œuvre par Nigay SA d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, autorisation n° 1271106, disponible sur le site www.legifrance.gouv.fr

[378] CNIL, Délibération n° 2009-128 du 26 fév. 2009 autorisant la mise en œuvre par la société Nigay SA d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux, autorisation n° 1336964, disponible sur le site www.legifrance.gouv.fr

2°. La fiabilité du système envisagé

279. Un système fiable est un système dans lequel il est permis d'avoir confiance. Les salariés doivent être assurés que la collecte des données personnelles pour laquelle ils ont donné leur consentement est sûre, c'est-à-dire que, de l'enrôlement au stockage, le système va garantir, d'une part, l'intégrité des données et, d'autre part, leur anonymat.

Pour qu'un système biométrique soit performant, donc fiable, il faut qu'il soit établi dans un milieu adéquat. Les fournisseurs de produits biométriques peuvent déconseiller l'emploi d'un dispositif, dès lors que l'environnement dans lequel il va être implanté, risque d'altérer ses performances. Ainsi, l'URSSAF de Corse[379] n'a pas pu avoir recours à l'emploi d'un dispositif de reconnaissance par empreintes digitales, car le prestataire de services biométriques estimait que cette technologie risquait de ne pas fonctionner, à cause des variations importantes des températures et de l'hygrométrie. De plus, la CNIL a donné un avis défavorable à l'URSSAF de Corse, car le dispositif biométrique sollicité, paraissait disproportionné par rapport à la finalité du traitement.

Il est permis de se réjouir d'une telle décision, dans la mesure où les prestataires de services biométriques sont attentifs à la fiabilité des dispositifs, au sein de l'environnement de l'entreprise.

280. La subsidiarité et la fiabilité des dispositifs biométriques ne garantissent pas, pour autant, leur usage raisonnable, pourtant indispensable à un traitement proportionnel des données. Les chefs d'entreprise peuvent être tentés de surveiller l'activité de leur personnel et d'outrepasser les finalités pour lesquelles le dispositif a été initialement installé. Il s'agirait, dans ce cas là, d'un usage déraisonnable des dispositifs et donc disproportionné (3°).

[379] CNIL, Délibération n° 02-045 du 18 juin 2002 portant avis sur un projet de décision du directeur de l'URSSAF de la Corse relatif à la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale destiné à contrôler les accès aux locaux professionnels de l'URSSAF, disponible sur le site au www.legifrance.gouv.fr

3°. L'usage raisonnable du dispositif biométrique au regard des finalités du traitement

281. On entend par usage raisonnable, l'emploi scrupuleux d'un dispositif biométrique en corrélation directe et en adéquation parfaite avec les finalités pour lesquelles il a été installé et pour lesquelles il intervient. En pratique, il incombe à la CNIL de s'assurer que la demande de traitement soit bien proportionnelle. Par exemple, la Commission estime qu'un traitement basé sur un dispositif de reconnaissance par empreintes digitales, stocké sur une base de données est proportionnel lorsque les zones protégées par le dispositif sont classées et nécessitent en cas d'accident ou de risques de contamination, une intervention immédiate. Les accès sont restreints et l'identification doit être rapide et fiable.

L'usage raisonnable d'un dispositif biométrique s'apprécie sur la base d'éléments factuels. Il nous semble que la constitution d'une base de données, aussi dangereuse qu'elle soit pour les libertés, semble raisonnable dès lors qu'il n'est pas possible d'envisager un autre mode de stockage pour atteindre la finalité assignée au traitement.

282. Au Canada, le Commissariat à la protection de la vie privée suit un cheminement de pensée proche de celui de la CNIL. Lorsqu'il a été question d'implanter, au sein d'une entreprise canadienne, un système de reconnaissance vocale, aux fins de modification des mots de passe, les employés ont porté l'affaire en justice afin de faire retirer le procédé biométrique qu'ils refusaient. Les salariés devaient appeler un serveur vocal et se soumettre au dispositif de reconnaissance vocale qui permettait de générer des mots de passe. Une fois identifié, le serveur leur fournissait le nouveau mot de passe.

Le Commissaire à la protection de la vie privée a estimé que le principe de proportionnalité devait être interprété, au sens de la loi sur la protection de la vie privée[380], comme l'équilibre entre le droit à la protection des données personnelles des individus et les informations personnelles qu'une entreprise a besoin de collecter, d'utiliser ou de divulguer pour une raison appropriée.[381]

---

[380] Au Canada elle se nomme Personal Information Protection and Electronic Documents Act (PIPEDA)

[381] "*It was noted that the purpose of PIPEDA was to balance the individual's right to privacy with the organization's need to collect, use or disclose personal information for appropriate purposes. This balancing exercise was characterized as one of proportionality (was the loss of proportionate to the benefits the employer*

C'est dans la recherche de ce « juste milieu » que réside toute la difficulté.
Dans l'affaire canadienne le consentement des individus est passé au second plan, le juge a donné raison à l'employeur. Il a estimé que l'empreinte vocale ne révélait pas beaucoup d'informations sur l'individu et qu'il y avait de faibles risques de détournement en authentification.

Ces faits ne sont pas sans rappeler l'autorisation, donnée par la CNIL à la société Michelin, d'installer ce même traitement au sein de l'entreprise[382]. L'usage de ce dispositif est raisonnable, s'il n'est pas utilisé de manière détournée pour identifier les employés et qu'il ne porte pas atteinte à leurs libertés. Le chef d'entreprise doit tenir compte des réticences soulevées par ses salariés et tenter d'apaiser les conflits. Avoir un comportement raisonnable c'est aussi savoir renoncer à la biométrie, dès lors qu'elle est mise en échec par ses utilisateurs. La biométrie apparaît, trop souvent encore, comme une technique d'instrumentalisation du corps humain, asservissant l'individu et la décision du magistrat canadien en faveur de l'entreprise ne change rien à cela. On ne peut s'approprier d'un élément corporel d'une personne, en ce qu'il est l'élément le plus intime de chaque être humain. Une résistance psychologique des salariés aboutit généralement à un échec d'identification.

283. La CNIL est le « garde-fou » des données personnelles des salariés dans l'environnement biométrique. Elle apprécie la proportionnalité du traitement en fonction de la traçabilité du dispositif biométrique déterminé par le responsable de traitement (Section 2).

---

would gain.)" "Biometrics in the workplace – Where to draw the line?" in Personal Information Protection Act Conference of Calgary Alberta, 2006, p. 10

[382] CNIL, Délibération n° 2007-248 du 13 sept. 2007 autorisant la mise en œuvre par la Manufacture française des pneumatiques Michelin d'un traitement automatisé de données à caractère personnel reposant sur un procédé de reconnaissance vocale et ayant pour finalité la gestion des mots de passe, disponible sur le site internet www.legifrance.gouv.fr

Section 2. La prise en compte de la traçabilité de la technologie biométrique

284. L'information sur la traçabilité est généralement employée dans le domaine industriel et commercial. Il s'agit d'une technique servant à suivre un produit tout au long de son processus de production. La traçabilité est souvent évoquée dans le domaine alimentaire et devient même un gage de qualité lorsque le produit possède un label.

Dans le domaine de l' « informatique et des libertés », la traçabilité est employée pour qualifier une technologie (RFID, Biométrie, Géolocalisation) de surveillance. Une technologie traçable est capable de pister les individus dans le temps (grâce à des moteurs de recherche) et dans l'espace (géolocalisation, biométrie, puces RFID). Ces technologies ont pour conséquence de porter atteinte à l'intimité de la vie privée. Une personne peut, à une période de sa vie, s'être épanchée sur un blog ou un réseau social (comme Facebook ou Twitter) et voir ses opinions ou photos le poursuivre des années plus tard. Certains employeurs lancent une recherche sur Google et obtiennent des informations sur leurs candidats à l'embauche.

Dans un premier temps, une technologie traçable fait courir des risques, comme la violation de la vie privée et de l'intimité de la personne, sans oublier que sa liberté d'aller et venir se trouve aussi altérée, par les titres de transports, équipés de puces RFID qui enregistrent les différents passages d'un individu. Dans un deuxième temps, un risque de détournement des données personnelles associées à ces technologies n'est pas anodin. Ces dernières peuvent être capturées par l'intermédiaire du périphérique de stockage des données, si celui-ci est branché en réseau. Le danger de propagation de virus informatiques est plus grand, si plusieurs ordinateurs adoptent ce mode de fonctionnement. C'est la raison pour laquelle il importe d'être particulièrement vigilant avec ces technologies dites « traçables ».

285. Le plus souvent, au sein des entreprises, l'intégration de dispositifs biométriques répond à un besoin de protection qui arrive fréquemment après que l'établissement ait été exposé à un danger (vol de matériel), ou que, tout simplement, l'employeur anticipe ce dernier. Pour cela, il veut se munir d'outils efficaces et fiables, pour sauvegarder les personnes, les locaux et les informations. Il s'agit alors de l'évaluation d'un risque, lié à un défaut ou à une faille dans le système réputé sécurisé. L'argument phare, régulièrement

avancé par les chefs d'entreprise, demeure la sécurité du personnel, des locaux et des biens, de telle sorte que l'usage de la biométrie se développe considérablement. Ce besoin, réel ou illusoire de sécurité justifierait, en général, l'emploi de tels dispositifs de façon préventive, mais malheureusement il arrive quelquefois qu'il soit utilisé de manière intrusive. Les responsables de traitement ne prennent pas toujours le temps de s'interroger, au préalable, sur la subsidiarité, la fiabilité ou la nécessité de l'emploi du dispositif.

286. Dès lors, il est important d'avoir des principes directeurs tels que le principe de proportionnalité afin d'assurer la maîtrise collective de la biométrie en entreprise. Dans le cadre de l'usage de dispositifs de reconnaissance par empreintes digitales, réputés traçables, la CNIL distingue « le fort impératif de sécurité », qui permet la constitution d'une base de données, « du besoin général de sécurisation » utilisé plus fréquemment pour une sécurisation courante (A). En ce qui concerne les autres techniques biométriques, l'enjeu est différent puisque, au vu des connaissances actuelles, les dispositifs ne sont pas traçables. Il convient d'apprécier l'opportunité de l'insertion des dispositifs biométriques et les moyens mis à disposition pour la protection des données personnelles des salariés de l'entreprise (B).

A. Les dispositifs de reconnaissance par empreintes digitales remis en cause par le principe de proportionnalité

287. Parce qu'ils permettent d'identifier une personne au moyen d'éléments corporels, les dispositifs de reconnaissance biométrique par empreintes digitales font l'objet d'une surveillance accrue. Si, de plus, afin d'abaisser le coût engendré par la création de badges personnels, un de ces dispositifs est associé à une base de données, les risques de détournements des données personnelles des salariés augmentent.

Le principe de proportionnalité intervient en biométrie pour pondérer, voire interdire, par le biais de la CNIL, l'usage des dispositifs estimés comme traçables, principalement les dispositifs reposant sur la reconnaissance par empreintes digitales. Une fois la technique biométrique choisie, son degré de traçabilité va être pris en compte. Dès qu'une personne pose ses doigts sur un objet, elle y dépose ses empreintes digitales. Ce sont donc des données

qui laissent des traces et avant qu'elles soient cryptées, le propriétaire de ces dernières n'est pas protégé, lors de la phase d'enrôlement. L'image de l'empreinte digitale n'a, alors, pas encore été traduite en gabarit biométrique. En cas de capture illégale des données à cet instant, le porteur légitime se retrouve « dépossédé » de ses données personnelles. Il ne peut plus, en conséquence, assurer la fiabilité de son identité par ce procédé puisque les données biométriques sont immuables. Il est donc important que les entreprises prennent conscience des dangers de l'usage de ces données biométriques en phase d'identification.

288. La constitution des bases de données biométriques doit être conforme au principe de proportionnalité, par le biais d'un « fort impératif de sécurité » (1°). Dans le cas contraire, la CNIL limite ses autorisations au stockage sur support individualisé lorsqu'il répond à un simple besoin de sécurisation (2°).

1°. Le fort impératif de sécurité mis à mal par le principe de proportionnalité

289. De toutes les catégories de données biométriques existantes à ce jour, l'empreinte digitale est une des données les plus « dangereuses » pour les libertés individuelles[383]. C'est une donnée constituante de l'homme, considérée comme une donnée sensible[384]. Les craintes relatives à ce type de données ne concernent pas tant leur collecte que leur stockage. Pour cette raison, il n'est pas permis de risquer le détournement et la divulgation des données, en laissant se multiplier des bases de données avec, comme but la « facilité d'organisation » au sein de l'entreprise. La CNIL a donc eu recours à la notion de « fort impératif de sécurité », pour déterminer si les atteintes éventuelles sur les données personnelles, occasionnées par la constitution d'une base de données, sont proportionnelles au danger pour lequel la base a été constituée. Les entreprises ont souvent recours à la biométrie pour des raisons de sécurité que nous avons déjà eu l'occasion de développer[385].

---

[383] Supra n°2, l'ADN est aussi une donnée constituante de l'homme qui peut porter atteinte à ses libertés, néanmoins, il ne fait pas l'objet de cette étude.
[384] L'art. 8 I de la loi n° 78-17 du 6 janvier 1978 modifiée énonce « *qu'il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelles de celle-ci.* »
[385] Supra n° 4.

La sécurité recouvre plusieurs acceptions dont la « *situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger, à aucun risque, en particulier d'agression physique, d'accidents, de vol, de détérioration*[386] » ou « *La situation de quelqu'un qui se sent à l'abri de tout danger* ». La première définition, qualifiée « d'objective[387] », peut s'appliquer au monde du travail et c'est celle que nous retiendrons dans le cadre des traitements biométriques en entreprise.

Le fort impératif de sécurité, comme décrit précédemment, suppose l'existence d'un danger inhérent à l'activité de l'entreprise, qui nécessite de recourir à un dispositif de reconnaissance par empreintes digitales, pour lequel le stockage dans une base de données, faciliterait l'accès « *à tout moment et sans délai, pour faire face à des situations d'urgence nécessitant une intervention aussi rapide que possible*[388] ». Les entreprises concernées exercent souvent une activité dangereuse qui peut avoir des répercussions sur la société dans son ensemble, comme c'est le cas, par exemple, des centrales nucléaires. Néanmoins, pour le stockage de données au sein d'une base centralisée, l'existence d'un fort impératif de sécurité ne garantit pas systématiquement l'autorisation de la CNIL car c'est une notion dépendante du principe de proportionnalité.

290. Les systèmes biométriques de reconnaissance par empreintes digitales avec stockage dans une base de données centralisée, sont préférés par les employeurs mais peu appréciés par les commissariats internationaux à la protection des données[389]. Cette préférence, s'explique par le faible coût de la mise en place d'une base de données, comparativement à la fabrication de cartes à puce individuelles sur lesquelles serait stocké le gabarit biométrique de l'empreinte digitale. Pourtant, les traitements de données personnelles qui utilisent ce mode de stockage, sont souvent déclarés disproportionnés au regard des finalités pour lesquelles ces données sont collectées. Dans les affaires qui concernent des dispositifs de reconnaissance par empreinte digitale, le principe de proportionnalité a été, dans la majeure partie des cas, le principe déterminant le refus d'autorisation de la CNIL et ce, même en présence d'un fort impératif de sécurité.

---

[386] Dictionnaire Larousse.
[387] C. Guerrier, « La CNIL et la biométrie », Programme Asphalès, in La sécurité aujourd'hui dans la société de l'information, Contributions réunies et coordonnées par S. Lacour, éd. L'Harmattan, 2007, p. 98
[388] CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, 2007, disponible sur le site internet de la CNIL au www.cnil.fr
[389] Cette affirmation est issue d'un constat personnel basé sur l'étude des jurisprudences européennes, canadiennes, et des pays du Pacifique (Australie et Nouvelle-Zélande).

Reprenons l'exemple de l'URSSAF de Corse[390] qui souhaitait installer dans ses locaux de Bastia et d'Ajaccio, un système d'identification de ses agents, par un dispositif biométrique reposant sur la reconnaissance de l'empreinte digitale. L'impératif était sérieux, puisque l'URSSAF avait essuyé des attentats à la bombe quelques années auparavant. Pour l'usage de ce système, la finalité soulevait « le fort impératif de sécurité » des locaux de l'entreprise. La CNIL a pourtant refusé l'autorisation sur trois points : la configuration des locaux, impropre à l'emploi de la biométrie, l'environnement dans lequel serait implanté le dispositif, comme nous l'avons évoqué précédemment, ainsi que la faculté d'employer un stockage individuel pour parvenir à la finalité de gestion d'accès. Sur la finalité, ce fort impératif de sécurité se matérialise par l'accès « ***d'un nombre limité de personnes*** *à* ***une zone bien déterminée*** *représentant ou contenant* ***un enjeu majeur dépassant l'intérêt strict de l'organisme et*** *ayant trait à la protection de l'intégrité physique des personnes ou à celle des biens et des installations ou à celles de certaines informations*[391] ».

Ce fort impératif de sécurité n'est pas contesté puisqu'il est question d'attentats à la bombe déjà perpétrés quelques années plus tôt. L'intégrité des personnes physiques est concernée puisque les attentats font comme premières victimes des membres de la société civile. Nous considérons que la finalité qui consiste à contrôler les accès à ces locaux est justifiée car le risque n'est pas simplement hypothétique mais bien réel.
Cependant, c'est du point de vue de la fiabilité du dispositif et de la disproportion entre la technologie employée et le choix du mode de stockage des données que l'autorisation a été refusée. Rappelons que selon la CNIL « *il importe de savoir si le système proposé est* ***bien adapté*** *ou* ***est le mieux adapté*** *à la finalité préalablement définie eu égard aux risques qu'il comporte en matière de protection des données à caractère personnel*[392] ».

Choisir un système adapté ou le mieux adapté à la finalité, revient à choisir le dispositif le plus approprié à l'environnement dans lequel il est installé. Dans ce contexte, la CNIL a

[390] CNIL, Délibération n° 02-045 du 18 juin 2002 portant avis sur un projet de décision du directeur de l'URSSAF de la Corse relatif à la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale destiné à contrôler les accès aux locaux professionnels de l'URSSAF. Site Internet www.legifrance.gouv.fr
[391] CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, 2007, disponible sur le site internet www.cnil.fr
[392] Ibid

constaté que la disposition des locaux ne se prêtait pas à l'implantation d'un dispositif biométrique[393].

Par ailleurs, l'environnement extérieur ne permettait pas non plus, de garantir les performances associées à ce dernier. Dans ces circonstances, la finalité ne pouvait être atteinte par ce dispositif[394]. L'apport de la preuve du fort impératif de sécurité ne suffit pas à estimer comme proportionnel, l'usage et la collecte des empreintes digitales. En ce qui concerne l'usage de l'empreinte digitale au sein de l'établissement d'Ajaccio, l'appréciation est bien plus complexe et tient compte de l'environnement extérieur, qui peut contrevenir à l'emploi de la technologie choisie initialement. Les variations de températures et d'hygrométrie ne pouvaient pas garantir la fiabilité du système et la préfecture aurait pu s'interroger préalablement sur la pertinence (environnement, fiabilité et choix raisonnable de la technologie) de l'emploi de cette technique biométrique.

Il importe de s'interroger sur la possibilité d'utiliser un moyen subsidiaire au stockage des données, au sein d'une base centralisée, comme par exemple la possibilité d'opter pour un stockage individuel des données. La CNIL a estimé que « *le recours à un système d'authentification par empreinte digitale dont le gabarit serait inclus dans la carte à puce sans être stocké par ailleurs au niveau du lecteur permettrait de garantir que seules des personnes habilitées et reconnues auraient accès aux locaux de l'URSSAF*[395] ». Cette décision fait application du principe de subsidiarité en vertu duquel, il est préconisé de privilégier la technologie la moins intrusive pour les libertés.

---

[393] La CNIL relate, en effet, que sur la prise en compte de l'environnement dans le choix d'un dispositif biométrique, « *s'agissant de l'antenne de Bastia, la disposition des locaux de l'URSSAF situés sur un étage d'immeuble auquel on ne peut accéder qu'après avoir franchi un hall d'accueil contrôlé par un agent et le faible nombre d'agents concernés (sept personnes) ne paraissaient pas justifier, dans des conditions garantissant la proportionnalité entre l'objectif poursuivi et les moyens mis en œuvre, un dispositif de reconnaissance des empreintes digitales des personnels alors que, de surcrédit, les autres personnes travaillant ou habitant cet immeuble n'y seraient pas soumises. »* Extrait de la délibération CNIL n° 02-045 du 18 juin 2002 portant avis sur un projet de décision du directeur de l'URSSAF de la Corse relatif à la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale destiné à contrôler les accès aux locaux professionnels de l'URSSAF. Site Internet www.legifrance.gouv.fr

[394] « *S'agissant de l'antenne d'Ajaccio,(...) ,* ***les variations locales de température et d'hygrométrie altérant considérablement les performances du système, selon le prestataire lui-même****. Dès lors, la Commission ne peut que constater que ce nouveau dispositif de sécurité serait, en tant que tel, impropre à prévenir le renouvellement d'événements de la nature de ceux dont l'URSSAF d'Ajaccio a déjà été la victime. »* Extrait de la délibération n° 02-045 du 18 juin 2002 précitée, disponible sur le site Internet www.legifrance.gouv.fr

[395] CNIL, Délibération n° 02-045 du 18 juin 2002 précitée, disponible sur le site Internet www.legifrance.gouv.fr

291. La CNIL a rejeté le stockage des empreintes digitales dans une base de données, pour le défaut de proportionnalité notamment pour la société Histoire et patrimoine qui désirait créer une base de données d'empreintes digitales pour « *faciliter l'ouverture des locaux le matin et leur fermeture le soir*[396] », ou pour l'Association Hospitalière de l'Ouest qui souhaitait installer un dispositif de reconnaissance par empreintes digitales avec stockage dans une base de données aux fins « *du contrôle d'accès aux blocs opératoires, salles de réveil, vestiaires des employés et les salles dans lesquelles le matériel coûteux est entreposé*[397] ». Dans ces délibérations, la biométrie n'a qu'un usage secondaire de sécurisation puisqu'elle a été choisie pour sa « *simplicité d'emploi* » ou parce que le dispositif présente des « *facilités d'installation* » et « *permet un accès facile du personnel* ».

La CNIL a donc tout simplement remis en cause le fondement « du fort impératif de sécurité ». Pour ce faire, elle a différencié l'existence d'un fort impératif de sécurité pour lequel il est nécessaire de recourir à un mode de stockage plus sûr, d'un besoin général de sécurisation où l'objectif de sécurisation des locaux est généralement secondaire et pourrait être atteint par une autre solution que la création d'une base de données d'empreintes digitales.

Il existe deux étapes dans le raisonnement de la CNIL. La première vise à reconnaître l'existence du fort impératif de sécurité avec les caractères qu'elle décrit dans sa communication de 2007. Une fois ce dernier admis, la deuxième étape consiste à observer objectivement l'environnement, la fiabilité et l'aspect raisonnable du choix du dispositif biométrique. Nous constatons que le fort impératif de sécurité ne suffit pas à lui seul à déterminer si un traitement est, ou non, proportionné.

Au-delà de la simple finalité de traitement, ces deux « verrous » permettent de faire une étude objective des dossiers. Si la CNIL avait largement admis le stockage au sein des bases de données, le remède aurait été pire que le mal. En pensant sécuriser les locaux et sauvegarder

[396] CNIL, Délibération n° 2008-233 du 17 juil. 2008 refusant la mise en œuvre par la société Histoire et patrimoine d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des accès aux locaux, autorisation n°1296677, disponible au www.legifrance.gouv.fr

[397] CNIL, Délibération n° 2008-328 du 11 sept. 2008 refusant la mise en œuvre par l'Association Hospitalière de l'Ouest d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, autorisation n°1244573, disponible sur le site internet www.legifrance.gouv.fr

les droits des salariés, la diffusion non maîtrisée des bases de données, associée à leur croisement aurait pu avoir pour conséquences, en cas de détournement, la perte de l'anonymat des personnes ainsi que l'atteinte à leur vie privée. Dès lors, il aurait été impossible pour les salariés, de s'identifier de façon fiable, par un dispositif biométrique. Nous ne savons pas comment, dans l'avenir, les dispositifs biométriques vont se développer dans la vie courante des individus, mais il importe, dès à présent, que soyons tous vigilants. En cas de dépossession de ses données personnelles, le salarié ne pourrait plus s'identifier avec fiabilité par ce procédé dans son travail comme dans tous les gestes de la vie courante. Les conséquences ne sont pas simplement circonscrites à la vie professionnelle mais touchent aussi à la vie privée.

292. Si la décision d'opter pour un dispositif biométrique est importante dans la protection des données personnelles, le choix du mode de stockage l'est tout autant. En effet, la CNIL apprécie la proportionnalité d'un traitement en partie au regard du mode de stockage des données. Si le responsable de traitement a opté pour une forme de stockage peu respectueuse des données personnelles des salariés, la CNIL refusera de donner son autorisation (2°).

2°. Le mode de stockage mis à l'épreuve par principe de proportionnalité

293. Avec l'appréciation du fort impératif de sécurité, le mode de stockage des empreintes digitales est un second élément à prendre en compte pour déterminer la proportionnalité d'un traitement. En 2005, un rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, a abordé les questions liées aux architectures de systèmes et aux choix opérés quant à la collecte des données. Il en ressort, que « *le choix entre l'enrôlement de l'image complète d'une caractéristique biométrique ou d'un extrait sous la forme d'un gabarit se réfère au principe selon lequel il ne faut pas collecter plus de données que celles nécessaires à la finalité pour laquelle ces données sont collectées*[398] ».

[398] Document du secrétariat du Conseil de l'Europe, « Les critères de sélection de l'architecture du système », Partie III paragraphes n° 43 et 44 pp. 10, Rapport disponible sur le site Internet de la Commission Européenne au http://www.coe.int/

294. S'il est vrai que l'empreinte digitale suscite des craintes en tant que technique, le risque réel vient peut être plus de la manière dont les données sont sauvegardées. Il est intéressant, sur cette question, de comparer les éléments de réponse, tant sur le plan national (2-1) qu'international (2-2).

2-1. Les éléments de réponse sur le plan national

295. Les problématiques liées à la biométrie dans les entreprises tiennent plus à la perméabilité des outils cryptographiques utilisés pour stocker les données personnelles, qu'aux technologies biométriques elles-mêmes[399]. Les solutions cryptographiques n'étant pas encore satisfaisantes, le stockage individuel des empreintes digitales est largement préféré par la CNIL aux bases de données.

La CNIL rappelle, dans la communication relative à la mise en œuvre de dispositifs de reconnaissance par empreintes digitales, avec stockage dans une base de données, que *« dans le cas d'un stockage sur support individuel (tel une carte à puce ou clé USB), exclusivement détenu par la personne concernée, la personne a la* ***maîtrise*** *de sa donnée biométrique. Celle-ci reste sous sa responsabilité et ne peut être utilisée pour l'identifier à son insu. En cas de vol ou de perte du support de stockage, on ne peut avoir accès qu'à une seule donnée biométrique éventuellement associée à l'identité de la personne*[400] ».

Par « *maîtrise* » de la donnée biométrique, il faut comprendre que la personne a une détention permanente et intégrale sur cette dernière. Elle a connaissance du contenu des données stockées, de la fréquence d'utilisation mais aussi des raisons pour lesquelles intervient le traitement. Aucun usage ne peut être effectué à son insu, sauf en cas de perte ou de vol.
Là encore, elle peut être tenue pour seule responsable des dommages occasionnés sur le support. Le stockage d'empreintes digitales sur un support individualisé est considéré généralement comme proportionnel, dès lors que la finalité pour laquelle le dispositif est

[399] V. J-F. Mainguet, « Fingerprints hashing », Encyclopedia of biometrics, Springer, 2009, pp. 543; A. Cavoukian, M. Snijder, "The relevance of untraceable biometrics and biometric encryption: a discussion of biometrics for authentication purposes", Information and privacy commissioner Ontario (Canada), August 2009, disponible sur le site www.eubiometricsgroup.eu
[400] CNIL, Communication relative au système de reconnaissance par empreinte digitale avec stockage dans une base de données, 2007, disponible sur le site www.cnil.fr

envisagé concerne le contrôle d'accès. C'est pourquoi nous ne reviendrons pas sur ces questions dans ce paragraphe et renvoyons le propos aux paragraphes précédents[401]. En revanche, lorsqu'il est question d'employer cette technologie pour d'autres finalités (par exemple pour la gestion des horaires) la CNIL, ou les juges du fond ne sont pas enclins à autoriser ce type de traitement de données personnelles.

296. Le tribunal de grande instance de Paris a eu l'opportunité de se prononcer, en matière de biométrie, dans le cadre d'un contentieux opposant la société Effia services, au comité d'entreprise de cette dernière ainsi qu'à la Fédération des syndicats Sud Rail[402]. Il s'agit du premier jugement français, touchant la biométrie, dans laquelle une entreprise est visée.

La société Effia Services avait décidé de mettre en place, au sein de son entreprise, une pointeuse biométrique permettant de contrôler le temps de présence des salariés. A l'époque des faits, les entreprises privées étaient simplement soumises à la procédure de déclaration du traitement auprès de la CNIL, sans que cette dernière, puisse s'opposer au traitement des données biométriques. Du point de vue de la procédure, la société s'était conformée aux obligations d'information des articles 32 de la loi Informatique et libertés et L. 1222-4 du Code du travail ainsi qu'à l'obligation de consultation de l'article L. 2323-13 du Code du travail. Par ailleurs, elle avait procédé à la déclaration de son traitement auprès de la Commission. Toutefois, le comité d'entreprise de la société, ainsi que le syndicat Sud Rail, ont engagé une action en justice sur deux griefs : le premier dénonçait des conditions d'implantation du dispositif, le second s'attaquait au caractère disproportionné de l'atteinte à leurs libertés individuelles.

Le tribunal a rejeté la première série d'arguments puisque la société s'était conformée à la procédure de déclaration et d'information du personnel. Cependant, le tribunal a ordonné que cette pointeuse soit retirée en précisant que « *l'empreinte digitale, même partielle, constitue une donnée biométrique morphologique qui permet d'identifier les traits physiques spécifiques qui sont uniques et permanents pour chaque individu* ». Le tribunal considère que « *l'objectif poursuivi (à savoir le contrôle des horaires de travail) n'est pas de nature à*

[401] Supra n° 194 et s.
[402] TGI Paris section sociale, 1ère chambre, 19 avril 2005, RG n° 05/00382 ou sur le site internet www.legalis.net

justifier la constitution d'une base de données d'empreintes digitales des personnels […], ***le traitement pris dans son ensemble n'apparaissant ni adapté ni proportionné au but recherché*** ».

297. Cette première décision judiciaire fait ressortir quelques imprécisions d'ordre technique, car seule, l'empreinte digitale partielle du salarié était stockée sur une carte à puce accompagnée d'un numéro de badge que le lecteur devait lire à l'arrivée et au départ du salarié. Le salarié devait présenter sa carte sur le lecteur et appliquer son doigt pour s'authentifier. Il n'était donc pas question, pour la société Effia services, de constituer une base de données d'empreintes digitales et certains commentateurs n'ont pas manqué de soulever l'erreur des magistrats[403]. La finalité du traitement consistait à améliorer la gestion des fiches de paie ainsi que le contrôle des horaires des salariés, puisque le système de pointeuse traditionnel ne permettait pas de garantir que le détenteur du badge en était le réel propriétaire.

298. Par ailleurs, le tribunal de grande instance de Paris, s'est fondé sur le code du travail en estimant qu'au regard de l'article L. 1121-1[404], l'usage d'une pointeuse biométrique pour contrôler le temps de travail était inadapté et disproportionné au but recherché. S'agit-il d'une application du principe de précaution en vertu duquel, en l'absence de recul sur les effets d'une technologie, il est préférable d'en limiter l'usage[405] ? Ou bien, peut-on réellement considérer que l'usage de l'empreinte digitale pour gérer les horaires des salariés est une restriction aux droits et libertés individuelles et collectives au sein d'une entreprise ?

L'article 1121-1 du Code du travail selon lequel « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* » peut faire l'objet de plusieurs interprétations. Ce texte, initialement inspiré de la jurisprudence du Conseil d'Etat en matière de règlement intérieur[406], a été étendu, suite au rapport rendu par

[403] M.-L. Laffaire et T. Elm, « Biométrie, la première décision d'une longue série » Expertises des systèmes d'information, août/septembre 2005, p. 299 et s.
[404] Ancien art. L. 120-2 du Code du travail.
[405] E. Barby « La biométrie dans l'entreprise : quand l'innovation se heurte à la culture de l'interdit », Gazette du Palais n°202, 21 juillet 2005, p. 7.
[406] CE Section, 16 mars 1962, Cie des tramways électriques d'Oran, Rec. p. 176, et JCP 1962 II, 12912, note J. Savatier.

Gérard Lyon-Caen[407], au droit du travail par la loi du 31 décembre 1992[408]. Le législateur a rédigé l'article L. 120-2 du Code du travail[409] à la lumière de la jurisprudence administrative. Le Conseil d'Etat exige, pour la légalité d'une mesure de police, la réunion de trois éléments : l'interdiction ne doit pas être totale « *la liberté est la règle, et la restriction de police l'exception*[410] », la restriction est nécessaire « *pour atteindre le but recherché*[411] » et elle doit être proportionnelle.

Selon Gérard Lyon-Caen « *les sujétions imposées à la personne du travailleur ne sont justifiées que dans la mesure où elles sont nécessaires au bon fonctionnement de l'entreprise*[412] ». Les droits et libertés ne peuvent subir que des restrictions, donc, une interdiction totale de l'employeur serait illégale. Ainsi, pour les clauses de non-concurrence, la mesure doit être indispensable à la sauvegarde des intérêts de l'entreprise[413]. Par ailleurs, les restrictions imposées par le chef d'entreprise à ses salariés doivent être justifiées. Suite à une série d'attentats, un employeur a imposé à tout son personnel la fouille des sacs à l'entrée de l'entreprise. Un salarié s'est opposé à cette mesure. La chambre sociale de la Cour de cassation a estimé que la restriction était justifiée[414]. Enfin, les restrictions apportées aux droits et libertés doivent être proportionnées au but recherché. En reprenant les faits de l'arrêt précédent, le juge a estimé la mesure proportionnelle car elle visait, suite à des attentats, la seule ouverture des sacs et non leur fouille.

Si nous revenons au cas de l'affaire Effia services, les salariés n'étaient pas privés de leur liberté d'aller et de venir et leurs données personnelles étaient protégées puisqu'elles étaient stockées partiellement sur un support individuel dont ils avaient la maîtrise. Nous n'estimons donc pas que l'emploi d'un dispositif de reconnaissance par empreinte digitale ait constitué alors une restriction aux libertés individuelles des salariés, puisqu'il assurait la protection des données personnelles des individus. De plus, avant de procéder à la collecte des données personnelles, l'employeur avait satisfait aux obligations d'information, de consultation des

---

[407] G. Lyon-Caen, Les libertés publiques et l'emploi, Rapp. min. Travail, emploi et formation professionnelle : La Documentation française, Paris, 1992.

[408] Loi n° 92-1446 du 31 déc. 1992 relative à l'emploi, au développement du travail à temps partiel et à l'assurance chômage, JO n° 1, 1er janvier 1993.

[409] Actuel article L. 1121-1 du Code du travail issu de la loi n° 2008-67 du 21 janv. 2008 ratifiant l'ordonnance n° 2007-329 du 12 mars 2007 relative au Code du travail.

[410] Conseil d'Etat, 10 août 1917 n° 59855, arrêt Baldy, Recueil Lebon 1917, p. 000 ; Rec. CE, p. 638

[411] Conseil d'Etat le 1er fév.1980, Dr social 1980 p 310 concl. Bacquet

[412] P. Waquet, L'entreprise et les libertés du salarié, collection droit vivant, éditions Liaisons, 2003, p. 87, extrait du rapport de G. Lyon-Caen, Les libertés publiques et l'emploi.

[413] Voir notamment : Cass. soc., 14 mai 1992, n° 89-45.300, Bull. civ. V, n° 309.

[414] Cass. Soc., 3 avr. 2001, D. Soc. 2001, p. 675, obs. Gauriau

organes représentatifs et avait donc obtenu le consentement des salariés. Plusieurs observateurs n'ont pas réservé un bon accueil à cette décision, notamment parce que cette interdiction était « *réductrice et regrettable (...) Il semble que l'on veuille aujourd'hui éviter les risques en posant un interdit*[415] » et qu'elle aurait pu avoir pour conséquences d'« *entraver de façon excessive le développement de pratiques qui, maniées avec la prudence qui s'impose, peuvent se révéler d'une grande utilité*[416] ».

299. En matière de contrôle d'accès, la CNIL autorise le stockage des empreintes digitales intégrales sur un support individualisé. Elle a déjà accepté ce type de traitement, dans le cadre de la gestion des horaires, associé à un système de contrôle d'accès. Par analogie, il serait envisageable d'estimer comme proportionnel le fait de conserver, sur une carte de stockage, une empreinte digitale partielle, ayant pour finalité, la gestion des horaires et les emplois du temps sur le lieu de travail. Aucun stockage n'est établi dans la mémoire du lecteur qui reconnaît simplement le numéro de badge du salarié. Mais, en aucun cas, la donnée biométrique de ce dernier n'y est conservée. La CNIL n'a pas eu l'occasion de se prononcer sur cette affaire, mais à cette époque, elle avait rendu des délibérations sur l'emploi de techniques de reconnaissance par empreintes digitales dans le cadre de la gestion des horaires de travail[417].

Antérieurement à cette décision, la CNIL avait refusé l'utilisation des pointeuses biométriques. Cette autorisation avait été demandée par la préfecture de l'Hérault[418], puis par la mairie de Goussainville [419], deux ans plus tard. Il est nécessaire de préciser que ces deux décisions concernaient le stockage des empreintes digitales dans une base de données. Comme nous l'avons vu précédemment, quelques mois après la décision rendue par le tribunal de grande instance de Paris, une délibération rendue par la Commission concernant la société Brisach SAS a autorisé la mise en œuvre d'un traitement automatisé de données à

[415] E. Barby « La biométrie dans l'entreprise : quand l'innovation se heurte à la culture de l'interdit », Gazette du Palais n° 202, 21 juil. 2005, p. 7.
[416] A. Lepage, « La biométrie refoulée de l'entreprise », Communication commerce électronique n°10, Octobre 2005, comm. 164.
[417] Cf. supra p. 87 et suivants
[418] CNIL, Délibération n° 00-057 du 16 nov. 2000 portant avis sur un projet d'arrêté présenté par le préfet de l'Hérault concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion du temps de travail des agents de la préfecture, disponible au www.legifrance.gouv.fr
[419] CNIL, Délibération n° 02-033 du 23 avr. 2002 relative à la demande d'avis présentée par la mairie de Goussainville concernant la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion des horaires de travail des personnels communaux, disponible sur le site www.legifrance.gouv.fr

caractère personnel qui reposent sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales avec le contrôle des horaires, pour finalité[420]. La société Brisach ne dissimulait pas ses intentions d'employer ce dispositif, en premier lieu pour gérer les horaires des salariés et ensuite pour assurer le contrôle d'accès aux locaux de l'entreprise. Il y a donc ici, deux finalités pour un seul dispositif envisagé[421]. A l'encontre des autres décisions de la CNIL, la société Brisach a obtenu son autorisation, car elle n'a pas cherché à constituer une base de données biométriques, étant donné qu'elle avait déjà recours au stockage individuel des données. Si elle avait souhaité recourir à ce mode de stockage elle aurait dû faire valoir « un fort impératif de sécurité », ce qui n'est pas le cas.

Toutefois, en émettant quelques réserves, et compte tenu de la singularité de la délibération, on peut en déduire qu'un dispositif de reconnaissance par empreinte digitale, et dont la finalité est la gestion des horaires des salariés, peut être proportionnel pour plusieurs raisons. D'abord s'il est doublé d'une finalité visant à renforcer la sécurité des biens, des personnes et des données traitées sur les postes de la salle informatique mais aussi, si le stockage est raisonnablement effectué sur un support individuel, garantissant au porteur une maîtrise totale de ses données personnelles. Lorsque le traitement n'est pas doublé d'une finalité de contrôle d'accès, la CNIL a quelques réticences, touchant sans doute à l'éthique, à donner ce type d'autorisation.

300. D'autres pays ont eu à s'interroger sur la proportionnalité de l'usage de l'empreinte digitale et de ses modes de stockage en fonction des finalités d'utilisation (2-2).

[420] CNIL, Délibération n° 2006-069 du 16 mars 2006 portant autorisation de la mise en œuvre par la société Brisach SAS d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalités le contrôle des horaires et le contrôle de l'accès aux locaux, disponible sur le site www.legifrance.gouv.fr
[421] Supra n° 198

2-2 Les éléments de réponse en droit comparé

301. Le droit comparé peut être une piste de réflexion sur ce sujet. Il semblerait qu'il y ait un consensus « informatique et libertés » entre les pays occidentaux. Tous conseillent la prudence en matière d'usage et de stockage des empreintes digitales. La Suisse, tout comme la France, reconnaît la dangerosité de l'empreinte digitale, surtout lorsqu'elle est stockée dans une base de données centralisée. Toutefois, en matière de gestion des horaires, le Préposé fédéral suisse à la protection des données n'est pas opposé à l'usage de l'empreinte digitale lorsque le stockage est effectué sur un support individuel et dans la mesure où seules, les minuties sont prélevées[422]. En effet, il est difficilement possible de reconstituer l'image intégrale de l'empreinte digitale à partir des seules minuties, « *le traitement de l'échantillon de référence dans une carte à puce à usage exclusif présentée par chaque employé lors du timbrage représente une solution plus proportionnée et donc compatible avec la législation sur la protection des données*[423] ». Dans la mesure où les salariés acceptent ce dispositif, que leurs données sont protégées et qu'ils en ont la détention, nous pensons que cette position est cohérente.

Outre-Atlantique, la gestion des horaires des salariés par l'emploi de dispositifs de reconnaissance par empreintes digitales a été l'objet d'un conflit, entre l'employeur et ses salariés. Ce fut le cas au Canada, dans l'affaire IKO Industries Ltd. contre USWA[424]. La société IKO souhaitait remplacer l'ancien système de gestion des horaires des employés (pointeuse badge) par une pointeuse biométrique. Le syndicat des salariés s'est vivement opposé à l'implantation de ce dispositif. Conformément à la loi de ce pays, un arbitre a dû intervenir pour étudier le dossier avant qu'il soit soumis à la Cour. Elle a dû se prononcer sur le bien fondé de l'implantation d'une pointeuse biométrique, en confrontant les différents arguments des deux parties. Pour l'employeur, il n'y avait pas d'atteinte à la vie privée. Il a invoqué le droit de gestion de sa propre entreprise, qui lui a permis, dans l'affaire citée plus haut, d'implanter un dispositif de reconnaissance vocale, servant à générer des mots de passe. Il a assuré que le système implanté était fiable, car les gabarits n'étaient ni enregistrés, ni

[422]Les minuties sont des points de repère situés sur les empreintes digitales. Ces points sont employés, de façon méthodique, pour comparer deux empreintes digitales.
[423] Rapport d'activité de l'année 2004-2005 du Préposé fédéral suisse à la protection des données, « Le contrôle des présences à l'aide des empreintes digitales, p. 63 et suivantes. Disponible sur le Site Internet http://www.edoeb.admin.ch/index.html?lang=fr
[424] Personal Information Protection Act Conference, April 2006, Calgary, Alberta "Biometrics in the workplace – Where to draw the line?" p. 13

conservés et que seuls, six employés chargés de la maintenance pouvaient répliquer l'image utilisée pour générer le gabarit biométrique, ce qu'ils ne pouvaient faire, à des fins étrangères à la finalité assignée au dispositif.

Le syndicat a aussi avancé ses arguments. Pour lui, le dispositif avait certainement une autre mission que le contrôle du temps de présence des salariés sur le lieu de travail. Ensuite, les employés n'avaient pas la maîtrise des données personnelles collectées, qui avaient été relevées sans leur consentement. Enfin, ils ont émis des réserves quant à la fiabilité du système et la possibilité d'un détournement des données à des fins étrangères, par un hacker.

L'arbitre a rappelé qu'il était nécessaire de mettre en balance le droit de gestion de l'employeur sur son entreprise avec la protection des données personnelles des salariés. Cependant, dans son argumentation, l'employeur n'a pas apporté la preuve de l'existence de fraudes multiples, qui prouverait le besoin de ce dispositif nécessaire à cette finalité. En conséquence, l'autorisation est refusée. La Cour a précisé que sa décision ne devait pas être considérée comme une mise à l'index de la biométrie sur un lieu de travail, mais, pour que l'on autorise sa mise en place, il était nécessaire que l'employeur apporte suffisamment de preuves, justifiant la finalité de l'utilisation d'un dispositif de reconnaissance par empreintes digitales.

302. Les avis sont donc partagés sur la question. La plupart des Etats refusent, pour le moment, d'autoriser les entreprises à contrôler les horaires par l'usage de l'empreinte digitale. Cependant, dans les faits, certaines entreprises ont la faculté de détourner la finalité de leur dispositif biométrique, utilisé pour le contrôle d'accès en pointeuse biométrique de gestion des horaires, puisque les historiques de passage, au moment du contrôle d'accès, sont sauvegardés.

303. Pour juger de la pertinence de l'emploi de techniques biométriques réputées « sans traces », la CNIL se fonde sur le principe de proportionnalité du mode de stockage des données (B).

B. Les techniques biométriques « sans traces » proportionnelles

304. Si l'empreinte digitale génère d'importantes interrogations en termes de protection des données, les autres techniques de reconnaissance biométrique sont moins susceptibles d'entraîner des difficultés. En l'état des connaissances actuelles, ces technologies sont réputées « sans traces », ce qui a pour conséquence, de favoriser leur développement au sein des entreprises. L'absence de traçabilité de ces dispositifs amène la CNIL à considérer leur usage, généralement comme proportionnel aux finalités pour lesquelles ils sont installés mais dans des conditions précises. La traçabilité d'un dispositif reste, encore et toujours, le point d'ancrage qui permet d'apprécier le principe de proportionnalité.

305. Le critère de proportionnalité est généralement admis pour les dispositifs de reconnaissance de la géométrie de la main (1°), pour les dispositifs du réseau veineux des doigts de la main (2°) ainsi que pour les dispositifs de reconnaissance vocale (3°).

1°. Le dispositif de reconnaissance du contour de la main

306. Ce dispositif est réputé par la CNIL comme étant « sans traces »[425], compte tenu des connaissances actuelles sur cette technologie, car il ne comporte pas de danger de détournement des données personnelles. Cette technique a eu un grand succès dans le début des années 2000. Succès qui se justifie d'abord par le refus de la CNIL, d'autoriser l'emploi de l'empreinte digitale, il fallait donc très vite, trouver une technique biométrique de substitution « autorisée ». Ensuite il y a l'attrait suscité par ce dispositif qui, de par sa facilité de mise en œuvre juridique ne nécessite qu'une autorisation unique[426]. Il suffit simplement de procéder à la déclaration du dispositif sans demander préalablement l'autorisation à la CNIL.
Le musée du Louvre a été le premier établissement à solliciter l'avis de la CNIL sur le projet qui tend à l'implantation de ce type de dispositif avec, pour finalités, la sécurité des œuvres

[425] CNIL, 21ième rapport d'activité 2000, Chapitre 4 – Les contrôles d'accès par biométrie, p. 102 et suivantes, disponible sur le site internet de la CNIL au www.cnil.fr
[426] CNIL, Délibération n° 2006-101 du 27 avr. 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail, disponible sur le site www.legifrance.gouv.fr

d'art et le contrôle des horaires des salariés, ainsi que celui des entreprises sous-traitantes[427]. Les seules informations conservées sont l'identité de la personne et ses heures de passage. La durée de conservation des données est d'une année, conformément à l'obligation qu'ont les entreprises de prouver les horaires de travail de leurs salariés, en cas de contrôle par l'inspection du travail. Les données collectées ont été déclarées adéquates, pertinentes et non excessives dans leur durée de conservation et traitement ultérieur. En conséquence, la CNIL a donné un avis favorable.

Pour s'assurer que le dispositif biométrique est bien proportionnel aux finalités pour lesquelles il est implanté, la CNIL étudie la finalité du traitement en fonction de la technologie choisie. Il importe aussi d'apprécier à la fois la qualité des données traitées ainsi que le choix de la technique en fonction de la traçabilité du dispositif.

En ce qui concerne les données traitées, nous rappelons qu'elles doivent être « *adéquates, pertinentes et non excessives* » comme l'énonce l'article 6 3° de la loi 78-17 du 6 janvier 1978 modifiée. Les données collectées puis traitées doivent revêtir les caractères précédemment énoncés pour que le traitement soit considéré comme proportionnel[428].

Pour ce type de dispositif, la CNIL a admis qu'était proportionnée la collecte des données suivantes :

- Données identifiantes de l'individu (nom, prénom)
- Données d'ordre professionnel : numéro de matricule ou code personnel associé
- Historique des passages et temps de présence lorsqu'il s'agit de contrôler les horaires
- Données de déplacement comme l'immatriculation du véhicule s'il s'agit d'un accès au parking[429].

Les données présentées ci-dessus sont proportionnelles en ce qu'elles n'apportent pas plus d'informations sur la personne que ce qu'il est nécessaire de récolter pour l'identifier et interconnecter des fichiers, pour le bon fonctionnement de l'organisation de l'entreprise.

---

[427] CNIL, Délibération n° 01-006 du 25 janv. 2001 portant avis sur un projet de décision présenté par l'établissement public du musée du Louvre concernant un traitement de contrôle des accès et des horaires de certains personnels par la reconnaissance du contour de la main, disponible sur le site www.legifrance.gouv.fr

[428] Supra n° 264 et s.

[429] CNIL, Délibération n° 01-006 du 25 janv. 2001 précitée

En ce qui concerne la traçabilité de la technologie, le dispositif de reconnaissance du contour de la main, est une technologie considérée, en l'état des connaissances actuelles, comme ne laissant pas de traces. Toutefois, même en l'absence de traçabilité des techniques, en 2005, la CNIL a refusé d'autoriser la constitution d'une base de données de gabarit du contour de la main, ayant pour finalité la gestion des horaires des salariés[430]. Elle a estimé que cette finalité, tout en étant légitime, ne pouvait aboutir à la collecte massive des données pour des raisons d'organisation ou de convenance de l'entreprise.

Le critère de traçabilité a fait place au mode de stockage choisi par l'entreprise. La CNIL s'attache, au-delà de la traçabilité du dispositif, à limiter la propagation des données. La constitution de bases de données, biométriques ou non, doit être limitée. La constitution d'une base de données est soumise à la conjonction de circonstances exceptionnelles[431].

307. Cette « doctrine » n'a pas été modifiée puisque l'autorisation unique n°AU-007[432] a permis aux entreprises d'implanter un dispositif biométrique reposant sur la reconnaissance du contour de la main avec, pour finalité, la gestion des horaires de travail, le

[430] Cinq délibérations ont été rendues le même jour. Elles visaient la constitution de bases de données du gabarit du contour de la main ayant pour finalité la gestion des horaires des salariés, disponible sur le site www.legifrance.gouv.fr

- Délibération 2005-035 du 17 fév. 2005. Délibération portant refus d'autorisation de la mise en œuvre par la société MFG Education d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés.

- Délibération 2005-037 du 17 fév. 2005. Délibération portant refus d'autorisation de la mise en œuvre par la mairie des Sables d'Olonne d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés.

- Délibération 2005-036 du 17 fév. 2005. Délibération portant refus d'autorisation de la mise en œuvre par la société Paris Monitoring d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés.

- Délibération 2005-034 du 17 fév. 2005. Délibération portant refus d'autorisation de la mise en œuvre par la société UCOM d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés.

- Délibération 2005-031 du 17 fév. 2005. Délibération portant refus d'autorisation de la mise en œuvre par la société UTEL d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés.

[431] Supra n° 226 et s.

[432] CNIL, Délibération n° 2006-101 du 27 avr. 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail, disponible au www.legifrance.gouv.fr

contrôle d'accès ainsi que le contrôle d'accès au restaurant d'entreprise. Les données sont stockées sur un support individualisé. La CNIL n'a pas souhaité généraliser la constitution d'une base de données et préfère apprécier sa pertinence au cas par cas. Elle ne l'interdit pas mais réserve cette solution aux circonstances exceptionnelles.

D'autres autorités de protection des données prennent la précaution de privilégier un stockage individuel des données, sans céder aux pressions opérées par les syndicats d'employés pour ne pas utiliser de dispositifs biométriques. Les autorités de protection des données n'entendent ni prohiber l'emploi de la biométrie ni freiner son développement, mais de responsabiliser son implantation au sein des entreprises. Au Canada, dans l'affaire Cascadia Terminal contre G.W.U[433] un litige, entre l'employeur et le syndicat des employés, a conduit à un arbitrage dans lequel l'arbitre a estimé que l'emploi d'un dispositif de reconnaissance de la main aux fins de gestion des horaires, sans constitution de base de données, était proportionné à la finalité et ne contrevenait ni à la protection des données personnelles, ni à la vie privée des salariés.[434] Pour fonder sa décision, il a relevé que ce dispositif était nécessaire à la bonne gestion de l'entreprise et qu'il ne contrevenait pas aux droits et libertés des salariés.

308. L'industrie, dans le domaine biométrique, se développe rapidement. Ainsi, les dispositifs du contour de la main sont entrés en « concurrence » au sein des entreprises, avec les dispositifs de reconnaissance du réseau veineux des doigts ou de la paume de la main. (2°)

[433] Affaire citée dans le document de Gary T Clarke "Biometrics in the workplace: Where to draw the line?", Personnal Information Protection Act Conference, Calgary, 26 and 27 April 2006, p. 7.

[434] "*Arbitrator ready concluded that the employer had the right to change the timekeeping system and implement a new one and that the collective agreement did not fetter this right. In reaching this conclusion he considered the following four factors:*

- *The purpose of the practice*
- *The impact of removing or continuing the practice*
- *The day-to-day efficiency of the operation; and*
- *The impact on employees (...)*

In the result, he concluded that the employer could move to a new timekeeping system whatever that system might be, subject only to the rising of valid concerns and the employer being willing to listen to those concerns."

2°. Reconnaissance du réseau veineux des doigts de la main

309. La technique de reconnaissance du réseau veineux des doigts de la main possède, à ce jour, d'excellents résultats techniques et conserve l'avantage d'être, en l'état des connaissances actuelles, une technologie biométrique « sans traces ». Depuis l'année 2007, la CNIL constate une augmentation des demandes tendant à l'emploi de cette technique pour la finalité de contrôle d'accès aux locaux de l'entreprise.
L'engouement pour ce dispositif s'explique, en premier lieu, par la difficulté pour les entreprises d'intégrer, au sein de leur architecture de sécurité, des dispositifs de reconnaissance par empreintes digitales et, en second lieu, par la récente autorisation unique n°AU-019, qui permet l'emploi d'un système de reconnaissance du réseau veineux des doigts de la main et qui a pour finalité le contrôle d'accès aux locaux sur les lieux de travail[435].

L'autorisation la plus représentative de cet engouement est celle du Graduate Management Admission Council (GMAC), organisateur de l'examen international de gestion et de management appelé GMAT. Le GMAC a saisi la CNIL d'une demande de traitement automatisé de données personnelles qui repose sur un dispositif de reconnaissance du réseau veineux de la paume de la main, avec pour finalité, le contrôle d'accès à des salles d'examen dans le but d'empêcher toute fraude[436]. Le GMAC souhaitait, par ailleurs, conserver les données au sein d'une base centralisée, hébergée aux Etats-Unis. Alors que la constitution de bases de données biométriques (d'empreintes digitales) est habituellement conditionnée à l'exigence d'un fort impératif de sécurité dépassant l'intérêt strict de l'organisme, il importait de déterminer si le traitement autorisé par la CNIL était proportionnel. Pour juger du caractère proportionnel du dispositif, la CNIL a, d'abord, apprécié la traçabilité de la technologie par rapport à la finalité pour laquelle le dispositif est envisagé (2-1) et, ensuite elle a jugé la qualité des données traitées (2-2). Enfin, la CNIL a dû apprécier la pertinence du mode de

[435] CNIL, Autorisation unique AU-019 - Délibération n° 2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail, disponible sur le site www.legifrance.gouv.fr
[436] CNIL, Délibération n° 2009-360 du 18 juin 2009 autorisant la mise en œuvre par le Graduate Management Admission Council (GMAC) représenté par Pearson Education France d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux de la paume de la main et ayant pour finalité de contrôler l'accès à des salles d'examen et d'empêcher la substitution de candidat à l'examen GMAT, demande d'autorisation n°1323460, disponible sur le site www.legifrance.gouv.fr

stockage des données, en l'occurrence la constitution d'une base de données biométriques (2-3).

2-1 La traçabilité de la technologie

310. Comme nous l'avons dit précédemment, les traces sont des marques laissées par les doigts comme les empreintes digitales par exemple. Dans un dispositif de reconnaissance du réseau veineux des doigts de la main, l'objectif n'est pas de relever les traces des doigts ou de la paume mais de relever l'entrelacement des vaisseaux de la main, « caché », puisqu'il se trouve l'intérieur du corps[437]. Cet entrelacement est unique pour chaque individu et garantit ainsi au dispositif, une fiabilité supérieure aux dispositifs de reconnaissance par empreintes digitales, du fait de l'inexistence du facteur environnemental[438].

Dans ce cas d'espèce, l'usage d'un dispositif biométrique semblait nécessaire, face à l'inefficacité des procédés précédents et à l'augmentation des fraudes à l'identité qui pouvaient remettre en cause la qualité du diplôme obtenu. Afin de maintenir la crédibilité de cet examen, il convenait d'avoir recours à la biométrie. Deux finalités ont été avancées. La première visait à la vérification biométrique de l'identité des participants en début de session, la seconde avait pour but le contrôle, par comparaison, des gabarits biométriques entre eux, au sein de la base centrale, afin de vérifier qu'une même personne ne se présente pas sous deux identités distinctes au GMAT.

311. Un certain nombre de données ont été collectées et il importe d'en évaluer la pertinence (2-2).

[437] Supra n° 91.
[438] Contrairement à l'empreinte digitale pouvant subir des traumatismes environnementaux (coupures, brûlures) le réseau veineux ne subit aucune contrainte extérieure, améliorant ainsi l'image et le taux de fiabilité.

2-2 Le contenu des données collectées

312. Lors du passage d'un examen universitaire ou d'une inscription scolaire, les données des candidats et des élèves sont relevées. Comme pour tout traitement, la collecte des données doit être conforme à l'article 6 de la loi Informatique et libertés modifiée et doit faire l'objet d'une déclaration auprès de la CNIL ou d'une demande d'autorisation préalable lorsque les données sont sensibles. En effet, lorsque les parents inscrivent leurs enfants dans un établissement, ce dernier relève un certain nombre de données (identité, coordonnées).

En 2005, à titre expérimental, une base de données spécifique aux élèves de maternelle et primaire du privé comme du public nommée « base élèves » a été créée à cet effet. Depuis 2009, elle s'est généralisée à l'ensemble des établissements et relève les informations sur l'inscription, l'admission, la fréquentation, le suivi des effectifs. Cette base a fait l'objet d'une simple déclaration auprès de la CNIL, même si le ministère de l'Education nationale a préféré encadrer son application par voie règlementaire[439]. Les données collectées sont les données d'identité et les coordonnées de l'élève et de ses responsables légaux, les informations sur la scolarité et les informations périscolaires. Aucune information n'est relevée sur la nationalité, situation familiale, l'absentéisme, la santé ou les notes et acquis des élèves. Seules, les données en corrélation directe avec la finalité du traitement sont récoltées. Par ailleurs, les données ne sont pas conservées au-delà de l'année scolaire.

313. Quant au contenu des données traitées et conservées par le GMAC, elles comportent le nom, le prénom, le sexe, la date et le lieu de naissance, le numéro de téléphone, l'adresse électronique, la langue maternelle, le numéro d'inscription GMAT ainsi que la photographie numérique, données relatives au test et le résultat de ce dernier.
Au regard de la finalité du dispositif, qui nécessite de garantir l'identité des candidats, la CNIL a déclaré les données collectées adéquates, pertinentes et non excessives puisqu'il s'agit de renseignements déjà relevés pour tous types d'examens ou d'inscriptions.

[439] Ministère de l'éducation nationale, arrêté du 20 octobre 2008 portant création d'un traitement automatisé de données à caractère personnel relatif au pilotage et à la gestion des élèves de l'enseignement du premier degré, JO du 2 nov. 2008, disponible sur le site www.legifrance.gouv.fr

314. La proportionnalité du dispositif ne dépend pas uniquement de sa traçabilité ou des données collectées, mais aussi du mode de stockage choisi (2-3).

2-3 La proportionnalité du dispositif quant au mode de stockage

315. La proportionnalité du traitement est appréciée par la CNIL en fonction du mode de stockage choisi par l'organisme. Pour l'autorisation donnée au GMAC, ce n'est pas tant le dispositif envisagé qui peut être sujet à discussion, mais le mode de stockage adopté par les organisateurs, car il est associé au transfert des données personnelles, autorisé vers un pays tiers, les Etats-Unis.

En effet, le stockage choisi est double. Le premier intervient localement, sur le poste de contrôle pour une durée s'échelonnant de vingt-quatre heures à sept jours, après la session d'examen. Le second intervient sur une base de données centrale, située aux Etats-Unis, dans laquelle les données personnelles seront enregistrées pour une durée de cinq années période correspondant à la durée de validité du test GMAT.

Afin de consolider la protection des données personnelles des candidats, la CNIL a signé deux conventions. La première correspond à un engagement du respect de l'autorisation et de coopération en cas de contrôle avec la CNIL, signée avec le directeur sous-traitant aux Etats-Unis, en date du 28 avril 2009. La seconde, signée le 26 mai 2009, a un objet plus général puisqu'elle concerne le respect des principes de protection des données personnelles. Par ailleurs, le sous-traitant a adhéré au dispositif « Safe Harbor »[440].
Nous mettons toutefois en exergue le fait que l'hébergeur des données personnelles, la société Pearson VUE, est située sur le territoire américain, ce qui constitue une difficulté géographique non négligeable en cas d'un éventuel contrôle de conformité de l'usage des données.

Or, nous pensons qu'une unique conservation sur le territoire français aurait permis un meilleur contrôle des données personnelles des candidats par la CNIL. Lorsque les données personnelles sont transférées à l'étranger, les entreprises sont moins vigilantes. L'affaire

[440] Supra n° 158.

SWIFT, quelques années auparavant, en est l'exemple concret. Cette affaire a ravivé les craintes liées aux transferts de données personnelles à l'étranger. Les autorités américaines (la CIA et le Trésor américain) avaient surveillé et collecté les données bancaires de ressortissants européens, par le biais de l'entreprise multinationale SWIFT dont le siège est situé en Belgique[441]. Les autorités américaines n'ont pas respecté les règles européennes en matière de protection des données. A la suite de cette affaire, il est primordial de s'assurer que les autorités américaines n'usent pas de leur influence pour consulter les données issues du GMAC.

Même si des conventions sont établies avec le GMAC, rien ne prouve dans les faits que les données ne seront pas détournées de leur finalité, ni exploitées de manière excessive. Selon les critères de la CNIL, lorsqu'il s'agit des dispositifs de reconnaissance par empreintes digitales, « *seul un fort impératif de sécurité peut justifier le stockage sur un terminal de lecture-comparaison ou sur un serveur*[442] ». La CNIL ne s'est pas prononcée lorsque le dispositif ne laisse pas de traces. Néanmoins, elle fonde sa décision et « *constate que l'examen GMAT présente* ***des caractéristiques très particulières*** *: cet examen est passé dans des conditions identiques et en anglais dans environ 110 pays, par plus de 200.000 candidats chaque année. Les résultats ("score") obtenus dans un pays sont reconnus dans tous les autres, et constituent un processus de sélection permettant aux candidats d'accéder à près de 1800 grandes écoles de commerce et de gestion, ou formations de niveau MBA/Mastère dans ce domaine. Ces organismes ne sont susceptibles d'utiliser le GMAT que si sa sécurité et sa fiabilité sont parfaitement et uniformément garanties dans l'ensemble des pays concernés. Or les enjeux d'un tel dispositif sont susceptibles de créer de fortes tentations de fraude, et son universalité comporte en particulier des possibilités sérieuses de substitution de candidats. De telles fraudes ont été constatées dans le passé, et ont conduit GMAC à mettre en œuvre dans la plupart des pays concernés un contrôle basé sur les empreintes digitales, biométrie « à traces » offrant moins de garanties que le nouveau dispositif proposé.* ***Dans ces conditions particulières, la Commission considère que le recours à la reconnaissance du***

[441] Supra n° 20.
[442] CNIL, Communication relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données, décembre 2007, www.cnil.fr

réseau veineux de la paume de la main répond à une finalité légitime et n'est pas excessif au regard de cette finalité[443] ».

La CNIL n'a pas défini les situations qu'elle estimait exceptionnelles mais, pour expliquer son choix au sein de cette délibération, elle a fourni des éléments de fait. La nature internationale de l'examen, sa notoriété, mais aussi l'existence incontestable de fraudes par le passé, la confortait dans l'idée de procéder à une identification fiable et, sur ces points, nous rejoignons la position de la Commission. Le GMAC a implanté quelques dispositifs biométriques dans plusieurs pays, tels que le Canada ou le Costa Rica[444]. La plupart du temps, il a opté pour des dispositifs de reconnaissance par empreintes digitales avec un stockage au sein d'une base de données gérée aux Etats-Unis. Ce choix, à juste titre, n'a pas été celui de la CNIL. Le caractère exceptionnel de la situation ne constitue pas pour autant une situation de danger, comparable au fort impératif de sécurité pour lequel il serait nécessaire de conserver des données identifiantes et traçables du corps humain au sein d'une base centralisée dans un pays où il serait délicat, en pratique, d'effectuer un contrôle. Sur ce point, même si un fort impératif de sécurité n'est pas exigé, il n'en demeure pas moins que le caractère exceptionnel de la situation doit être apprécié, au fur et à mesure, afin d'éviter la prolifération de bases de données personnelles, qu'elles soient biométriques ou non.

316. En conséquence, les situations dans lesquelles des bases de données biométriques sont constituées doivent rester exceptionnelles et déterminées au cas par cas, même si les dispositifs biométriques employés ne permettent pas la traçabilité de l'individu. Les informations stockées sur les serveurs peuvent être détournées et cette précaution ne vise pas exclusivement les données biométriques mais aussi les données de santé, bancaires ou d'assurance par exemple. Par ailleurs, il n'est pas bénéfique que des données personnelles soient transférées à l'étranger où les autorités de contrôle françaises ne peuvent pas facilement exercer leurs prérogatives même en présence de conventions bilatérales. Cette décision est

[443] CNIL, Délibération n° 2009-360 du 18 juin 2009 autorisant la mise en œuvre par le Graduate Management Admission Council (GMAC) représenté par Pearson Education France d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux de la paume de la main et ayant pour finalité de contrôler l'accès à des salles d'examen et d'empêcher la substitution de candidat à l'examen GMAT, demande d'autorisation n°1323460, disponible sur le site www.legifrance.gouv.fr

[444] Site Internet du GMAC au lien suivant :
http://www.gmac.com/gmac/NewsandEvents/GMNews/2004/JanFeb/GMATBiometricSecurity.htm

novatrice car elle est la première, en biométrie, à autoriser la constitution d'une base de données personnelles, issue d'un dispositif dit « sans traces » et qui concerne une entité privée étrangère.

317. Les entreprises sont aussi intéressées par les dispositifs de reconnaissance vocale, à l'image de la société Michelin qui a opté pour ce dispositif d'authentification de ses salariés (3°).

3°. Reconnaissance vocale

318. Le dispositif de reconnaissance vocale vise principalement au renouvellement des mots de passe sur des postes informatiques, dans le cadre du contrôle d'accès logique. La fiabilité de ce dispositif peut être limitée, en fonction de l'état de santé de la personne, par exemple si elle est affectée par un mal de gorge, mais aussi en fonction de l'environnement dans lequel le procédé est développé comme, notamment, les bruits extérieurs. La prolifération des mots de passe et des problèmes liés aux pertes ou vol de ces derniers poussent les entreprises à recourir à la biométrie. Une enquête publiée en septembre 2005 par un intégrateur américain de solutions biométriques[445], a révélé que plus d'un quart des salariés doit retenir au moins treize mots de passe pour les diverses applications informatiques professionnelles ou privées qu'ils doivent gérer. L'accroissement d'outils de sécurité qui permettent de protéger les données peut entraîner l'effet inverse, par la perte ou le vol de ces mots de passe.

Pour que le dispositif biométrique soit déclaré proportionnel, même en l'absence de traçabilité, les données traitées doivent être adéquates, pertinentes et non excessives, conformément à l'article 6 de la loi Informatique et libertés modifiée. Par ailleurs, elles ne doivent pas être stockées et conservées pour une durée incompatible avec la finalité pour laquelle le dispositif a été implanté.

[445] RSA Security, RSA Security Survey Reveals Multiple Passwords Creating Security Risks and End User Frustration. Cette enquête a été réalisée sur un échantillon de mille sept cents entreprises américaines High Tech, disponible sur le site internet de RSA, http://www.rsa.com/press_release.aspx?id=6095

319. L'emploi du dispositif biométrique de reconnaissance vocale est récent, puisque la CNIL en a autorisé pour la première fois son utilisation, en 2007[446], à la société des pneumatiques Michelin. Cette société souhaitait implanter un dispositif de reconnaissance vocale afin de modifier, par mot de passe, les codes d'accès aux ordinateurs. Le fonctionnement du dispositif de reconnaissance vocale est le suivant : les employés consultent un serveur vocal, lors de la réinitialisation du mot de passe une comparaison est effectuée entre le gabarit vocal préalablement enregistré et la voix du salarié.

Cette technologie est considérée par la CNIL comme « sans traces » et assez fiable si elle est employée dans un environnement clos, imperméable aux bruits[447]. L'accumulation de bruits parasites peut altérer la fiabilité du dispositif et le rendre inefficace. Par exemple, un dispositif de reconnaissance vocale en extérieur n'est pas judicieux.

En ce qui concerne la qualité des données, celles qui sont enregistrées sont les données identifiantes du salarié ainsi que son identifiant professionnel. Elles sont pertinentes, adéquates et non excessives au regard de la finalité pour laquelle le dispositif est implanté c'est-à-dire la réinitialisation des mots de passe. Ce sont les données qu'il est permis raisonnablement de traiter en relation avec la finalité du traitement.

Si l'on considère l'opportunité de l'emploi de la biométrie plutôt qu'une autre technique, l'explication réside simplement dans le fait que la modification des mots de passe, peut être effectuée manuellement, donc, sans garantir que l'employé qui procède à l'enregistrement vocal, soit bien le propriétaire du mot de passe. Nous tenons à rappeler, que dans ce cas de figure, l'utilisation de la biométrie, n'est que secondaire, puisque l'authentification principale du salarié, sur son poste de travail s'accomplit à l'aide du mot de passe. En conséquence, le dispositif est proportionnel à la finalité de contrôle d'accès logique.

320. Si, en France, ce dispositif n'a pas soulevé de problèmes, au Canada, l'implantation d'un dispositif de reconnaissance vocale a posé quelques difficultés.

---

[446] CNIL, Délibération n° 2007-248 du 13 sept. 2007 autorisant la mise en œuvre par la Manufacture française des pneumatiques Michelin d'un traitement automatisé de données à caractère personnel reposant sur un procédé de reconnaissance vocale et ayant pour finalité la gestion des mots de passe, disponible sur le site www.legifrance.gouv.fr

[447] Supra n° 97.

Un groupe de salariés s'est opposé à l'employeur qui souhaitait la mise en place d'un dispositif de reconnaissance de la voix[448] avec, pour finalité la modification des mots de passe. Les salariés soutenaient qu'ils n'avaient pas consenti à la collecte de données biométriques. Le dispositif de reconnaissance vocale visait à accéder à certaines applications de travail, il s'agissait simplement d'un système de contrôle d'accès.

L'assistant du commissaire à la vie privée en charge de cette affaire, a estimé que l'employeur avait respecté la loi sur la protection de la vie privée et des documents électroniques du Canada[449]. Il a décidé de mettre en « balance les intérêts » des parties, entre la protection de la vie privée et les intérêts économiques d'une entreprise. Dans ce cas particulier, le principe de proportionnalité a joué un rôle déterminant car il a permis de mesurer les intérêts des parties en présence. Il a cependant été à l'avantage de l'employeur, car la perte de la vie privée des salariés était proportionnée aux bénéfices qu'il estimait lui revenir, en améliorant la sécurisation de l'accès à ses applications informatiques.

321. A la lumière de ces exemples, nous concluons que le principe de proportionnalité vise à garantir la prééminence des droits fondamentaux du salarié sur la liberté et la bonne gestion d'une entreprise. Il permet de s'interroger sur la nécessité de l'emploi de la biométrie mais aussi sur ses implications.

La démarche intellectuelle proposée par l'Irlande auprès des entreprises qui désirent implanter un dispositif biométrique, est non seulement pédagogique, mais aussi nécessaire. Beaucoup d'entreprises françaises et européennes ont une conscience encore trop limitée des risques liés à la collecte et au traitement des données biométriques et plus généralement de toute catégorie de données personnelles.

Par ailleurs, le principe de proportionnalité détermine la pertinence du choix du mode de stockage. Nous évoluons dans un monde qui tend à collecter de plus en plus de données personnelles sur les individus. L'accumulation de données au sein de bases centralisées, si elle est nécessaire pour sauvegarder les intérêts de la Nation, ne se justifie pas, à l'échelle de

[448] Affaire anonymisée, PIPEDE Case summary 281, issue de l'article de Gary T. Clarke « Biometrics in the workplace – Where to draw the line?" Personal Information Protection Act Conference 2006, April 26 and 27, Calgary, Alberta (Canada), p. 9.
[449] Loi nommée PIPEDA (Personal Information Protection and Electronic Document Act)

l'entreprise, sauf à avancer des circonstances exceptionnelles ou « un fort impératif de sécurité ». Ce principe contribue, effectivement à l'encadrement de la maîtrise collective de l'usage de la biométrie.

CONCLUSION DU TITRE I

« *Il faut donc choisir de deux choses l'une :*
ou souffrir pour se développer, ou ne pas se développer,
pour ne pas souffrir. Voilà l'alternative de la vie,
voilà le dilemme de la condition terrestre[450] »

322. La façon selon laquelle une technique biométrique est utilisée, plus ou moins invasive pour le corps humain, peut avoir des conséquences sur l'individu, quelle que soit la manière dont ces données sont prélevées mais surtout, la manière avec laquelle il va appréhender l'usage de ce mode d'identification, dans le contexte de son activité professionnelle. Il incombe donc, aux responsables de traitement, de mesurer la juste nécessité du recours à des outils biométriques, face à la « menace » pour laquelle elle est souhaitée.

323. Selon les pays, la biométrie est perçue, acceptée ou utilisée de manières différentes.
Au Canada, une entreprise peut utiliser des dispositifs biométriques sans autorisation préalable, elle a pour seule obligation de déclarer son traitement de données, en adjoignant à sa déclaration, le formulaire de consentement à la cueillette des données personnelles des employés[451]. C'était le cas de la France, pour les entreprises du secteur privé, avant la réforme de la loi n°78-17 du 6 janvier 1978 modifiée par la loi n°2004-801 du 6 août 2004.

En Australie, grâce à l'association Biometric Institute, le gouvernement a mis en place un Code de conduite dans l'usage des données biométriques[452]. Ce code ne garantit pas le risque zéro mais il a vocation à responsabiliser les signataires et à garantir aux tierces personnes, la bonne utilisation des données biométriques. Toute entreprise signataire de ce code de conduite prend la mesure de ses engagements. Ce dernier contribue à instaurer un climat social de confiance vis-à-vis des salariés, puisque il a une valeur juridique mais aussi une éthique, dans le monde des affaires, auprès des partenaires économiques. L'entreprise se distingue par son

[450] Th. Jouffroy (1796 – 1842), extrait de Cours d'esthétique, 1843
[451] Cf. Annexe 4
[452] Biometric Institute Privacy Code, disponible sur le site internet http://www.biometricsinstitute.org/

engagement dans la protection des données personnelles. Cette charte pourrait être comparée à une certification ou un label dans le domaine technique. Elle va plus loin que nos actuelles chartes informatiques qui n'ont vocation qu'à encadrer les droits et obligations « informatiques » entre l'employeur et le salarié.

En Australie, en Nouvelle-Zélande ou au Canada, les offices de protection des données personnelles mettent en place des procédures de déclaration tout en instaurant des principes clés.

324. Le travail effectué est considérable, rares sont les pays en dehors de l'Union européenne qui procèdent à l'étude préalable des demandes tendant à l'insertion d'outils biométriques dans les entreprises. Les commissions de protection de la vie privée interviennent souvent dans le cadre d'un contrôle a posteriori, pour avertir ou sanctionner. Les entreprises doivent déclarer leur traitement mais il n'y a pas de contrôle quant à la nature de l'usage de la biométrie, ni de pédagogie si le traitement est disproportionné.

Du point de vue procédural, le contrôle a priori[453], a l'avantage de réguler l'insertion de la biométrie en entreprise tout en véhiculant de façon pédagogique les principes « informatique et libertés ». En contre-partie, il a l'inconvénient de mobiliser plus de personnel et de moyens à l'heure où les différents gouvernements adoptent des plans d'austérité pour leurs administrations. La déclaration de conformité est un outil extrêmement efficace qui a de nombreux avantages. Cette procédure oriente les responsables de traitement dans le choix du dispositif biométrique, en fonction de la finalité du traitement et ne nécessite pas de lourdes formalités. On ne peut souhaiter que son élargissement à d'autres techniques déclarées pour l'heure « sans traces ».

S'agissant de la procédure d'autorisation préalable à l'emploi de dispositifs biométriques, elle est encore majoritairement utilisée. Elle est peut être la solution dissuasive à l'égard des responsables de traitement mais au prix d'une importante charge de travail et d'une certaine « lourdeur administrative » pour la Commission qui reconnaît elle-même avoir des difficultés à concilier ses missions de prévention, de sensibilisation, d'étude des demandes d'autorisation et de contrôle des dispositifs. Néanmoins, les autorisations données par la CNIL tiennent

[453] Supra n° 147.

compte de la difficulté de trouver un juste milieu entre protection des libertés individuelles et intégration des progrès technologiques dans les entreprises. Avec la multiplication des industries à risques mais aussi des entreprises « high tech » friandes de nouvelles technologies, elle est garante d'un équilibre tripartite entre l'employeur, les salariés avec leurs représentants mais aussi, la population vivant autour de l'entreprise, car la Commission est indirectement un acteur responsable (en donnant certaines autorisations) dans la sécurisation de cette dernière, si elle est bien protégée par une technique biométrique. En effet, une usine, une entreprise de produits dangereux ou une centrale nucléaire, mieux protégées, plus sécurisées peuvent éviter, non les accidents, malheureusement, mais les vols de données industrielles ou au pire, les attentats.

325. Le principe de finalité a une vocation dissuasive de part son double aspect (objectif du traitement, sanction en cas de détournement ou dépassement de cet objectif). Le principe de proportionnalité possède une vocation « pédagogique », en obligeant les responsables de traitement des entreprises à réfléchir sur la nécessité de l'emploi de la biométrie et au devenir des données personnelles des salariés de l'entreprise. C'est en ce sens que nous parlons de responsabilité des chefs d'entreprise dans ces principes de finalité et proportionnalité. Ces deux principes doivent, néanmoins, être plus développés dans ces deux fonctions. Les entreprises ne motivent pas suffisamment les raisons pour lesquelles elles ont recours à la biométrie. Elles évoquent bien souvent une nécessité de sécuriser les accès mais n'expliquent pas, en quoi cette sécurisation biométrique permettrait d'améliorer substantiellement la qualité de leurs produits et services ou permettrait de sécuriser plus efficacement un bâtiment ou une salle etc. La précision de ces motivations ne vise pas à alourdir la procédure mais à justifier plus encore l'emploi du dispositif. La biométrie est, comme la plupart des nouvelles technologies, séduisante, sans que soient suffisamment mesurées les implications de ce choix.

Ces principes concourent efficacement à l'encadrement de la maîtrise collective des outils biométriques. Ces deux principes sont complémentaires et l'on pourrait extrapoler en avançant qu'ils sont supplantés par un principe de responsabilité « juridique », dans sa signification initiale d'une personne qui « *doit rendre compte devant une autorité de ses actes ou des actes de ceux dont il a la charge* ». Par ailleurs, il existe la responsabilité dans son sens moral que les responsables de traitement et les employeurs doivent garder à l'esprit. La règle

juridique intervient a priori pour la mise en œuvre du dispositif et a posteriori pour le contrôler ou le sanctionner. Néanmoins, elle ne remplace pas les rapports de confiance qu'il est nécessaire d'avoir dans toute relation de travail. Lorsqu'un dispositif biométrique est sollicité pour la gestion des horaires ou la restauration en entreprise, il n'est pas pertinent de stocker les données au sein d'une base centralisée. En revanche, l'usage d'un dispositif de reconnaissance par empreintes digitales pour le contrôle d'accès aux locaux est justifié pour une entreprise dont l'activité est réputée dangereuse (nucléaire, produits dangereux). Il importe de faire confiance aux industriels et aux chefs d'entreprise. Le coût de l'implantation d'un dispositif biométrique est plus élevé qu'une architecture traditionnelle de sécurité. Une entreprise qui investit plus d'argent dans la sécurité de ses biens, informations et installations le fait nécessairement pour un but précis autre que la simple surveillance de ses salariés.

326. Parallèlement au contrôle collectif de l'usage des dispositifs biométriques, intervient le contrôle individuel qu'effectue le salarié. Ce dernier a un rôle actif, il est un acteur de l'entreprise, qui a des devoirs mais surtout des droits vis-à-vis de l'utilisation de ses données personnelles. Il a un droit de regard et d'action quant à l'usage de la biométrie. (Partie II)

TITRE II – Le contrôle individuel de l'usage de la biométrie en entreprise

«*Biometric technologies are not*
inherently good or bad for privacy.
They become good or bad for privacy depending on
how they are designed, developed and deployed[454] ».

327. L'affirmation du Commissaire à la protection des données australien Timothy Pilgrim est une piste de réflexions sur l'intégration de la biométrie dans notre société et de façon plus circonscrite, dans l'entreprise. Si le problème ne venait pas de la technologie en elle-même mais plutôt des choix faits par les entreprises quant à sa conception, son utilisation, son déploiement ?

Tous les salariés doivent participer à la « maîtrise individuelle » de leurs données biométriques. Il faut entendre par là, la participation individuelle du salarié dans la manière dont il entend consentir à « la cueillette »[455] de ses données biométriques, après avoir été dûment informé sur les finalités de l'usage d'un tel dispositif et des résultats qui en sont attendus. Le principe de participation trouve sa source dans le Préambule de la Constitution de 1946 qui proclame que « *Tout travailleur participe, par l'intermédiaire de ses délégués, à la détermination collective des conditions de travail ainsi qu'à la gestion des entreprises*[456] ».

Les représentants des travailleurs ont eu un rôle essentiel dans la conception des droits et libertés au travail. La Constitution du 27 octobre 1946 a consacré les droits collectifs des salariés comme le droit de grève ou la liberté syndicale apparue plus tôt, avec la loi Waldeck-Rousseau du 21 mars 1884. Les instances représentatives du personnel font partie de ce que nous appelons le « processus informationnel », au cours duquel se déroule le dialogue social

[454] « *Les technologies biométriques ne sont pas intrinsèquement bonnes ou mauvaises pour la vie privée. Elles le deviennent dépendamment de la façon avec laquelle elles sont conçues, développées et déployées* » Timothy Pilgrim, Deputy Privacy Commissioner "Biometrics and Privacy" Speech to Biometrics Institute 21 november 2007, p. 3 site internet de l'Australian Government Office of the privacy Commissioner: http://www.privacy.gov.au/index.php

[455] Pour reprendre l'expression québécoise concernant la phase d'enrôlement pendant laquelle les données biométriques sont recueillies.

[456] Préambule de la Constitution du 27 octobre 1946, 8°, disponible sur le site internet du Conseil Constitutionnel au www.conseil-constitutionnel.fr

(information, consultation) entre l'employeur et les salariés. Elles incarnent, au sein de l'entreprise, la voix collective de l'ensemble des salariés qu'elles représentent. Par conséquent, avant l'implantation de toute nouvelle technologie, l'employeur est soumis à une obligation d'information des salariés et de consultation des instances représentatives du personnel.

L'introduction de nouvelles technologies peut modifier considérablement les conditions de travail. Fort de ce constat, le législateur a pensé qu'il était primordial sur ces questions, d'intégrer les organes représentatifs du personnel au dialogue social. Celui-ci inclut, « *tous types de négociation, de consultation ou simplement d'échange d'informations entre les représentants des gouvernements, des employeurs et des travailleurs selon des modalités diverses, sur des questions relatives à la politique économique et sociale présentant un intérêt commun*[457] ». Ce dernier est crucial et doit aboutir à un consensus entre les différents acteurs du monde du travail.

C'est pourquoi le droit du travail réaffirme l'obligation d'information et de consultation des organes représentatifs du personnel, doublée d'une information individuelle des salariés, aux termes des articles L. 2323-13 et L. 2323-32 du Code du travail[458]. Bien qu'hésitante en la matière, la négociation collective tend à se développer sous l'impulsion des organisations syndicales et patronales depuis la signature d'une position commune sur les voies et moyens de l'approfondissement de la négociation collective, le 16 juillet 2001[459].

Toutefois, cette dernière se matérialise de manière hétérogène, notamment en fonction du nombre de salariés ou de la taille de l'entreprise. Ainsi, les délégués du personnel sont élus dès que l'entreprise comporte onze salariés ou plus[460]. Pour les entreprises inférieures à deux cents salariés, le législateur a prévu la mise en place d'une délégation unique de représentants du personnel dont les attributions sont identiques à celles des représentants du personnel jointes à celles du comité d'entreprise[461]. Pour ces grandes et moyennes entreprises nous pouvons dire que « l'union fait la force » mais pour les plus petites qui comportent moins de

[457] Organisation Internationale du Travail (OIT), définition du dialogue social. Disponible sur le site internet au lien suivant http://www.ilo.int/public/french/dialogue/ifpdial/areas/social.htm

[458] Loi n° 2008-67 du 21 janv. 2008 (anciens art. L. 432-2 et L. 432-2-1 du code du travail) ; Cf. Annexe 12

[459] Position commune du 16 juil. 2001 sur les voies et moyens de l'approfondissement de la négociation collective, document disponible sur le site internet au www.vie-publique.fr

[460] C. trav. Art. L. 2313-1

[461] C. trav. Art. L. 2326-1 et suivants

onze salariés, la plupart du temps, l'information est faite directement au personnel, ou par l'intermédiaire d'un salarié spécifiquement mandaté pour représenter l'ensemble du personnel de l'entreprise ce qui peut altérer, par exemple, la qualité de l'information et fausser le consentement.

328. Le consentement au traitement des données est une obligation encadrée par l'article 7 de la loi Informatique et libertés. Préalablement à la collecte des données et sauf pour les exceptions énoncées au même article, le responsable de traitement doit avoir reçu le consentement de la personne concernée. Le Code civil français dans les articles 1108 et suivants, ne définit pas le consentement, mais énonce les vices qui peuvent l'entacher. Il doit être empreint de liberté et de conscience car la validité de la convention est conditionnée à la réunion de ces caractères.
Le Comité consultatif national d'éthique rappelle qu'en matière de traitements biométriques « *l'exigence du consentement est un élément essentiel lors de la collecte des données biométriques* ».

329. Il importe de s'intéresser à la qualité de l'information et de la consultation des salariés sur l'introduction des nouvelles technologies, afin de jauger l'application des dispositions que sont l'information sur les appareils biométriques, celles sur la durée du stockage, ou sur le devenir des données (Chapitre 1) et d'identifier l'effectivité du consentement des personnes dans l'environnement biométrique (Chapitre 2).

Chapitre 1- Les obligations d'information et de consultation des salariés dans l'environnement biométrique

« *A man without privacy is a man without dignity;*
the fear that Big Brother is watching and listening
threatens the freedom of the individual
no less than the prison bars[462] ».

330. Les textes fondamentaux en matière de protection des données personnelles prescrivent pour tout individu, l'information préalable et incontournable, de la collecte de ses données personnelles. La Convention du Conseil de l'Europe STE n°108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a été la première convention à concilier la protection de la vie privée avec la circulation des informations.[463] Ainsi, la personne doit avoir connaissance de l'existence du fichier et être en mesure de se faire communiquer les informations collectées, ainsi que la faculté d'exercer un droit de rectification sur les données.

Selon les lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel de l'OCDE « *toute personne physique devrait avoir le droit :*
a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant ;

[462] « Un homme sans vie privée est un homme sans dignité ; la peur que Big Brother nous observe et nous écoute n'est pas moins une menace pour les libertés individuelles que des barreaux de prison. » Professor Zelman Cowen, 1969, « The Private man », Boyer Lectures, Australian Broadcasting Commission, p9-10

[463] « *Toute personne doit pouvoir:*
- a. ***connaître l'existence*** *d'un fichier automatisé de données à caractère personnel, ses finalités principales, ainsi que l'identité et la résidence habituelle ou le principal établissement du maître du fichier;*
- b. ***obtenir*** *à des intervalles raisonnables et sans délais ou frais excessifs* ***la confirmation de l'existence*** *ou non dans le fichier automatisé, de données à caractère personnel la concernant ainsi que la communication de ces données sous une forme intelligible;*
- c. ***obtenir,*** *le cas échéant,* ***la rectification*** *de ces données ou* ***leur effacement*** *lorsqu'elles ont été traitées en violation des dispositions du droit interne donnant effet aux principes de base énoncés dans les articles 5 et 6 de la présente Convention;*
- d. ***disposer d'un recours*** *s'il n'est pas donné suite à une demande de confirmation ou, le cas échéant, de communication, de rectification ou d'effacement, visée aux paragraphes b et c du présent article.* »

Art. 8 de la Convention STE n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janv. 1981, disponible sur le site internet du Conseil de l'Europe www.coe.int

b) de se faire communiquer les données concernant ;

i) dans un délai raisonnable ;

ii) moyennant éventuellement, une redevance modeste ;

iii) selon des modalités raisonnables ; et

iv) sous une forme qui lui soit aisément intelligible ;

c) d'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet ; et

d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger[464] ».

La Directive n° 95/46 CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, consacre une section IV à l'« *Information de la personne concernée* ». La loi Informatique et libertés modifiée réaffirme ce principe au sein des articles 32 et suivants et dans le Chapitre V intitulé « *Obligations incombant aux responsables de traitements et droits des personnes.* »

L'article 27 de la Charte des droits fondamentaux de l'Union européenne permet d'élever ce droit en droit fondamental à l'information puisqu'il énonce que « *Les travailleurs ou leurs représentants doivent se voir garantir, aux niveaux appropriés, une information et une consultation en temps utile, dans les cas et conditions prévus par le droit communautaire et les législations et pratiques nationales*[465] ».

Les règles « informatique et libertés » s'entrelacent avec la législation du travail. Cette dernière, soucieuse de la protection des données personnelles des salariés, prévoit un double mécanisme de protection qui s'échelonne entre l'information-consultation des organes représentatifs du personnel, et l'information individuelle du salarié par le biais de notes explicatives et autres procédés comme une charte internet. L'information connaît différentes acceptions, mais n'a pas fait l'objet de définitions dans la loi Informatique et libertés n° 78-17

[464] Lignes Directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontaliers de données à caractère personnel, Partie 2 « principes fondamentaux applicables au plan national », Annexe à la recommandation du conseil du 23 sept.1980, éditions de l'OCDE, 2002, p. 16

[465] Charte des droits fondamentaux de l'Union Européenne 2000/C 364/01, signée et proclamée lors du Conseil européen de Nice le 7 déc. 2000, JO 18 déc. 2000, disponible sur le site internet du parlement européen au www.europarl.europa.eu

du 6 janvier 1978 modifiée. Il peut s'agir par exemple de l'« *action d'informer quelqu'un, un groupe, de le tenir au courant des événements*[466] », ou bien aussi de « *tout événement, tout fait, tout jugement porté à la connaissance d'un public plus ou moins large, sous forme d'images, de textes, de discours, de sons*[467] ». Nous retiendrons cependant cette définition plus juridique « *élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué*[468] ».

L'information peut être véhiculée par différents acteurs de la protection des données personnelles et du monde du travail : la CNIL, les industriels lorsqu'il s'agit des techniques biométriques, le responsable de traitement ou bien le correspondant informatique et libertés, s'il a été désigné conformément à l'article 22 de la loi Informatique et libertés modifiée.

331. Dans la majeure partie des cas, cette information est transmise au salarié par le responsable de traitement qui peut désigner, depuis la loi de 1978, un correspondant informatique et libertés. Les salariés doivent bénéficier d'une information complète sur la collecte et le devenir de leurs données personnelles ainsi que sur les finalités du traitement (section 1). L'importance des modifications engendrées par les nouvelles technologies implique la consultation des représentants du personnel (section 2).

[466] Dictionnaire Larousse en ligne, disponible sur le site www.larousse.fr
[467] Ibid
[468] Définitions du dictionnaire Larousse électronique. Site Internet : http://www.larousse.fr/dictionnaires

Section 1. L'information loyale des salariés

332. Tout salarié a le droit d'être valablement informé sur l'utilisation de ses données personnelles et sur les finalités du traitement qui conduisent à la collecte. Le Code du travail énonce qu'« *aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance*[469] ». Les données personnelles doivent donc être traitées loyalement, à l'image des relations contractuelles liant l'employeur au salarié en vertu desquelles « *le contrat de travail doit être exécuté de bonne foi*[470] ».

Cette expression, exclusivement réservée aux obligations contractuelles, a été consacrée par le législateur, pour les relations de travail, au sein de la loi de modernisation sociale du 17 janvier 2002[471]. La loyauté est nécessaire à tout moment de la relation contractuelle pour instaurer un rapport de confiance, notamment en matière de nouvelles technologies, où l'implantation de dispositifs de contrôles ou de gestion, est souvent ressentie comme de l'espionnage.

L'information est chronologiquement, l'étape préalable à toute collecte de données personnelles. Elle favorise la confiance et la transparence dans les relations de travail. Dès lors, on peut dire que le salarié dispose « d'un droit passif » dans le sens où il reçoit, de droit, l'information, plus qu'il n'agit sur ses données personnelles[472].

333. La qualité du consentement du salarié sera grandement liée à la qualité de l'information donnée par les personnes qui en sont garantes et les sanctions afférentes en cas de manquements (A). En effet, depuis la loi n° 2004-801 du 6 août 2004, les responsables de traitement disposent d'obligations plus lourdes dues à l'accroissement légal des informations à transmettre (B).

[469] C. trav. art. L. 1222-4 issu de la loi n° 2008-67 du 21 janv. 2008, JO 23 janv. 2008
[470] C. trav. art. L. 1222-1
[471] Loi n° 2002-73 du 17 janv. 2002 de modernisation sociale, JO 18 janv. 2002, p. 1008
[472] Contrairement aux droits d'accès, de rectification qui sont à son initiative.

A. Les obligations et les sanctions des garants de l'information des salariés

334. Dans la rédaction initiale de la loi n°78-17 du 6 janvier 1978, le responsable de traitement n'était pas défini, ni dans son rôle, ni dans son statut. Pourtant, il importait de pouvoir identifier la personne physique ou morale, dont la mission était de traiter les données personnelles. Le rapport Braibant, chargé de la transposition de la Directive avait considéré que « *La définition du " responsable du traitement " est essentielle – et doit figurer en tête de la loi – dans la mesure où elle détermine la personne physique ou morale sur laquelle les obligations prévues par la directive reposent, et où le lieu d'établissement de cette personne constitue le premier critère de détermination de la loi nationale applicable*[473] ».

335. La loi du 6 août 2004 a défini le statut du responsable de traitement, comme un personnage garant des données personnelles (1°) ainsi que les sanctions qui en découlent dans les hypothèses du défaut d'information (2°).

1°. Le statut de responsable de traitement

336. La réforme opérée par la loi de 2004 a eu pour effet de renforcer les droits des personnes sur leurs données personnelles. Une entité au sein des entreprises est chargée de veiller au bon déroulement de l'information, de la collecte et du traitement des données personnelles : cette entité est le responsable de traitement. L'article 3 I de la loi du 6 janvier 1978 modifiée définit le responsable de traitement comme étant « *sauf désignation expresse par les dispositions législatives ou règlementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens* ». En droit français, il est considéré comme une entité distincte des employés de l'entreprise, qu'ils soient salariés ou sous-traitants, ces derniers effectuant les traitements pour son compte.

337. Au sein des entreprises, le responsable de traitement doit se soumettre à de multiples obligations qui ont élargi sa mission (1-1). Néanmoins, il a la faculté de déléguer

[473] G. Braibant, « Données personnelles et société de l'information », Rapport au Premier ministre sur la transposition en droit français de la Directive n° 95/46, Doc. fr. janv. 1998, p. 45, disponible sur le site www.ladocumentationfrancaise.fr

cette mission pour certains traitements, en nommant un correspondant informatique et libertés (1-2).

1-1. Les Missions du responsable de traitement

338. Afin d'assurer la protection des données personnelles des salariés d'une entreprise, celle-ci doit obligatoirement nommer un responsable de traitement. L'article 2 d de la Directive 95/46 CE du 24 octobre 1995 définit pour la première fois le responsable du traitement comme « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel; lorsque les finalités et les moyens du traitement sont déterminés par des dispositions législatives ou réglementaires nationales ou communautaires, le responsable du traitement ou les critères spécifiques pour le désigner peuvent être fixés par le droit national ou communautaire* ».

La Directive de 1995 laissait subsister un doute quant à l'interprétation de cette disposition à savoir, s'il pouvait y avoir plusieurs responsables conjoints pour un traitement, ou un responsable qui agit seul ou conjointement avec d'autres personnes. La loi du 6 août 2004 qui a transposé la Directive de 1995, a supprimé toute action conjointe avec d'autres intervenants sur les données personnelles, afin de faciliter la mise en œuvre des mécanismes de responsabilité. Pour des questions de responsabilité et de conflit de lois lorsque des entreprises étrangères sont concernées, une seule personne peut être garante des données personnelles. A ce titre, l'article 3 I de la loi n°78-17 du 6 janvier 1978 a limité le responsable de traitement à **«** *la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens* ». Cette disposition a permis de le distinguer, des autres interlocuteurs « informatique et libertés » potentiels de l'entreprise que sont le sous-traitant qui procède aux traitements pour son compte ou le correspondant informatique et libertés.

Depuis la réforme de 2004, le responsable de traitement a la faculté de nommer un correspondant informatique et libertés sans pour autant s'exonérer de sa responsabilité[474]. Les articles 45 et suivants de la loi Informatique modifiée font explicitement mention au « responsable de traitement », comme une entité indépendante. En cas de perte, détérioration

[474] Infra n°342

ou détournement des données personnelles, seule la personne physique ou morale déclarée pour cette mission est visée par la loi. Le responsable de traitement définit, seul, les finalités et les moyens du traitement au correspondant et reste l'unique personne habilitée à intervenir en cas de manquement du subordonné[475].

339. Au sein des entreprises, la fonction de responsable de traitement se matérialise par une personne physique, un employé de l'établissement ou une personne morale tel un service juridique. Il peut s'agir aussi de toute entité extérieure compétente pour exercer cette mission, par exemple, un cabinet d'avocats. Ses obligations sont disposées aux articles 32 et suivants de la loi.

Dans le cadre de l'utilisation d'un dispositif biométrique, le responsable de traitement doit se conformer aux procédures existantes, selon les finalités du traitement envisagé et de la technologie choisie (autorisation préalable ou déclaration simplifiée). Il doit informer et obtenir le consentement des salariés dont les données sont recueillies. Son rôle est prépondérant de par la nature des données collectées et des mesures à prendre pour garantir leur sécurité, surtout que les données biométriques ne sont jamais récoltées seules, mais sont le plus souvent associées à des renseignements liés à l'identité.

Enfin, une fois l'autorisation donnée, il doit veiller au respect de la durée de conservation des données ainsi qu'à l'application des droits d'accès, d'opposition, de rectification et d'effacement des données. Le responsable de traitement est non seulement le garant de la sécurité des données, mais aussi et surtout celui de l'information et de la consultation des organes représentatifs du personnel ainsi que des salariés conformément aux articles 2323-13 et 2323-32 du Code du travail. Il a donc une fonction prépondérante dans le bon déroulement du dialogue social.

340. Avec un statut consolidé, un rôle accru et des obligations importantes, le responsable de traitement a la faculté, depuis la loi n°2004-801 du 6 août 2004, de nommer un

[475] Art. 52 du décret 2007-451 du 25 mars 2007 « *Lorsque la Commission nationale de l'informatique et des libertés constate, après avoir recueilli ses observations, que le correspondant manque aux devoirs de sa mission, elle demande au responsable des traitements de la décharger de ses fonctions en application du III de l'article 22 de la loi du 6 janvier 1978 susvisée.* »

correspondant informatique et libertés compétent en la matière, à qui il peut déléguer le suivi de certains traitements. (1-2)

1-2. La faculté de délégation de certains traitements au Correspondant informatique et libertés

341. Une des innovations de la loi n° 2004-801 du 6 août 2004, modifiant la loi n° 78-17 du 6 janvier 1978, est que le responsable de traitement peut désigner un correspondant informatique et libertés (CIL) ou nommé correspondant à la protection des données à caractère personnel (CPDCP). L'article 22 III de la loi 78-17 du 6 janvier 1978 modifiée énonce que « ***III.*** - *Les traitements pour lesquels le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi sont dispensés des formalités prévues aux articles 23 et 24, sauf lorsqu'un transfert de données à caractère personnel à destination d'un État non membre de la Communauté européenne est envisagé.*
La désignation du correspondant est notifiée à la Commission nationale de l'informatique et des libertés. Elle est portée à la connaissance des instances représentatives du personnel.

Le correspondant est une personne bénéficiant des qualifications requises pour exercer ses missions. Il tient une liste des traitements effectués immédiatement accessible à toute personne en faisant la demande et ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions. Il peut saisir la Commission nationale de l'informatique et des libertés des difficultés qu'il rencontre dans l'exercice de ses missions.

En cas de non-respect des dispositions de la loi, le responsable du traitement est enjoint par la Commission nationale de l'informatique et des libertés de procéder aux formalités prévues aux articles 23 et 24. En cas de manquement constaté à ses devoirs, le correspondant est déchargé de ses fonctions sur demande, ou après consultation, de la Commission nationale de l'informatique et des libertés. »

342. Dans l'entreprise, le correspondant est un intermédiaire entre le responsable de traitement et la CNIL. Sa désignation a pour avantage d'alléger les procédures au sein de l'entreprise puisqu'il permet de l'exonérer de toute déclaration préalable ordinaire ou simplifiée des articles 23 et 24 de la loi du 6 janvier 1978 modifiée. Le décret d'application n° 2007-451 du 25 mars 2007 fixe le cadre juridique de la mission du CIL au sein d'un Titre III intitulé « *Des correspondants à la protection des données* », il décrit ses modalités de désignation, les conditions d'exercice de sa mission ainsi que la fin de sa fonction[476].

Préalablement à toute information à la CNIL, la désignation d'un correspondant informatique et libertés doit être portée à la connaissance des organisations représentantes du personnel. Ensuite, cette nomination est notifiée à la Commission, par une lettre recommandée avec accusé de réception, dans laquelle la personne choisie comme correspondant à la protection des données à caractère personnel, a joint son accord par écrit. Par ailleurs, le responsable de traitement doit préalablement à la désignation du CIL informer les instances représentatives du personnel par lettre remise contre signature[477]. Cette disposition permet de les informer de la désignation d'une tierce personne en charge de certains traitements. La fonction de CIL s'adresse principalement aux groupes d'entreprises pouvant désigner en intranet, un correspondant qui sera compétent pour tout le groupe, en détachant des individus référents pour chaque filiale. En ce qui concerne les petites entreprises, elles ont la faculté de désigner un correspondant soit en interne, soit en externe avec la possibilité de mutualiser cette personne entre plusieurs entreprises[478].

Le rôle du CIL est de faire des recommandations, de conseiller le responsable du traitement qui le consultera pour toute mise en œuvre d'un nouveau traitement. Il doit aussi tenir à jour la liste des traitements automatisés mis en œuvre au sein de l'établissement. Il reçoit aussi les demandes et réclamations des personnes intéressées relatives aux traitements dont il a la charge. Il dresse un bilan annuel de ses activités qu'il présente au responsable de traitement et qu'il tient à la disposition de la CNIL. En cas de manquements constatés, il doit informer le responsable de traitement avant de saisir la Commission.

---

[476] Décret n° 2007-451 du 25 mars 2007 modifiant le décret n° 2005-1309 du 20 oct. 2005 pris pour application de la loi n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés, JO 23 mars 2007, p. 5782.
[477] Art. 45 du décret n° 2007-451 du 25 mars 2007 précité.
[478] M.-P. Fenoll-Trousseau, « Le correspondant informatique et liberté », JCP E 2005, 1771

Les règles relatives à la protection des données personnelles sont d'ordre public, leur non-respect est passible de sanctions pénales. Néanmoins, les contours de la responsabilité du correspondant sont encore flous. Le texte de loi et le décret ne prévoient pas, par exemple, de délégation de responsabilité du responsable de traitement au correspondant informatique et libertés comparable à celle existant en droit du travail.

En effet, la délégation de pouvoir, consacrée par la jurisprudence, permet à l'employeur de s'exonérer de sa responsabilité pénale dès lors qu'il a assigné au préposé une mission spécifique accompagnée de l'autorité, des moyens et de la compétence nécessaires à l'accomplissement de cette dernière[479]. On peut donc en conclure, en se référant à l'adage « *là où la loi ne distingue pas il n'y a pas lieu de distinguer* » que les correspondants informatique et libertés ne peuvent être tenus pénalement responsables en lieu et place du responsable de traitement. En revanche, l'article 22 III in fine de la loi de 1978 modifiée précise qu'il peut être déchargé de ses fonctions en cas de manquement constaté par le responsable de traitement après avis de la Commission ou par la Commission elle-même[480].

343. En matière de biométrie, il ne peut pas y avoir de dispense de déclaration pour la nomination du correspondant puisque les données concernées sont considérées comme sensibles, il est donc nécessaire de procéder aux déclarations préalables ou aux déclarations de conformité[481]. L'intérêt de sa fonction n'est donc pas dans la dispense de formalités mais sans doute dans la spécificité de sa mission. Le responsable de traitement peut lui confier comme tâche, de traiter uniquement les données biométriques afin de leur porter une attention particulière.

Le correspondant informatique et libertés reste normalement la personne la plus compétente au sein de l'entreprise pour procéder à ces traitements et s'assurer que les personnes qui en font la demande puissent être valablement informées et qu'elles puissent exercer leur droit

[479] Les règles de la délégation de pouvoirs sont issues de la jurisprudence de la Cour de cassation, cinq arrêts de la Chambre criminelle du 11 mars 1993 sont venus définir le régime de la délégation de pouvoir : « *Hors les cas où la loi en dispose autrement, le chef d'entreprise qui n'a pas personnellement pris part à la réalisation de l'infraction peut s'exonérer de sa responsabilité pénale s'il rapporte la preuve qu'il a délégué ses pouvoirs à une personne pourvue de la compétence, de l'autorité et des moyens nécessaires.* » n° 90-84.931, commentaire de Bernard Bouloc, RSC 1994 p. 101 ; Rec. Dalloz 1994 p. 156.
[480] Art. 52 et 53 du décret n° 2007-451 du 25 mars 2007 modifiant le décret no 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO 28 mars 2007, p. 5782
[481] Article 25 8° de la loi de 1978 modifiée.

d'accès ou d'effacement des données. A l'étranger, le correspondant a une mission de sensibilisation et de formation des employés au sein de l'entreprise. Ces missions « pédagogiques » sont tout à fait nécessaires pour informer les salariés sur la protection de leurs données personnelles et particulièrement en matière de biométrie.

344. La création du correspondant informatique et libertés a été vivement critiquée lors des débats visant à transposer la Directive 95/46 du 24 octobre 1995[482]. En effet, en principe, il doit être en mesure d'effectuer son travail librement et de respecter scrupuleusement ses obligations sans être inquiété dans l'exercice de sa mission. L'alinéa 3 de l'article 22 III de la loi de 78 modifiée l'énonce, « *il ne peut faire l'objet d'aucune sanction de la part de l'employeur du fait de l'accomplissement de ses missions*[483] ». Cependant, dans les faits, ce correspondant est souvent nommé au sein de grandes entreprises, où il fait déjà partie du personnel de cette dernière. Même s'il existe une incompatibilité de fonction entre celle de responsable de traitement et celle de correspondant informatique et libertés, le décret ne précise pas si cette fonction est conciliable avec celle d'un Directeur des ressources humaines ou d'un Directeur de la sécurité informatique.

Malgré son indépendance de principe, il fait généralement partie de l'entreprise et peut être soumis à de nombreuses pressions de la part de son employeur. Il y a donc des risques de conflits d'intérêts entre la fonction initiale qu'il exerce au sein de l'entreprise et celle de correspondant informatique et libertés. Cela soulève des interrogations sur la réelle indépendance du salarié qui agit comme correspondant alors que son contrat de travail le place en position de subordination vis-à-vis de son employeur. Comme le soulèvent Eric A. Caprioli et Isabelle Cantéro « *La loi ne met pas en place un statut de salarié protégé, réservé aux représentants du personnel et, dans ce cas, le CPDCP devra servir les intérêts de son entreprise tout en veillant au respect des dispositions légales et réglementaires. Ménager ces deux intérêts pourra, dans la pratique, donner lieu à quelques difficultés pour le CPDCP*[484] ». Le salarié doit pouvoir faire respecter les dispositions de la loi Informatique et libertés. En cas de conflit avec son employeur sur l'application de cette dernière, il a la faculté de saisir la

[482] G. Braibant, « Données personnelles et société de l'information », Rapport au Premier ministre sur la transposition en droit français de la directive n° 95/46, Doc. fr. janv. 1998, p. 45, disponible sur le site www.ladocumentationfrancaise.fr

[483] Article précité 22 III al. 3 de la loi n°78-17 du 6 janvier 1978.

[484] E. A. Caprioli, I. Cantéro, « Le choix d'un correspondant à la protection des données personnelles. », JCP E n° 25, 22 juin 2006, 1976.

CNIL « *des difficultés qu'il rencontre dans l'exercice de ses missions* ». Il doit en quelque sorte dénoncer les manquements de l'employeur auquel il est subordonné. Selon la CNIL, en 2009 près de 5500 entreprises ont nommé un CIL dont 90% sont dans le secteur privé. Nous déplorons l'ambiguïté du statut de salarié-CIL. Cette nouvelle fonction semble avoir un certain succès auprès des entreprises privées, le bilan apparaît pour l'heure positif[485].
Dans les faits les entreprises préfèrent recourir à un CIL extérieur à l'entreprise et il est sans doute préférable qu'il en soit ainsi afin de garantir l'exercice effectif de sa mission.

345. Le responsable de traitement ainsi que le correspondant informatique et libertés doivent accomplir valablement leur mission sous peine de sanctions (2°).

2°. Les manquements sujets à sanctions

346. Le fondement de l'obligation d'information réside dans le fait qu'aucun salarié ne doit être surveillé par un dispositif dont il ignore l'existence. Le responsable de traitement est garant de la sécurité des données mais il reste surtout l'interlocuteur privilégié des salariés, au sein de l'entreprise, sur la protection des données personnelles. Il doit être un vecteur de confiance, ne pas être l'objet de méfiance ou être considéré comme le « mandataire de surveillance » de l'employeur. De par l'importance de sa mission, il est nécessaire que des sanctions soient prises en cas d'inexécution ou de manquement à ses obligations.

347. Les articles 45 et suivants de la loi Informatique et libertés prévoient de nombreuses sanctions graduées à l'encontre du responsable de traitement qui n'aurait pas respecté scrupuleusement ses obligations. Les sanctions peuvent être prononcées par le biais d'une procédure normale (2-1) pour les manquements les moins graves. En cas d'urgence, une procédure spéciale est mise en œuvre pour faire cesser les violations aux droits et libertés (2-2). Enfin, pour les manquements les plus graves aux droits et libertés, une procédure juridictionnelle est engagée (2-3).

[485] CNIL, « Les CIL franchissent le cap des 5000 », article du 23 nov. 2009, www.cnil.fr

2-1. La procédure normale

348. Pour les manquements les moins graves, la CNIL peut prononcer un avertissement à l'encontre du responsable de traitement. Si ce dernier ne s'exécute pas, elle peut le mettre en demeure de faire cesser le manquement constaté dans un délai qu'elle fixe. Enfin, si le responsable de traitement n'entend toujours pas régulariser la situation, elle peut prononcer après une procédure contradictoire, des sanctions plus contraignantes : « ***1°*** *Une sanction pécuniaire, dans les conditions prévues par l'article 47, à l'exception des cas où le traitement est mis en œuvre par l'État* ».

Cette sanction est régulièrement employée par la CNIL, par exemple à l'encontre d'une SCP d'huissiers de justice qui avait enregistré des commentaires désobligeants sur des clients de l'étude ainsi que des données sensibles à l'encontre de ces derniers. Après une mise en demeure de la Commission, la SCP a persisté à collecter des données de santé. La CNIL a décidé de faire application de sanctions pécuniaires pour un montant de cinq mille euros[486]. Cette sanction a aussi été employée à l'encontre d'un employeur qui n'avait pas déclaré son traitement et qui n'avait pas valablement informé le personnel de l'usage de caméras de vidéosurveillance[487]. La CNIL a procédé à l'envoi d'une mise en demeure de procéder aux formalités dans un délai d'un mois. En application de l'article 47 I 1° une amende de 10 000 euros a été prononcée, avec publication de la décision sur le site internet de la Commission ainsi que sur le site legifrance.

Lors de ses contrôles, nous observons que la CNIL a pour vocation première la sensibilisation aux dispositions « informatique et libertés ». Les sanctions n'interviennent que dans un troisième temps, après un avertissement et une mise en demeure. Par ailleurs, la publicité des sanctions est particulièrement redoutable pour les entreprises puisque son rôle consiste à informer le grand public de l'absence du respect des règles de protection des données personnelles. L'impact économique est à craindre, puisque les partenaires ont aussi connaissance de ces mauvais comportements, ce qui donne une image négative de

[486] CNIL, Délibération n° 2006-173 du 28 juin 2006 prononçant une sanction pécuniaire à l'encontre de la SCP X, disponible sur le site www.cnil.fr
[487] CNIL, Délibération n° 2009-201 du 16 avr. 2009 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Jean-Marc Philippe, disponible au www.cnil.fr

l'entreprise. Les sanctions de publicité ont bien souvent plus d'impact sur les sociétés que les simples sanctions pécuniaires.

349. Le 2° de l'article 45 expose la possibilité qu'a la CNIL de prononcer « *Une injonction de cesser le traitement, lorsque celui-ci relève des dispositions de l'article 22, ou un retrait de l'autorisation accordée en application de l'article 25*[488] ». Les dispositifs biométriques sont visés par cette mesure car ils sont soumis à la procédure d'autorisation préalable de l'article 25 8° de la loi Informatique et libertés. Cette mesure a été employée récemment pour un traitement illégal des données biométriques.

350. Suite à une injonction de cesser le traitement restée infructueuse, la CNIL a dû avoir recours à la procédure d'urgence (2-2).

2-2. La procédure d'urgence

351. L'article 47 II de la loi Informatique et libertés dispose qu' - *En cas d'urgence, lorsque la mise en œuvre d'un traitement ou l'exploitation des données traitées entraîne une violation des droits et libertés mentionnés à l'article 1er, la commission peut, après une procédure contradictoire :*

***1°** Décider l'interruption de la mise en œuvre du traitement, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26, ou de ceux mentionnés à l'article 27 mis en œuvre par l'État ;*

***2°** Décider le verrouillage de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ;*

***3°** Informer le Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui sont mentionnés au I et au II de l'article 26 ; le Premier ministre fait alors connaître à la commission les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.*

[488] Art. 45 I 1° de la loi n°78-17 du 6 janvier 1978 modifiée

Cette procédure a été appliquée aux traitements biométriques mis en œuvre par une société d'habillement militaire qui a, malgré le refus d'autorisation de la CNIL, persisté à traiter les données biométriques de ses salariés. Le traitement illégal portait notamment sur l'enregistrement d'empreintes digitales avec, pour finalité, le contrôle d'accès aux locaux.

A la suite d'un contrôle sur place, la CNIL a envoyé une mise en demeure restée infructueuse. Même si la Commission a relevé l'absence de péril imminent, l'urgence est caractérisée « *dès lors qu'une circonstance est susceptible d'entraîner, s'il n'y est porté remède à bref délai, un préjudice grave et immédiat aux droits et libertés mentionnés à l'article 1er de la loi du 6 janvier 1978 modifiée. Une telle situation d'urgence s'apprécie au regard des intérêts qui sont en cause, de la gravité de leur atteinte ainsi que du nombre de personnes concernées*[489] ». La société avait une possibilité de recours à un dispositif biométrique alternatif à l'empreinte digitale, dans la mesure où les accès à protéger concernaient un local informatique et des bureaux. Le responsable de traitement procédait, depuis un certain temps, à l'authentification biométrique de ses salariés en l'absence d'autorisation et persistait à l'emploi de ce dispositif au jour de l'audience de la CNIL. Dès lors, la CNIL a ordonné l'interruption du traitement pour une durée de trois mois à compter de la notification de la décision. Pour que cette mesure soit efficace elle doit être appliquée par la société. Nous émettons des réserves en ce qui concerne l'exécution de cette décision par cette entreprise mais aussi en ce qui concerne la faculté de la CNIL, de contrôler dans le temps, le respect de cette mesure.

352. En toute hypothèse, lorsque les manquements persistent, la CNIL a recours à la procédure judiciaire (2-3).

[489] CNIL, Délibération n° 2010-072 du 18 mars 2010 de la formation restreinte décidant l'interruption d'un traitement mis en œuvre par la Société M., disponible sur le site www.cnil.fr

2-3. La procédure juridictionnelle

353. La procédure juridictionnelle est la dernière procédure que la CNIL peut mettre en œuvre en cas d'atteinte grave et immédiate. L'article 45 III de la loi Informatique et libertés dispose qu' *« en cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er, le président de la commission peut demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure de sécurité nécessaire à la sauvegarde de ces droits et libertés.* » La CNIL peut saisir la juridiction judiciaire ou administrative dans les dispositions de l'article 81 du décret de 2007 pris pour application de la loi Informatique et libertés modifiée.
Cette procédure n'est pas employée fréquemment car la CNIL parvient à faire cesser les traitements illégaux par les sanctions pécuniaires ou par le biais des sanctions de publicité, mais elle peut s'avérer utile si les manquements persistent.

354. Les responsables de traitement ont donc tout intérêt à respecter les différentes obligations disposées au sein de la loi Informatique et libertés. La loi n° 78-17 du 6 janvier 1978, prévoyait initialement l'obligation pour le responsable de traitement d'informer les salariés avant de procéder à tout traitement de données personnelles. Toutefois, les informations restaient insuffisantes. La loi n° 2004-801 du 6 août 2004 renforce les obligations incombant au responsable de traitement (B).

B. Le renforcement légal de l'obligation d'information

355. L'obligation d'information existait sous déjà dans la loi n° 78-17 du 6 janvier 1978. Toutefois, dans un souci de meilleure protection des individus, il était nécessaire de la rendre plus pragmatique, en adéquation avec les nouveaux outils de sécurisation. La loi Informatique et libertés modifiée distingue l'information obligatoire des personnes, visée à l'article 32, en ce qui concerne les traitements soumis à formalités préalables et de l'information « à la demande[490] » des intéressés visée à l'article 39[491].

L'obligation d'information découle du principe général de loyauté. L'article 6 1° de la loi n°78-17 du 6 janvier 1978 modifiée dispose que « *les données sont collectées et traitées de manière loyale et licite.* » La loyauté ou « la transparence[492] » dans l'information des personnes a été érigée comme principe fondamental au sein de l'article 7 de la Charte européenne des droits fondamentaux du 7 décembre 2000. Contrairement à la notion de traitement, la notion de collecte n'a pas été définie par la loi Informatique et libertés, néanmoins, la Cour de cassation a eu l'opportunité d'en donner une définition sous le visa de l'ancien article 226-18 du Code pénal. Pour elle, « *constitue une collecte de données nominatives le fait d'identifier des adresses électroniques et de les utiliser, même sans les enregistrer dans un fichier, pour adresser à leurs titulaires des messages électroniques*[493] ». La collecte ainsi définie ne se limite pas exclusivement à la conservation des données.

La collecte des données biométriques ne déroge pas à l'obligation d'information. Par ailleurs, cette information est double puisqu'elle concerne non seulement les salariés de l'entreprise mais aussi les représentants du personnel qui doivent être consultés préalablement à l'introduction de nouvelles technologies dans l'entreprise. L'information loyale peut être directement transmise par le responsable de traitement ou être obtenue par l'intermédiaire de la CNIL. En effet, la CNIL met à disposition du public la liste des traitements automatisés qui

---

[490] Document de synthèse établi par la direction des affaires juridiques, internationales et de l'expertise de la CNIL « La loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel : quels changements dans la loi Informatique et libertés du 6 janvier 1978 ? » disponible sur le site internet de la CNIL www.cnil.fr

[491] « I Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir … »

[492] Terme employé par le Conseil de l'Europe au sein d'un rapport « Les nouvelles technologies : un défi pour la protection de la vie privée ? », Strasbourg 1989, spéc. p. 38.

[493] Cass. crim., 14 mars 2006, Bull. crim., n° 69

a fait l'objet d'une des formalités prévues aux articles 23 à 27 de la loi Informatique et libertés modifiée[494].

356. La loi n°2004-801 du 6 août 2004 a renforcé les obligations incombant au responsable de traitement tant sur la transmission de l'information (1°) que sur la teneur de cette dernière (2°).

1°. L'information des salariés

357. Le responsable de traitement doit collecter loyalement les données personnelles des salariés (1-1) et les informer de leurs droits (1-2).

1-1. L'information loyale des salariés

358. Depuis 1804, l'article 1134 al. 3 du Code civil énonce que les « *conventions légalement formées doivent être exécutées de bonne foi* ». Le principe de loyauté, minimisé au XIX° siècle et pendant la première moitié du XX° siècle[495], trouve un nouveau souffle en droit du travail, pour lequel il est indispensable d'instaurer un rapport de confiance. La loi du 6 janvier 1978 modifiée par la loi n° 2004-801 du 6 août 2004 a vocation à règlementer tous les traitements de données personnelles. Elle interdit toute collecte de données par un moyen frauduleux, déloyal ou illicite[496]. Il s'agit là d'une application du principe de loyauté à la collecte des données personnelles. Par exemple, la CNIL estime déloyale, l'utilisation d'annonces qui ne correspondent pas à un poste à pourvoir, mais auraient pour seul objet de constituer un fichier de candidatures[497]. Ce n'est pas tant l'emploi d'un dispositif traçable qui est contesté mais l'ignorance de l'utilisateur sur son existence. L'information du salarié sur ses données biométriques doit être loyale, tant sur les éléments techniques du procédé

[494] Art. 31 I de la loi n° 78-17 du 6 janv. 1978 modifiée.
[495] B. Bossu, « Les notions fondamentales du droit du travail », sous la direction de B. Teyssié, collection Colloques, éd. Panthéon Assas, LGDJ, 2003, p. 185
[496] Art. 6 de la loi n° 78-17 du 6 janv. 1978 modifiée.
[497] CNIL, Délibération n°02-017 du 21 mars 2002 portant adoption d'une recommandation relative à la collecte et au traitement d'informations nominatives lors d'opérations de recrutement.

biométrique choisi, que sur l'exercice des droits sur des personnes concernées et sur le, ou les personnes chargées des traitements de données à caractère personnel[498].

359. En ce qui concerne les données biométriques dans l'entreprise, elles permettent d'identifier les salariés pour différentes finalités, comme le contrôle d'accès, celui des horaires ou de la gestion des ressources humaines. Généralement, à ces données biométriques sont associées des données identifiantes, comme le nom, le prénom et autres renseignements personnels ou professionnels en relation avec la finalité du traitement. La spécificité de ces données nécessite, à plus forte raison, qu'avant toute collecte, une information loyale soit donnée aux salariés. Avant toute implantation de dispositifs biométriques ou demande d'autorisation auprès de la CNIL, il est nécessaire de se conformer à l'obligation d'information.

Dès lors, deux sources du droit s'enchâssent. D'une part, il incombe au responsable de traitement d'informer les salariés conformément à l'article 32 de la loi n° 78-17 du 6 janvier 1978, d'autre part, le droit du travail précise la manière dont cette obligation d'information doit se matérialiser auprès des instances représentatives du personnel ainsi que des salariés. L'article L. 1222-4[499] du Code du travail impose à l'employeur d'informer personnellement les salariés et candidats à l'emploi, sur les dispositifs utilisés, comme des caméras de vidéosurveillance ou des dispositifs biométriques. Le défaut d'information est passible de sanctions pénales[500]. Le décret d'application de la loi de 1978 modifiée renvoie à l'article R. 625-10 du Code pénal lequel punit de l'amende prévue pour les contraventions de la cinquième classe le fait notamment de ne pas informer la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant[501].

360. Le droit du travail et la loi Informatique et libertés sont complémentaires en ce qu'ils mettent en exergue la transmission de l'information aux salariés (1-2).

---

[498] Infra n°365

[499] C. trav. anc. art. L. 121-8 « Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance. »

[500] C. pén. Art. 226-16 à 226-24

[501] Art. 110 du décret n° 2007-451 du 25 mars 2007 pris pour application de la loi n° 78-17 du 6 janv. 1978 modifiée, JO 28 mars 2007, p. 5782

1-2 La transmission de l'information

361. L'article 32 I de la loi Informatique précise que la personne « *est informée* » sur les données recueillies, sans préciser par quel biais elle peut l'être. Les modalités de transmission de l'information sont énoncées à l'article 90 du décret d'application de 2007 qui établit que les données sont portées à la connaissance des individus « *sur le support de collecte, ou à défaut, sur un document préalablement porté à leur connaissance en caractères lisibles* ».

Les informations peuvent aussi être communiquées par voie électronique ou par voie d'affichage. Le législateur a laissé le choix au responsable de traitement, d'employer le mode de transmission de l'information le plus efficace selon le fonctionnement de l'entreprise ou l'équipement des salariés. Par exemple, l'information par voie électronique sera pertinente si l'entreprise emploie couramment ce procédé et que les salariés disposent d'une adresse électronique.

La CNIL rappelle à ce titre, que l'information peut être transmise par tout moyen « *approprié*[502] » comme les panneaux d'affichage, une page « protection des données » ou « informatique et libertés » sur l'intranet de l'entreprise.
De ce point de vue, nous pensons qu'il serait judicieux d'intégrer les fournisseurs d'outils biométriques dans le processus informationnel. La finalité serait mieux appréhendée si les salariés bénéficiaient d'une présentation technique du dispositif. Cette pratique existe déjà dans certaines entreprises qui organisent, antérieurement à l'installation du nouveau système, des réunions d'information à destination des employés. Cela permet aux salariés utilisateurs de prendre entièrement connaissance des contraintes inhérentes à la biométrie mais aussi des avantages pratiques qu'ils peuvent en retirer. Une entreprise que nous avons interrogée[503], a déclaré avoir organisé une réunion d'information avec les fabricants de dispositifs biométriques afin d'expliquer aux salariés et représentants du personnel, la finalité du dispositif, son fonctionnement, les données collectées et la faculté de refuser le traitement. Par ailleurs, une note personnelle a été donnée à chaque salarié, associée à une mention sur le

[502] CNIL, Guide pour les employeurs et les salariés, éd. 2010, p. 5, disponible au www.cnil.fr
[503] Tel est le cas pour la société La Compagnie des desserts établie à Lézignan Corbières qui préalablement à l'implantation de son dispositif biométrique de reconnaissance du contour de la main a organisé une réunion d'information réunissant tous les salariés et représentants du personnel. http://www.polesud.org/

règlement intérieur[504]. Enfin, un affichage sur un panneau informatif visible et lisible par tous, a été disposé au sein de l'entreprise. Cette initiative pourtant très pragmatique n'est pas systématique. Il y a encore un assez grand nombre d'entreprises qui informe « a minima » les salariés, en affichant simplement sur le panneau central de l'entreprise l'existence du dispositif.

Nous proposons l'élaboration d'une note explicative précise et renforcée au besoin par des schémas clairs et colorés, pour décrire le nouveau système biométrique proposé, dans le but, d'instruire le salarié mais aussi de dédramatiser l'arrivée de la future installation.
Cette note serait systématiquement adressée aux salariés et devrait récapituler les informations préalablement relevées sur le traitement, les finalités du dispositif ainsi que les coordonnées claires et précises du responsable de traitement. La transmission de l'information est d'autant plus simplifiée que la CNIL propose des formules pré-rédigées à destination des responsables de traitement lesquelles s'adaptent à tous les procédés[505].

362. Enfin, l'implantation d'un dispositif biométrique, quelle que soit sa finalité, doit obligatoirement être inscrite dans le règlement intérieur qui traite de la sécurité et de la discipline[506]. Il n'est introduit, modifié ou retiré qu'une fois soumis préalablement au comité d'entreprise[507]. L'absence de consultation de ce dernier rend le règlement intérieur inopposable aux salariés. Notons qu'une charte informatique ou une note de service sont considérées en vertu de l'article L. 1321-5 du Code du travail, comme « *des adjonctions aux règlements intérieurs* ». Il est donc indispensable de privilégier le règlement intérieur pour toute information inhérente à la santé, la sécurité et les conditions de travail des salariés.

363. L'information est obligatoire mais son importance se mesure, autant à la valeur de son contenu qu'à la façon dont elle a été traitée (2°).

---

[504] Art. 1321-1 du Code du travail « *Le règlement intérieur est un document écrit par lequel l'employeur fixe exclusivement :*
1° Les mesures d'application de la réglementation en matière de santé et de sécurité dans l'entreprise ou l'établissement, notamment les instructions prévues à l'Article L4122-1 ;
2° Les conditions dans lesquelles les salariés peuvent être appelés à participer, à la demande de l'employeur, au rétablissement de conditions de travail protectrices de la santé et de la sécurité des salariés, dès lors qu'elles apparaîtraient compromises ;
3° Les règles générales et permanentes relatives à la discipline, notamment la nature et l'échelle des sanctions que peut prendre l'employeur. »
[505] CNIL, Guide pour les employeurs et les salariés, éd. 2010, p. 44 et suivantes, www.cnil.fr
[506] C. trav. article L. 1321-1
[507] C. trav. article L. 1321-4

2°. Le contenu de l'obligation d'information

364. Le contenu de l'obligation d'information a été élargi par la loi n° 2004-801 du 6 août 2004 bien qu'une majorité des obligations déjà existantes ont été reprises. Désormais, les personnes doivent être informées de l'identité du responsable de traitement, de la finalité du traitement, de l'existence du droit d'accès et d'opposition, des transferts de données envisagés vers des pays non membres de l'Union européenne. Lorsqu'il y a une collecte de données, qu'elle soit directe ou indirecte, le responsable de traitement doit informer toutes les personnes de l'entreprise concernées. L'article 11 de la Directive, imposait l'obligation d'information, seulement quand les données n'étaient pas prélevées de manière directe. Il s'agit là d'une nouvelle disposition, puisque la loi n° 78-17 dans sa rédaction initiale, n'obligeait pas l'entreprise à aviser le salarié pour une collecte indirecte de ses données.

Le contenu de l'information à donner aux salariés est énoncé à l'article 32 I de la loi de 1978 modifiée : « *la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant est informée, sauf si elle l'a été au préalable, par le responsable du traitement ou de son représentant :*
1°) De l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
2°) De la finalité poursuivie par le traitement auquel les données sont destinées ;
3°) Du caractère obligatoire ou facultatif des réponses ;
4°) Des conséquences éventuelles, à son égard, d'un défaut de réponse ;
5°) Des destinataires ou catégories de destinataires des données ;
6°) Des droits qu'elle tient des dispositions de la section 2 du présent chapitre (droits des personnes à l'égard des traitements de données) ;
7°) Le cas échéant, des transferts de données à caractère personnel envisagés à destination d'un Etat non membre de la Communauté européenne.

Lorsque de telles données sont recueillies par voie de questionnaires, ceux-ci doivent porter mention des prescriptions figurant aux 1°, 2°, 3° et 6°. »

365. Le responsable de traitement, son sous-traitant ou le CIL doivent être nommés, identifiables, c'est-à-dire que le salarié doit avoir leur identité complète mais ils doivent

surtout être accessibles. Aussi simple que cela puisse paraître, en pratique au sein de grandes entreprises, le responsable de traitement ne se situe pas sur le même lieu géographique que les salariés de l'entreprise. Il est nécessaire de s'assurer qu'il soit effectivement accessible, en donnant la totalité de ses coordonnées, son adresse e-mail ou un accès intranet permettant de le contacter rapidement. L'article 1222-4 du Code du travail rappelle à l'employeur qu' « *Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.* » Ce texte impose une obligation d'information préalable des salariés et « *découle clairement du principe de loyauté dans l'exécution du contrat de travail*[508] ».

366. L'indication de la finalité de traitement permet de préciser, dans un premier temps, les objectifs de l'entreprise dans le projet d'implantation d'un dispositif biométrique mais aussi de vérifier qu'elle s'y conforme, postérieurement à l'octroi de l'autorisation. Il est important que le salarié soit informé de la finalité en vue de laquelle le traitement biométrique intervient. L'information sur la finalité doit être réalisée avant la demande d'autorisation puisque la CNIL s'assure auparavant que l'obligation de consultation a été respectée.

367. En ce qui concerne les destinataires des données personnelles, le salarié doit être en mesure, comme le mentionne l'article 32 I 5° de la loi de 1978 modifiée, de savoir précisément quelles personnes peuvent accéder à ses données biométriques et les traiter. Ces personnes sont, par exemple, certains employés protégés lorsqu'un accord sur le temps de travail est passé, ou bien ce sont les personnels habilités des services de sécurité. Par ailleurs, ces destinataires sont souvent limités par la finalité du traitement biométrique au seul gabarit biométrique, sans qu'ils puissent procéder à une quelconque modification car ils sont limités par le temps puisque les données doivent être effacées. Le principe est simple : moins il y a de personnes destinataires ou utilisatrices des données biométriques, plus faible est le risque de détournement des données.

368. La méconnaissance de ces obligations est sujette à sanctions. Le décret de 2007 pris pour application de la loi n°78-17 du 6 janvier 1978 modifiée précise dans son article 90 que l'absence des mentions prescrites à l'article 32 de la loi (informations sur l'identité du

[508] L. Marino, « NTIC et droit du travail », Jurisclasseur communication, fasc. n° 4820, côte 08, 2005 p. 29.

responsable de traitement, sur la finalité, sur le droit d'accès de rectification ou d'opposition etc.) est punie d'une amende prévue pour les contraventions de cinquième classe.

369. Malgré l'élargissement du contenu de l'obligation d'information, subsistent, dans la loi Informatique et libertés, quelques zones d'ombre qui ne sont pas résolues par le Code du travail, particulièrement celles qui ont trait à l'information sur l'interconnexion des fichiers (2-1) et à l'information sur la durée de conservation des données personnelles (2-2).

2-1. L'information nécessaire mais aléatoire sur l'interconnexion des fichiers

370. L'interconnexion est un procédé qu'il convient préalablement de définir tant les approches diffèrent selon le domaine technique dans lequel elle intervient. Ainsi, l'article 32 9° du Code des postes et télécommunications électroniques (CPCE) en donne la définition suivante : « *On entend par interconnexion les prestations réciproques offertes par deux exploitants de réseaux ouverts au public qui permettent à l'ensemble des utilisateurs de communiquer librement entre eux, quels que soient les réseaux auxquels ils sont raccordés ou les services qu'ils utilisent.*
On entend également par interconnexion les prestations d'accès au réseau offertes dans le même objet par un exploitant de réseau ouvert au public à un prestataire de service téléphonique au public.) » Cette définition recouvre deux catégories de prestations différentes, d'une part la mise à disposition d'une liaison physique et logique pour un ou plusieurs opérateurs, d'autre part, une prestation de fourniture d'accès à un prestataire de service téléphonique au public. Dans le domaine « Informatique et libertés », la CNIL définit l'interconnexion comme « *tout traitement automatisé mis en œuvre par un ou plusieurs responsables qui consiste à mettre en relation (à corréler) des données ayant une finalité avec d'autres données ayant une finalité identique ou différente*[509] ». Cette dernière définition sera celle que nous retiendrons pour les développements successifs.

[509] CNIL, « Premières décisions de la CNIL en matière d'autorisations », Rubrique Commentaire, disponible sur le site internet www.cnil.fr

371. En biométrie, comme dans d'autres domaines liés aux nouvelles technologies, il existe une tendance à la collecte et au croisement de données à caractère personnel qui permettent de faire fonctionner plusieurs programmes entre eux. L'interconnexion est souvent évoquée lorsqu'il est question, pour les passeports biométriques, du croisement des données et de son impact sur la protection des données personnelles. A ce titre, le préposé fédéral à la protection des données personnelles suisse estime, quant à l'introduction de données biométriques dans les documents d'identité que « *seul un cadre légal rigide peut limiter les risques d'abus et de dérapages ainsi que le risque d'utilisation des données biométriques comme clés d'accès à diverses banques de données, et partant, d'interconnexion de différents fichiers*[510] ».

372. L'interconnexion n'est pas légalement délimitée en ce qui concerne les données biométriques. Le salarié est souvent mal informé sur le devenir de ses données (a) tandis que le responsable de traitement doit satisfaire à l'obligation de déclaration des fichiers interconnectés auprès de la CNIL (b).

a. L'information des salariés

373. En matière d'identification, l'interconnexion de fichiers comprend de nombreux risques qui sont à minimiser en matière d'authentification puisqu'aucune base de données n'est constituée. Par exemple, les entreprises peuvent interconnecter le gabarit du contour de la main avec des applications de gestion de la restauration ainsi qu'un système de paiement associé comme le permet l'autorisation unique n°AU-007[511].
Dans les deux cas l'information sur l'interconnexion des données n'est pas comprise dans les informations obligatoires à fournir directement au salarié avant de procéder à la collecte (art. 32 de la loi 78-17 du 6 janvier 1978). Le Code du travail reste quant à lui silencieux sur le contenu même de l'information à fournir.

[510] Préposé fédéral suisse à la protection des données et à la transparence (PFPDT), 15ème Rapport d'activité 2007-2008 « Introduction de données biométriques dans les documents d'identité. », p. 17, disponible sur le site internet au http://www.edoeb.admin.ch/
[511] CNIL, Délibération n° 2006-101 du 27 avr. 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail, JO n° 138 du 16 juin 2006, disponible sur le site internet au www.cnil.fr

Pourtant, l'information sur l'interconnexion des fichiers, n'est pas dénuée de tout intérêt car, même si les données biométriques ne donnent pas d'informations sur la santé, elles peuvent être dangereuses pour la vie privée si elles sont associées à d'autres données telles que les données d'identité ou professionnelles. Un code PIN peut être changé, ce qui n'est pas le cas des données biométriques. Les technologies biométriques sont de plus en plus utilisées dans les activités de la vie courante[512], les industriels développent des applications biométriques pour l'Internet. Deux solutions informatiques seraient envisagées. L'une, pour identifier les internautes, cette application nécessiterait alors de constituer une base de données, l'autre, pour authentifier le droit d'accès d'un internaute par l'intermédiaire d'une carte sur laquelle serait conservé le gabarit biométrique[513]. Ces applications ne sont pas encore mises sur le marché, mais si les données biométriques centralisées étaient interconnectées avec d'autres données comme des habitudes de consommation ou des données d'identité, il pourrait y avoir un détournement de finalités.

374. Si les salariés ne sont pas informés, les responsables de traitement doivent néanmoins déclarer les interconnexions de fichiers auprès de la CNIL (b).

b. L'information de la CNIL

375. L'employeur doit déclarer les interconnexions de fichiers directement auprès de la CNIL en vertu de l'article 30 I de la loi 78-17 du 6 janvier 1978 modifiée : « *les demandes d'autorisation et demandes d'avis adressées à la Commission nationale de l'informatique et des libertés en vertu des dispositions des sections I (déclaration) et 2 (autorisation) précisent : (...) 3°) Les cas échéant, les interconnexions, les rapprochements ou toutes autres formes de mise en relation avec d'autres traitements ;* »

Du point de vue procédural, la première interrogation est de savoir, si cette déclaration visée à l'article 30 I de la loi Informatique est distincte de celle prévue à l'article 25 8°) de la loi qui concerne la déclaration préalable des traitements biométriques, ou si elle doit être intégrée

[512] Supra n° 118 et s.
[513] J. Richiardi, Entretient sur les aspects techniques de l'application de la biométrie sur internet, disponible sur le site internet e-sens au www.e-sens.unige.ch

dans une même déclaration. Il faut distinguer la procédure d'autorisation préalable, de la procédure de déclaration de conformité.

Pour les autorisations uniques, visées à l'article 25 II de la loi Informatique et libertés modifiée, les interconnexions sont mentionnées, dès lors que le responsable de traitement ne procède pas à une autre déclaration. Par exemple, l'autorisation unique n°AU-007 permet les interconnexions entre la donnée biométrique du gabarit du contour de la main qui sert au contrôle d'accès, avec un programme de gestion des horaires de travail ou/et de restauration. Plusieurs combinaisons sont admises[514].

Pour la procédure d'autorisation préalable, il semblerait que le responsable de traitement doive procéder à une unique déclaration. L'article 30 I de la loi Informatique et libertés, intégré au sein de la section 3 intitulé « *Dispositions Communes* », exige pour les différentes procédures, les mêmes mentions dont celle sur les interconnexions. Le changement ultérieur des données non-conforme à la déclaration ou l'autorisation de traitement, oblige le responsable de traitement à informer sans délai la CNIL (article 30 II de la loi n°78-17 du 6 janvier 1978 modifiée).
Sur le fond, il est nécessaire de conserver une cohérence d'ensemble et de ne pas trop élargir les interconnexions, car s'il est estimé que la collecte de données biométriques est dangereuse, l'interconnexion de ces mêmes données peut avoir des conséquences bien pires. Les chances de détournement sont multipliées d' autant qu'il y a de personnes ayant accès à ces fichiers.
Il a été vu précédemment dans les autorisations uniques de la CNIL, que l'interconnexion est limitée aux finalités définies dans l'autorisation, mais surtout qu'elle intervient au niveau interne de l'entreprise. Pour les grandes entreprises qui disposent de filiales, une diffusion des données d'un site à un autre n'aurait aucun intérêt pratique, puisque la donnée biométrique du salarié est généralement valable localement, sur un site défini, tout comme l'interconnexion avec des applications de gestion des horaires ou/ et de restauration.

[514] CNIL, Délibération n° 2006-101 du 27 avr. 2006 portant autorisation unique AU-007 de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail, disponible sur le site www.legifrance.gouv.fr

Du point de vue de la CNIL, en vertu de l'article 31 de la loi 78-17 du 6 janvier 1978 modifiée, tout salarié peut demander à consulter ses données personnelles, détenues par l'entreprise.
Il est fondamental que les salariés concernés puissent avoir connaissance de l'existence de cette interconnexion, pour faire valoir utilement leurs droits. L'adjonction de cette information sur l'interconnexion garantirait sans doute une information du salarié plus complète et, par conséquent, plus loyale.

376. Si l'information sur la durée de conservation des données est généralement déclarée par le responsable de traitement, il serait toutefois nécessaire d'aller plus loin et d'instaurer une information obligatoire d'effacement de ces données à l'échéance de cette durée (2-2).

2-2. La carence de l'information sur la durée de conservation des données biométriques

377. La conservation des données traitées permet à une entreprise de les utiliser selon le besoin, conformément à la finalité, sans qu'il soit nécessaire de pratiquer une collecte systématique. Néanmoins, cette conservation n'est pas permanente mais limitée dans le temps, conformément à la finalité du traitement[515], qu'elle concerne le contrôle d'accès ou la gestion des horaires et de la restauration. Le fait de conserver des données personnelles est licite si ces données « *sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées*[516] ». Lorsqu'une entreprise établit une demande d'autorisation qui vise à implanter un dispositif biométrique, elle doit, en vertu de l'article 30 5° de la loi 78-17 du 6 janvier 1978 s'assurer que « *Les actes autorisant la création d'un traitement en application des articles 25 (autorisation par la CNIL) ... précisent :*
La durée de conservation des informations traitées. »

Cependant, ces délais ne coïncident pas forcément avec les obligations du Code du travail, notamment celles disposées à l'article L. 3245-1 qui concernent le délai de prescription des créances salariales[517]. C'est pourquoi, dans une délibération, la CNIL a échelonné les délais de conservation des données personnelles des salariés. Elles seront conservées de trois mois à cinq ans, au-delà du terme du contrat de travail[518], pour les déclarations de conformité à cette norme simplifiée, alors que les données relatives aux déplacements ne peuvent être gardées que trois mois. Pour les fiches de paie, les délais maximum de conservation sont aussi de cinq ans après le terme du contrat, mais de deux ans après le dernier contact avec le candidat à l'embauche, et d'un mois pour les enregistrements de vidéosurveillance[519].

---

[515] « *Les données à caractère personnel ne peuvent être conservées au-delà de la durée prévue au 5° de l'article 6 (durée nécessaire à la finalité) qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques ; le choix des données ainsi conservées est opérée dans les conditions prévues à l'article L. 212-4 du code du patrimoine* » Art. 36 1° de la loi 78-17 du 6 janv. 1978 modifiée.
[516] Article 6 5° de la loi 78-17 précitée
[517] « « *L'action en paiement ou en répétition du salaire se prescrit par cinq ans conformément à l'article 2224 du Code civil.* »
[518] CNIL, Délibération n° 02-001 du 8 janv. 2002 concernant les traitements automatisés d'informations nominatives sur les lieux de travail, pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration, disponible sur le site internet www.legifrance.gouv.fr
[519] CNIL, Guide pour les employeurs et les salariés, éd. 2010, p. 4, disponible sur le site internet www.cnil.fr

Les délais de conservation des données biométriques ne sont pas visés par cette délibération mais sont énoncés dans les autorisations uniques de la Commission et apparaissent systématiquement dans les autorisations préalables.

378. Quant à la finalité de contrôle d'accès, pour les dispositifs « à traces » comme l'empreinte digitale, la CNIL a estimé, dans l'autorisation unique AU-008[520], que la durée de conservation des données doit être égale au temps pendant lequel la personne concernée est habilitée à pénétrer dans les locaux ou les zones de haute sécurité. Ces zones sont rigoureusement délimitées par l'organisme demandeur de la restriction de circulation. Après le départ de l'employé, la durée de conservation peut être de cinq ans maximum alors que trois mois suffiront, à compter de la dernière venue d'un visiteur pour les données relatives à l'identité, à la vie professionnelle ou à la gestion du parking. Cette durée est de trois mois au maximum, pour les éléments relatifs au déplacement des personnes. Le stockage sur un support individuel ne pose pas de grande difficulté, le salarié devrait être informé des précautions à prendre tout comme cela existe pour les possesseurs de carte bancaire quant à cette conservation. Cette durée de conservation nous semble conforme à la finalité pour laquelle elle est requise. Néanmoins, à l'issue de ce délai le salarié devrait être informé de l'effacement de ses données.

379. Pour les dispositifs « sans traces » dont la finalité est le contrôle d'accès, deux autorisations uniques précisent les durées de conservation des gabarits biométriques. L'autorisation unique AU-007[521], concernant les dispositifs basés sur la reconnaissance du contour de la main, énonce que la durée de conservation du gabarit du contour de la main et du code d'authentification associé, est égale au temps pendant lequel elle est autorisée à accéder à ces zones. La conservation des données biométriques est donc liée à la fonction de la personne identifiée. C'est parce que la personne est employée par l'entreprise pour une fonction précise que ses données biométriques sont conservées au cours de la durée de son contrat. Il est nécessaire qu'elle ait accès à certaines zones protégées pour effectuer sa

[520] CNIL, Délibération n° 2006-102 du 27 avr. 2006, portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail, disponible sur le site www.cnil.fr

[521] CNIL, Délibération n° 2006-101 du 27 avr. 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail, JO n°138 du 16 juin 2006, disponible sur le site www.legifrance.gouv.fr

mission. En conséquence, il est plus compréhensible que le salarié soit identifiable pendant toute la durée de son contrat de travail.

En revanche, lorsque le responsable de traitement doit procéder à une demande d'autorisation préalable, il doit préciser la durée de conservation des données biométriques. La CNIL apprécie la conformité de ce délai à la finalité du traitement conformément aux dispositions de l'article 6 5° de la loi 78-17 du 6 janvier 1978[522]. Ainsi, par exemple, dans la délibération n° 2007-051 du 21 mars 2007[523] la société Millennium Chimicals Thann SAS a été autorisée à conserver le gabarit des empreintes digitales de ses salariés jusqu'au terme du contrat de travail.

380. En ce qui concerne les dispositifs ayant pour finalité la gestion des horaires et de la restauration, les applications entrent dans le régime de l'autorisation unique AU-007. Pour cette finalité, la durée de conservation du gabarit biométrique varie : elle est de trois mois pour les données monétaires en cas de paiement direct ou à l'avance, des repas et elle peut être portée à cinq ans, en cas de paiement par retenue sur le salaire. Cette durée est justifiée par la durée légale de conservation des documents administratifs en entreprise[524]. Par ailleurs, ce délai correspond aussi à celui de la prescription de la créance salariale de l'article L. 3245-1 du Code du travail.

Nous préconiserions qu'à l'issue de cette durée, un courrier papier ou électronique soit transmis au salarié par le responsable de traitement, son sous-traitant ou le correspondant informatique et libertés afin de l'informer de l'effacement de ses données personnelles.

381. Pour que le processus informationnel soit valable, le responsable de traitement doit consulter les instances représentatives du personnel avant l'introduction de nouvelles technologies (section 2).

---

[522] « *Un traitement ne peut porter que sur des données à caractère personnel qui satisfont aux conditions suivantes :*
5°) Elles sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. »

[523] CNIL, Délibération n°2007-051 du 21 mars 2007 autorisant la mise en œuvre par Millennium Chemicals Thann SAS d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles, disponible sur le site www.legifrance.gouv.fr

[524] Le Code de commerce impose, selon la nature des documents administratifs, une durée légale de conservation. Pour les actes de gestion du personnel la plupart du temps cette durée est de cinq ans.

Section 2. La consultation des représentants des salariés

382. Le rôle primordial des représentants du personnel est d'informer les salariés de l'entreprise sur les dernières lois les concernant. Ils sont particulièrement actifs lorsqu'il s'agit d'améliorer la négociation collective, en vue de la signature de conventions touchant la réduction du temps de travail, ou, autre exemple, à la mise en place du télétravail. Cependant, depuis quelques années, leur rôle est aussi de négocier l'introduction de nouvelles technologies dans l'entreprise. Le législateur, conscient de l'ampleur de ces mutations, impose donc à l'employeur de consulter les représentants des salariés sur ces questions. Consulter signifie, dans son sens premier, « *Demander à quelqu'un son avis, son conseil, chercher des renseignements auprès de lui ; interroger*[525] ». La jurisprudence, constante sur la signification de ce terme, énonce qu'il s'agit d'un échange de points de vue, d'une réponse de la direction aux questions pertinentes[526]. Tout refus de discussion est d'ailleurs considéré comme une entrave à la consultation.

Les salariés sont informés, mais seuls les représentants du personnel sont consultés sur le projet de l'insertion de nouvelles technologies. Cette différence terminologique apparaît dans le Code du travail où le terme « consultation » est employé pour les représentants du personnel alors qu'il emploie le terme « information » pour les salariés. La loi Informatique quant à elle, emploie invariablement les termes information et consentement puisqu'il est question d'individus et non uniquement de salariés. L'explication réside sans doute dans la fonction même des représentants des salariés au sein de l'entreprise. Pour des raisons de bonne organisation et d'efficacité, il semble plus aisé de communiquer avec un nombre plus restreint de salariés élus que de demander l'avis de l'ensemble des salariés.

383. L'employeur a le droit de contrôler l'activité professionnelle de ses salariés, toutefois, comme l'a rappelé la Cour de cassation, ce droit n'est pas illimité et reste conditionné. « *Si l'employeur a le droit de contrôler et de surveiller l'activité de son personnel durant le temps de travail, il ne peut mettre en œuvre un dispositif de contrôle qui n'a pas été porté préalablement à la connaissance des salariés*[527] ». Plus récemment la Cour de cassation a rappelé que « *L'employeur a le droit de contrôler et de surveiller l'activité de*

[525] Définition du dictionnaire Larousse, disponible sur le site www.larousse.fr
[526] Cass. crim. 4 juin 2002, n° 01-83.062, disponible au www.legifrance.gouv.fr
[527] Cass. soc. 20 nov. 1991, n° 88-43.120, Bull. civ. V, n° 519.

ses salariés pendant le temps de travail, l'emploi de procédés clandestins de surveillance étant toutefois exclu[528] ». Les employeurs avaient eu recours à des dispositifs de surveillance à l'insu de leurs salariés, pour prouver une faute professionnelle de leur part. Derrière l'usage illégal de ces dispositifs, l'employeur recherchait des preuves en vue de licencier un salarié, pour un usage abusif de l'Internet par exemple. L'emploi de nouvelles technologies est justifié si ce dernier s'accompagne de l'information et de la consultation des instances représentatives du personnel « *préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail*[529] ».

384. L'information faite aux représentants du personnel et la consultation qui a suivi, sont encadrées par le Code du travail qui en précise les modalités (A). Toutefois, en matière de consultation, leur rôle est limité puisque leur avis n'est que purement consultatif (B).

[528] Cass. soc. 14 mars 2000, n° 1270, n° 98-42.090, Bull. civ. V, n° 101 concernant un système d'écoute téléphonique.
[529] C. trav., art. L. 2323-13

A. Les modalités d'information et de consultation des représentants des salariés

385. Les organes représentatifs des salariés sont élus pour, bien sûr, les représenter et défendre leurs intérêts au sein de l'établissement dans lequel ils sont employés. A ce titre, ils doivent être valablement informés et consultés sur le projet qui vise à implanter une nouvelle technologie dans l'entreprise.

386. Ces organes représentatifs sont de diverses catégories selon l'importance du nombre d'employés. On parlera de comité d'entreprise, s'il y a cinquante salariés et plus[530] (1°), à défaut, le ou les représentants du personnel[531], selon les effectifs (l'article L. 2314-1 du Code du travail mentionne que ce chiffre est déterminé par décret), ensuite, le ou les délégués syndicaux, ainsi que le comité d'hygiène, de sécurité et des conditions de travail (CHSCT) constitué dans les établissements disposant d'au moins cinquante salariés[532] (2°). L'expert en technologie peut prendre part au débat en soutien pour fournir des éclaircissements ou explications (3°). Ces différents protagonistes ont pour point commun d'intervenir pour la protection des droits et libertés des salariés, dès lors qu'il convient de modifier les conditions de travail.

1°. La consultation du Comité d'entreprise

387. Dans tout établissement, l'implantation de nouvelles technologies peut amener une modification importante des conditions de travail. Un comité d'entreprise est créé dans chaque établissement employant au moins cinquante salariés[533]. Il assure l'expression collective des employés et s'attache à la défense de leurs intérêts, dans les décisions relatives à la gestion et l'évolution économique et financière de l'entreprise. Il a aussi un avis consultatif sur l'organisation du travail, la formation professionnelle et les techniques de production. C'est pourquoi, « *Le comité d'entreprise est informé et consulté sur les questions intéressant l'organisation, la gestion et la marche générale de l'entreprise et, notamment, sur*

[530] C. trav., art. L. 2321-1 et s
[531] C. trav., art. L. 2311-1
[532] C. trav., art. L. 4611-1
[533] C. trav. art. L. 2321-1

les mesures de nature à affecter le volume ou la structure des effectifs, la durée du travail, les conditions d'emploi, de travail et de formation professionnelle[534] ».

L'implantation d'un dispositif biométrique modifie, d'une part, l'approche de la sécurisation des locaux, en matière de contrôle d'accès, puisque les salariés devront employer un moyen d'authentification différent et d'autre part, elle modifie aussi la politique des ressources humaines lorsqu'il est question d'implanter un dispositif biométrique dont la finalité est la gestion des horaires ou de la restauration.

De plus en plus d'entreprises recherchent dans les applications biométriques, un dispositif qui permet d'effectuer plusieurs tâches. Par exemple, un dispositif de reconnaissance du contour de la main peut avoir une finalité initiale de contrôle d'accès mais aussi permettre de calculer le temps de présence ou la fréquence de passage. Plus de vingt-cinq ans après la loi du n° 82-915 du 28 octobre 1982, l'esprit du texte reste le même, soulève peu de contentieux et propose même quelques solutions sur le sujet.

388. Le législateur a introduit un mécanisme de consultation du comité d'entreprise par l'article L. 432-2 du Code du travail, actuel article L. 2323-13 du même code, en vertu duquel « *Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail.*
Les membres du comité reçoivent, un mois avant la réunion, des éléments d'information sur ces projets et leurs conséquences sur chacun des sujets mentionnés au premier alinéa. »

Selon sa nature et sa finalité, l'insertion d'un dispositif biométrique peut avoir pour conséquence la modification de l'organisation, de la gestion et de la marche générale de l'entreprise. Ce qui peut être le cas, par exemple, pour les dispositifs biométriques de reconnaissance du contour de la main, aux fins de gestion des horaires, qui nécessitent la formation du personnel sur l'utilisation de ce procédé et peuvent affecter l'organisation de l'entreprise.

[534] C. trav. art. L. 2323-6

389. L'information et la consultation s'effectuent sur la base d'un projet (1-1) car l'introduction de nouvelles technologies dans l'entreprise doit respecter certains critères (1-2). Le comité a la charge de la preuve du respect de ces conditions, soumises à l'appréciation souveraine des juges.

1-1. La présentation d'un projet

390. L'employeur informe puis consulte le comité d'entreprise en lui soumettant un projet d'installation de nouvelles technologies au sein de l'établissement. Il importe de savoir ce que l'on entend par « projet », car, ce n'est ni une esquisse[535], ni une étude préliminaire [536] mais celui-ci doit comporter des éléments nouveaux, importants et de nature à modifier de façon significative les conditions de travail. Le nombre de salariés concerné par la mesure peut être un indicateur de l'importance du projet[537]. Néanmoins, il ne doit pas forcément comporter de mesures précises et concrètes[538].

391. La lettre des textes reste muette sur le contenu exact de l'information à fournir lors de la consultation, elle précise cependant que « *pour lui permettre de formuler un avis motivé, le comité d'entreprise dispose d'informations* ***précises*** *et* ***écrites*** *transmises par l'employeur,* ***d'un délai d'examen suffisant*** *et de la réponse motivée de l'employeur à ses propres observations*[539] ». L'information doit être écrite et précise, comporter les éléments techniques de présentation de la technologie proposée, développer la finalité pour laquelle elle est requise, exposer les mesures de sécurité prises pour veiller au bon fonctionnement du système mais surtout elle doit mettre le personnel au courant, sur les conséquences à envisager avec l'implantation de ce dispositif, pour la santé, le travail ou les données personnelles des salariés. Les conséquences peuvent être d'ordre social, car pour les salariés, elles sont liées à l'acceptabilité de la technique biométrique, mais elles sont aussi d'ordre technique, par rapport à la collecte des données personnelles. Des contraintes physiques, environnementales ou économiques sont à envisager.

---

[535] Circ. DRT., n° 12, 30 nov. 1984, Dr. Ouv. 1985, p. 48
[536] Cass. soc. 3 mars 1988 Bull. civ. V, n° 152, D. 1988, somm. 312, obs. Lyon-Caen
[537] Cass. soc. 15 oct. 1987, Bull. civ. V, n° 569
[538] Cass. soc. 12 nov. 1997, Dr. soc. 1998, n° 87, obs. M. Cohen
[539] C. trav. art. L. 2323-4

Par ailleurs, le délai d'examen du projet doit être suffisant. Entre l'information et la consultation, le comité doit être en mesure d'effectuer ses propres recherches qui lui permettront d'émettre des observations voire de faire appel à des organismes spécialisés comme la CNIL, pour obtenir tous renseignements utiles. L'employeur doit répondre aux observations du comité d'entreprise, ce qui signifie qu'un échange doit s'établir.

392. La plupart des dispositifs biométriques sont implantés en vue du contrôle d'accès, du contrôle des horaires et de la gestion de la restauration ou de logiciels de fiches de paie. L'insertion de dispositifs biométriques peut faire l'objet d'un projet, s'il modifie l'organisation de l'entreprise et les conditions de travail des salariés (1-2).

1-2. Les caractères du projet

393. Le législateur a décrit les trois caractères, que doit comporter le projet soumis à la consultation du comité d'entreprise. Il doit être important, introduire de nouvelles technologies et être susceptible d'avoir des conséquences sur l'emploi, la formation ou les conditions de travail. L'importance du projet est appréciée à la lumière des modifications apportées dans l'organisation de l'entreprise, par exemple, lorsque l'introduction d'un nouveau système informatique affecte plus de six cents postes de travail et implique la formation du personnel[540]. En revanche, n'est pas important, le projet qui aboutit à l'introduction ultérieure d'un nouveau logiciel alors que l'entreprise est déjà informatisée.[541] L'implantation d'un dispositif biométrique satisfait à ce critère d'importance dans la mesure où il s'applique, la plupart du temps, à l'ensemble du personnel qui doit être sensibilisé sur la technique de reconnaissance, même si le dispositif implique l'installation d'une ou deux bornes sur l'ensemble des locaux.

De plus, le projet doit introduire une nouveauté technologique. Cette notion doit être appréhendée par « *l'importance du bouleversement concret subi à tous les niveaux de l'entreprise*[542] ». Les juges font une interprétation large du concept de nouveauté et considèrent notamment, que la technologie est nouvelle, lorsqu'un ordinateur de troisième

[540] Cass. soc. 28 oct. 1996, Dr. soc. 1996 n° 1105
[541] Cass. crim. 3 mai 1994, Bull. crim. 1994 n° 164 p. 375
[542] Cass. crim. 17 juin 1986, Dr. ouvrier 1987 n° 273, note J. G.

type, plus performant, vient remplacer un ordinateur du même type[543]. Il en va de même lorsque le nouveau procédé au sein d'une banque implique la formation de tout le personnel[544]. La biométrie est une technologie nouvelle qui bouleverse les schémas traditionnels de pointage et d'organisation de l'entreprise. Les salariés doivent se familiariser à ce nouveau dispositif d'identification qui peut réorganiser l'activité et s'interconnecter avec d'autres applications.

Enfin, le projet doit avoir une incidence sur les conditions de travail, de formation ou d'organisation de l'entreprise ou, tout au moins, une probabilité d'impacter sur ces éléments. Rares sont les projets qui ne remplissent pas ces conditions. Il est difficilement imaginable que l'insertion d'une nouvelle technologie n'ait aucune influence, ne serait-ce que sur les conditions de travail. La biométrie modifie la perception de la gestion des temps de présence. Les salariés ne sont plus seulement identifiés par un badge, mais aussi par ce qu'ils sont à travers la géométrie de leur main, le réseau veineux de leurs doigts ou de leurs empreintes digitales. A ce jour, nous n'avons pas connaissance de contentieux sur le projet d'insertion d'un dispositif biométrique.

394. Après avoir consulté le comité d'entreprise, l'employeur a pour obligation de consulter le CHSCT, organe directement concerné par ces mesures (2°).

[543] Cass. soc. 2 juill. 1987, Bull. civ. V, n° 438
[544] Cass. soc. 1997 RJS 11/1997 n° 1252; TPS 1997, n° 264, obs. Teyssié

2°. La consultation du CHSCT

395. La mise en place d'un Comité hygiène, sécurité des conditions de travail (CHSCT) est obligatoire au sein des entreprises qui ont un effectif supérieur à cinquante salariés pendant au moins douze mois consécutifs ou non au cours des trois années précédentes[545]. A défaut, les délégués du personnel ou les salariés remplissent ses fonctions. Le Comité a pour mission de contribuer à la protection de la santé mentale et physique des salariés, d'améliorer les conditions de travail et de veiller à l'observation des prescriptions légales dans ces domaines[546]. Le CHSCT est consulté « *avant toute décision d'aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail et, notamment, avant toute transformation importante des postes de travail découlant de la modification de l'outillage, d'un changement de produit ou de l'organisation du travail, avant toute modification des cadences et des normes de productivité liées ou non à la rémunération du travail*[547] ». A défaut, il a le pouvoir de suspendre et d'interdire la mise en œuvre du projet jusqu'à ce qu'intervienne la consultation[548]. Par ailleurs, le CHSCT peut faire appel au même expert en technologie que le comité d'entreprise et obtenir un complément d'expertise sur les conditions de travail[549]. L'expertise doit être effectuée dans le délai d'un mois avec la faculté de proroger ce dernier, tout en n'excédant pas un délai total de quarante-cinq jours. Les frais afférents sont supportés par l'employeur. En cas de contestation sur la nécessité, le coût ou la désignation de l'expert, le président du tribunal de grande instance, saisi en urgence, est compétent.

396. Le recours à l'expert n'est pas obligatoire, mais semble nécessaire, notamment pour donner des renseignements sur le ou les dispositifs biométriques à installer, dont les représentants des salariés ne connaissent pas vraiment le fonctionnement, les bénéfices et les inconvénients (3°).

---

[545] C. trav. art. L. 4611-1
[546] C. trav. art. L. 4612-1
[547] C. trav. art. L. 4612-8
[548] TGI Rouen, 6 juin 1996, Dr. ouv. 1997, p. 24
[549] C. trav. art. L. 4614-12 2°

3°. L'intervention facultative de l'expert en technologie

397. L'expert en technologie est une innovation de la loi n° 82-915 du 28 octobre 1982. Il peut être sollicité uniquement dans les entreprises qui comportent plus de trois cents salariés[550]. Sa désignation ne se matérialise que par l'accord entre l'employeur et la majorité des membres élus du comité d'entreprise[551]. L'accord porte sur le choix, l'étendue de la mission et la rémunération de l'expert. En tout état de cause, l'employeur est en mesure de s'opposer à la nomination d'un expert. En cas de litige entre le comité et l'employeur, le président du tribunal de grande instance, statuant en urgence, est compétent pour traiter du litige. La mission de l'expert consiste à fournir des explications et des éclaircissements au comité d'entreprise sur le projet d'introduction de nouvelles technologies. Comme la fonction d'expert en technologie n'est pas officiellement reconnue, toute personne dont les compétences sont respectées dans ce domaine, peut s'acquitter de cette mission et rien n'empêche que ce soit un salarié de l'entreprise. En matière de biométrie, il pourrait s'agir également d'un chercheur dans cette spécialité, ou bien d'un industriel qui expliquerait, notamment, la technicité du dispositif, son emploi, ses perspectives de développement, son coût et ses risques.

398. Incontestablement, il est nécessaire d'informer et de consulter les organes représentatifs, fervents défenseurs des intérêts des salariés. Néanmoins, il est regrettable que l'avis prononcé par ces derniers ne soit que purement consultatif ce qui entraîne des conflits (B).

[550] C. trav. art. L. 2325-35
[551] C. trav. art. L. 2325-38

B. La nature purement consultative de l'avis

399. L'article L. 2323-32 du Code du travail dispose que « *Le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de celles-ci.*
Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci.
Le comité d'entreprise est informé et ***consulté, préalablement*** *à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.* »

L'avis exprimé par les organes représentatifs n'est que purement consultatif et ne s'impose pas à l'employeur[552]. Rien, dans le texte, ne mentionne que le refus du comité d'entreprise lie l'employeur, dans le choix de la technologie à venir. A défaut d'être opposable, il ne faut pas négliger l'influence de cet avis sur des organismes extérieurs, comme la CNIL qui donne ou non les autorisations de traitements biométriques. Les articles 29 et 30 de la loi 78-17 du 6 janvier 1978 n'obligent pas les entreprises à fournir les justificatifs de consultation des organes représentatifs du personnel, mais nous supposons qu'ils seraient vivement appréciés par la Commission.

Toutefois, la jurisprudence nous a appris, qu'en matière de vidéosurveillance, certains de ces conflits internes n'avaient pour issue qu'une décision de justice. L'insertion d'un dispositif biométrique de reconnaissance par empreintes digitales n'a pas dérogé à cette issue. Gardons en mémoire les mésaventures de la société Effia Services et l'implantation de la pointeuse biométrique de gestion des horaires utilisant la technologie de l'empreinte digitale. Pour ce faire, elle a informé et consulté les salariés ainsi que les organes représentatifs du personnel conformément aux dispositions légales. L'avis consultatif du personnel n'a pas dû être entendu par le chef d'entreprise, car le syndicat des salariés, opposé au dispositif, a engagé une procédure devant le tribunal de grande instance de Paris. Les juges de premier degré ont entériné les formalités informatives et consultatives à l'attention du personnel de l'entreprise, mais ont rejeté le dispositif biométrique, jugé disproportionné aux finalités pour lesquelles il était sollicité. Malgré le respect des dispositions légales et le caractère purement consultatif de

[552] L. Marquet de Vasselot, De l'expression par le comité d'entreprise de son avis, RJS 8-9/00, p. 607

l'avis, c'est en définitive les arguments du syndicat qui ont été pris en compte[553]. Il importe de savoir quelle source de droit devait être privilégiée. Les magistrats ont visé, à juste titre, le Code du travail, pour valider le respect des formalités d'information des salariés et de consultation des instances représentatives du personnel.

Cependant, aucune disposition du Code ne permet d'apprécier la finalité et la proportionnalité d'un dispositif biométrique, pas plus que l'ampleur des restrictions apportées aux droits et libertés du salarié. C'est pourquoi les magistrats ont appliqué l'article L. 1121-1 du Code du travail, à la lumière des dispositions Informatique et libertés et des délibérations de la CNIL. Les deux sources de droit sont complémentaires et protègent, toutes les deux, l'information et le consentement des personnes. Cette décision est liée à un contexte particulier, en l'absence d'obligation d'autorisation préalable du traitement de ces données auprès de la CNIL. Néanmoins, il ne faudrait pas que ces confrontations conduisent systématiquement au procès.

Emettons l'hypothèse que les avis des organes représentatifs du personnel aient une force contraignante, l'employeur ne pourrait certainement pas exercer son pouvoir règlementaire et avoir recours, notamment, à la biométrie. Tout changement lié à une technologie serait sans doute perçu comme de l'espionnage et aboutirait à un refus. C'est pourquoi nous pensons que le projet de consultation devrait obligatoirement être transmis à la CNIL en pièce jointe à la demande d'autorisation. Les organes représentatifs auraient la garantie qu'un organisme tiers et neutre a tenu compte de leur position avant de se prononcer. La CNIL, de son côté, serait en mesure de s'assurer de la réalité de la consultation.

400. L'absence de consultation des organes représentatifs du personnel est sujette à sanction par la CNIL mais aussi par les tribunaux. La loi Informatique et libertés n°78-17 du 6 janvier 1978 modifiée prévoit dans son chapitre VII des sanctions que la CNIL peut prononcer à l'encontre du responsable de traitement qui ne se serait pas conformé aux obligations qui lui incombent[554]. Les sanctions vont du simple avertissement à la sanction pécuniaire. La Cour de cassation sanctionne l'absence d'information et de consultation[555] par le rejet de preuves établies par des moyens illicites (preuves issues de la vidéosurveillance ou d'enregistrements audio non autorisés).

[553] TGI Paris, 19 avr. 2005, Gazette du palais 2005 n° 202, p. 7, commentaire de E. Barbry, S. Rouillé-Mirza.
[554] Supra n° 346.
[555] Cass. soc. 7 juin 2006, n° 04-43.866, Girouard c/ Continent France, Bull civ. V, n° 206 ; D. 2006, 1704

401. L’information et la consultation des salariés sont un préalable à l’obtention du consentement au traitement de leurs données biométriques et à l’exercice de leurs droits actifs sans lesquels aucun traitement ne peut intervenir. (Chapitre 2).

Chapitre 2. L'exercice du consentement et des droits actifs des salariés

« *Science sans conscience n'est que ruine de l'âme*[556] ».

402. L'Histoire nous rappelle à quel point certaines découvertes technologiques ont des conséquences dommageables pour l'homme dès lors qu'elles sont utilisées de façon peu consciencieuse. Le choix de l'utilisation de certaines techniques biométriques comme mode d'identification[557] pourra s'avérer, s'il se systématise, irréversible sur l'anonymat des données et a fortiori sur la vie privée des individus. Ce choix doit donc être réfléchi mais surtout consenti par les personnes qui s'y soumettent.

Le consentement est la manifestation de la volonté ferme, claire et non équivoque qui détermine l'engagement d'une personne, dans un acte juridique, à un moment donné. Il est dans notre droit, un des quatre piliers des contrats, l'élément premier et déterminant de l'acte juridique[558]. Sans la rencontre des volontés et sa manifestation extériorisée, aucune convention ne peut voir sa réalisation juridique. Outre son exigence en matière contractuelle, il est indispensable dans bien d'autres domaines notamment en « informatique et libertés » où la collecte et le traitement des données personnelles ne peuvent se faire, sauf exceptions depuis la loi n° 2004-801 du 6 août 2004, sans l'accord de la personne concernée. L'exigence du consentement ne figurait pas dans l'ancienne rédaction de la loi. La personne avait la faculté de s'opposer à la collecte et au traitement pour des raisons légitimes. Désormais, le consentement a été érigé en règle de principe même s'il souffre de nombreuses exceptions.

403. L'article L. 1121-1 du Code du travail[559] limite le pouvoir règlementaire de l'employeur, en étendant à l'ensemble de la matière, les principes de finalité et de

---

[556] François Rabelais (1493-1553), Pantagruel, 1532, chapitre VIII, éd Garnier, 1884, p. 131

[557] Ce terme est pris dans son sens large comme évoqué dans l'introduction. Nous ne distinguons pas ici identification d'authentification, Infra p. 4.

[558] V. c. civ. art. 146 et 1108

[559] « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.* » Ancien article L. 120-2 du Code du travail.

proportionnalité, initialement proclamés pour le règlement intérieur[560]. Par ailleurs, lorsque l'employeur veut collecter et traiter les données personnelles de ses salariés, le Code du travail exige qu'il les informe et consulte les organes représentatifs du personnel.

Cependant, les règles du droit du travail traditionnelles ne prévoient pas de protection particulière lorsqu'il s'agit de traitement automatisé de données personnelles même si elles sont protectrices des droits et libertés des salariés. Ces dernières sont d'inspiration commune à la loi Informatique et libertés, qui proclame dans son article 1er 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.* »

C'est pourquoi la CNIL, autorité administrative indépendante, est bien fondée à veiller à la protection des données personnelles des salariés et exige du responsable de traitement qu'il obtienne leur consentement avant toute collecte. La plupart des autorités nationales de protection des données personnelles s'accorde à exiger, en matière de biométrie, le consentement de la personne. Surtout qu'en pratique, certaines applications biométriques cumulées à des applications de vidéosurveillance offrent la possibilité de contrôler l'activité des personnes sans avoir obtenu leur consentement préalable. Nous faisons allusion aux applications de reconnaissance faciale par lesquelles il est possible, à l'aide d'une photographie ou d'un film, de reconnaître une personne quelques années plus tard[561] alors que cette dernière n'a pas consenti à la capture de ses données. Cet exemple révèle que les technologies biométriques peuvent facilement être détournées de leur usage principal et employées à l'insu des personnes. Le consentement ne peut donc intervenir et être valable que dans la mesure où une information loyale et transparente a été donnée au salarié qui se prononce[562].

Cependant, pour certains traitements, l'article 7 loi Informatique et libertés n° 78-17 du 6 janvier 1978 modifiée prévoit le principe, mais aussi des exceptions, qui assouplissent

[560] Loi n° 82-689 du 4 août 1982, ancien article L. 122-35 du Code du travail
[561] La technologie de reconnaissance faciale a été employée notamment pour la photographie de Steve McCurry de la « jeune afghane aux yeux clairs » Sharbat Gula, alors âgée de douze ans, publiée dans National Geographics en 1985, afin de la retrouver quelques années plus tard dans un camp afghan. Cette technologie, employée à l'insu de Sharbat Gula, a permis de la reconnaître parmi plusieurs femmes qui se disaient être elle.
[562] Supra n° 332 et s.

incontestablement l'exigence de l'obtention du consentement de la personne. De ce fait, nous pouvons nous demander si, lorsqu'il s'agit d'un dispositif biométrique, le consentement du salarié est effectif dès lors qu'il fait partie d'un processus général de sécurisation de l'entreprise.

404. En biométrie, le recueil du consentement des personnes doit répondre à des exigences de fond et de forme (section 1). Cependant, ce consentement n'est pas figé, il est mouvant et peut changer. Le salarié a la faculté de s'opposer au traitement de ses données biométriques (section 2).

Section 1. La manifestation de la volonté du salarié dans l'environnement biométrique

405. Le consentement biométrique à la collecte de données au sein des entreprises, est généralement le résultat d'une information transparente et loyale mais aussi comme nous l'avons présenté précédemment, le fruit d'une consultation des organes représentatifs du personnel. Les salariés connaissent, en principe, les tenants et aboutissants de l'installation d'un tel dispositif et s'apprêtent à se prononcer sur le traitement de leurs données biométriques. Pour que le consentement soit valable, un certain nombre de conditions doit être réuni. Par ailleurs, le salarié a aussi la faculté de s'opposer à la collecte et au traitement des données s'il estime que le dispositif peut, par exemple, porter atteinte à sa vie privée ou que la sécurité des données n'est pas suffisante.

406. La spécificité de la donnée biométrique implique que le consentement du salarié sur la collecte de ses données personnelles, soit expressément déclaré (A). Ce qui exclut tout consentement tacite. A défaut, le salarié a la faculté de s'opposer au traitement de ses données biométriques (B), faculté qui, en pratique, peut être, difficile à mettre en œuvre.

A. Le consentement exprès biométrique

407. En droit français, le consentement peut être exprès ou tacite. Il est qualifié d'exprès lorsque la personne, libre de son choix, manifeste clairement son consentement. Il est tacite dès lors que le silence produit des effets sur le contrat (comme pour les contrats par tacite reconduction). En matière de traitement de données personnelles, le responsable de traitement doit collecter et traiter les données avec le consentement exprès des personnes.[563]

408. Le consentement exprès est une condition de licéité du traitement des données biométriques (1°), même si ce principe souffre de nombreuses exceptions (2°).

1°. Le consentement comme condition de licéité du traitement de données biométriques

409. Pour être valable, le responsable de traitement doit respecter des conditions de fond (1-1) et de forme (1-2) pour recueillir le consentement des salariés.

1-1. Les conditions de fond

410. L'article 1108 du Code civil dispose, et ce depuis 1804, que le consentement est l'une des conditions de validité des conventions[564]. A ce titre « *Il n'y a point de consentement valable, si le consentement n'a été donné que par erreur, ou s'il a été extorqué par violence ou surpris par dol*[565] ». La volonté détient une place essentielle dans la conclusion de l'acte juridique. Elle est le « *produit achevé d'une réflexion, d'une délibération éclairée par l'intelligence, elle est fondamentalement rationnelle*[566] ».

[563] Article 8 II 1° de la loi de 78-17 du 6 janvier 1978 modifiée
[564] C. civ., Art. 1108 « *Quatre conditions sont essentielles pour la validité d'une convention :*
Le consentement de la partie qui s'oblige ;
Sa capacité de contracter ;
Un objet certain qui forme la matière de l'engagement ;
Une cause licite dans l'obligation. »
[565] C. civ., Art. 1109
[566] M. Villey, « Essor et décadence du volontarisme juridique », Arch. phil. dr. 1957. 87

Par extension, le consentement du salarié est requis avant toute collecte et traitement des données personnelles. Cela implique que la volonté de la personne soit réelle, effective. Elle est le « *résultat d'une délibération mentale, la volonté juridique suppose chez son auteur, l'intention arrêtée de voir se réaliser l'opération qui constitue l'objet de l'acte*[567] ». Cela explique que toute personne ayant une absence de discernement ou des facultés mentales temporairement altérées ne puisse pas juridiquement agir. L'absence de consentement ou sa violation ont pour effet d'anéantir la convention.

411. La Directive n° 95/46/CE du 25 octobre 1995 sur la protection des données à caractère personnel définit le consentement dans l'article 2 intitulé « Définitions » comme « *toute manifestation de volonté,* ***libre****,* ***spécifique*** *et* ***informée*** *par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.* »

Le consentement exprès, par opposition au consentement tacite, doit émaner de la personne de façon ferme, claire et non équivoque. De plus, afin qu'il produise les effets juridiques escomptés, il doit être extériorisé. Le consentement à la collecte des données biométriques ne peut être qu'exprès comme tout autre type de traitement, « *la personne concernée a indubitablement donné son consentement*[568] » L'article 7 de la loi n° 78-17 du 6 janvier 1978 modifiée qui a transposé la Directive de 1995 reprend qu' « *Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée (...)* ». L'article 8 II 1° renchérit et exige pour certaines catégories de données, dont les données biométriques, que la personne concernée donne son consentement exprès. Les caractères du consentement ne sont pas mentionnés, en revanche, cinq exceptions à la liberté de consentir sont énumérées. L'exigence initiale du recueil systématique du consentement était bien trop restrictive pour être laissée en l'état. C'est pourquoi certaines exceptions ont été accordées. Nous étudierons ces réserves ultérieurement[569].

La Directive de 1995 caractérise le consentement comme devant être « *libre, spécifique et informé* ». Nous proposerions d'ajouter quelques caractères plus spécifiques à la biométrie comme l'exigence d'un écrit selon le seuil de risque encouru par la collecte ou

[567] C. Brenner, Chapitre 1er Théorie Générale de l'Acte Juridique in Répertoire de droit civil, Dalloz, sept. 2006
[568] Art. 7 a de la Directive n° 95/46 CE du 25 octobre 1995, JOCE L. 281/31, 23 nov. 1995, disponible sur le site internet
[569] Infra n° 417 et s.

l'interconnexion des fichiers, qui serait associé au recueil des données biométriques. Le point de départ de tout consentement est l'information. Une information loyale et transparente doit avoir été donnée au salarié préalablement au recueil du consentement par le responsable de traitement[570].

Par ailleurs, il n'y a pas de consentement de portée générale, il doit être spécifique, car il s'accorde étroitement avec la finalité du traitement qui va de pair avec un dispositif biométrique. En biométrie, le consentement sera octroyé uniquement pour le recueil et le traitement des données biométriques voire des données identifiantes connexes comme le nom, le prénom ou l'identifiant du salarié. Par exemple, le responsable de traitement obtiendra le consentement du salarié pour un dispositif de reconnaissance du réseau veineux des doigts de la main mais pour la seule finalité du contrôle d'accès. Le consentement ne peut, en aucun cas, être donné pour une autre de ces données biométriques, tels le contour de la main, la reconnaissance par empreintes digitales ou la reconnaissance vocale.
Il doit être explicite c'est-à-dire que le salarié doit affirmer clairement sa volonté de voir ses données biométriques collectées et traitées.

Enfin, le consentement doit être donné librement, et pour cela, l'intéressé doit connaître les implications et les conséquences qui découleront de son engagement. Il ne faut pas négliger l'aspect psychologique, car consentir au recueil de ses données personnelles représente une manifestation volontaire de l'individu, c'est une décision libre qui ne peut être obtenue par erreur, dol ou violence. A ce sujet, la jurisprudence précise que cette violence peut être physique ou morale[571]. La liberté de consentir à l'usage d'un dispositif biométrique quel qu'il soit, à traces ou non, n'est pas si évidente. En pratique, il est souvent difficile de connaître l'effectivité du consentement des personnes. Le refus d'un certain nombre de salariés a des répercussions financières sur l'entreprise dans la mesure où l'employeur sera dans l'obligation de conserver l'ancien dispositif de reconnaissance, associé au nouveau dispositif biométrique, ce dernier étant utilisé par la partie consentante du personnel. Toutefois, les pressions morales exercées au sein de certaines entreprises peuvent contraindre le salarié à consentir à l'emploi d'un dispositif biométrique, alors qu'il émet quelques réserves sur ce dernier.

[570] Supra n° 358 et s.
[571] Exemple Civ 1ère, 29 juin 1999, JCP 1999. II. 10187, note R. Martin

412. Une des garanties de la validité du consentement réside dans la mise en place de conditions de forme (1-2).

1-2. Les conditions de forme

413. Le consentement à l'identification biométrique comprend l'élément moral inhérent à toute manifestation de volonté et sa matérialisation physique dès lors que le salarié procède à l'enrôlement. L'élément moral est d'une nature particulière puisque la personne va consentir à une collecte de données personnelles dans le cadre de son travail, contrairement à la « biométrie de confort » et aux passeports biométriques, où l'individu fait le choix délibéré de recourir à la biométrie, pour son confort personnel ou pour voyager. C'est pourquoi, nous pensons que le consentement devrait être mentionné par écrit systématiquement d'autant plus si une base de données biométriques est constituée.

Pourtant, la Directive de 1995, dans son « Considérant » 30, soumet la licéité des traitements à l'obtention du consentement de l'intéressé sans exiger des Etats membres la mise en place de conditions de forme[572]. La loi Informatique et libertés n'est pas allée plus loin que la Directive puisqu'elle n'impose pas de conditions formelles et n'oblige pas le responsable de traitement à recueillir le consentement du salarié par écrit. Dans les formulaires de déclaration en ligne, la CNIL n'exige pas plus que le déclarant apporte la preuve du consentement des salariés. Les inconvénients souvent avancés sont la lourdeur administrative et le coût engendré par la procédure. Néanmoins, ces arguments ne sont pas recevables puisque la signature d'un formulaire écrit pourrait intervenir lors de l'information des salariés à l'occasion, par exemple, d'une réunion avec l'intégrateur du dispositif biométrique. Ainsi, le consentement écrit ne se matérialiserait donc pas simplement dans la signature de l'accord, mais s'inscrirait dans une démarche générale de compréhension des implications de la collecte et de l'usage des données biométriques.

[572] (30) « considérant que, pour être licite, un traitement de données à caractère personnel doit en outre être fondé sur le consentement de la personne concernée » Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO n° L 281 du 23 nov. 1995 p. 0031 – 050

414. La loi canadienne sur la protection des renseignements personnels et les documents électroniques (LPRPDE) exige sauf exceptions limitativement énumérées, qu'une organisation communique les renseignements personnels des individus avec le consentement de la personne. Au Québec, l'article 44 de la loi concernant le cadre juridique des technologies de l'information énonce que « *Nul ne peut exiger, **sans le consentement exprès de la personne**, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. L'identité de la personne ne peut alors être établie qu'en faisant appel au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose et que parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance*[573] ».

Le consentement d'une personne au recueil des données biométriques est exprimé au sein d'un formulaire que le salarié doit remplir[574]. Ce formulaire doit impérativement être joint au dossier de déclaration d'une banque de caractéristiques ou de mesures biométriques[575], sous peine d'irrecevabilité du dossier. Dans ce formulaire, l'entreprise doit fournir tous les renseignements la concernant, prouver le consentement de la personne et indiquer un mode alternatif à la biométrie qui pourrait être proposé aux personnes s'opposant à ce système de traitement. En l'absence de mode alternatif, l'entreprise doit justifier la nécessité, pour elle, d'avoir recours à la biométrie avec documents à joindre, prouvant cette nécessité au regard de la finalité du traitement. Nous préconiserions, en France, l'emploi de ce même type de formulaire à joindre à la demande d'autorisation de traitement à la CNIL.

415. La biométrie est souvent intégrée au sein d'un projet global de sécurisation ou de ressources humaines. Au sein des entreprises, le consentement peut parfois être biaisé et donné sous le poids de « pressions » conscientes ou non des chefs d'entreprise. Le salarié doit avoir le choix d'accepter ou de refuser d'utiliser la biométrie. En cas de refus de ce dernier, l'employeur devrait avoir pour obligation de trouver une solution alternative. Idéalement, c'est ce qui est préconisé, mais pour des raisons de coût, les deux méthodes sont souvent difficiles à conserver en même temps. En matière de gestion des horaires, un salarié qui

[573] L.R.Q., chapitre C-1.1 site internet : http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_1_1/C1_1.html
[574] Cf. Annexe 4
[575] Le Québec emploie une procédure de déclaration et non d'autorisation préalable. Les entreprises doivent joindre plusieurs documents garantissant la sécurité des données, l'information des personnes et la destruction des données au terme de la finalité du traitement.

s'oppose à un dispositif de reconnaissance du contour de la main devrait pouvoir conserver son badge et son code pin. Seulement, cette liberté a un coût d'entretien important et en pratique les salariés réfractaires pourraient céder sous la pression du plus grand nombre.

416. Tout en étant érigé comme principe, il n'en reste pas moins que le consentement exprès peut souffrir de quelques réserves (2°).

2°. Les réserves quant à l'exercice d'un consentement exprès

417. Avec la signature du contrat de travail, le salarié abandonne une part de sa liberté individuelle pour être subordonné à son employeur. Cette subordination néanmoins limitée aux horaires et missions du contrat de travail, peut aboutir à réduire la sphère de libertés individuelles octroyées au salarié. Ainsi, l'article 7 de la loi n°78-17 du 6 janvier 1978 prévoit plusieurs exceptions à la liberté de consentir et précise qu'« *Un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée ou satisfaire à l'une des conditions suivantes :*
***1°** Le respect d'une obligation légale incombant au responsable du traitement ;*
***2°** La sauvegarde de la vie de la personne concernée ;*
***3°** L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;*
***4°** L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;*
***5°** La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée* ». Cette dernière exception peut être invoquée par les entreprises pour outrepasser le consentement des salariés.

La notion d'intérêt légitime peut recouvrir plusieurs sens. Sur ce point, le rapport n° 218 du Sénat[576] précise la portée générale de cette dernière exception. Elle émane de la Directive de

[576] Sénat, Rapport de la session ordinaire 2002-2003, au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale sur le projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi

1995 qui ne donnait elle-même aucune précision. Quelques exemples étaient présentés mais ils ne couvraient pas la majeure partie des finalités de traitement utilisée par le secteur privé. Le rapport précise d'ailleurs que « *Cette clause de sauvegarde pourrait à terme recouvrir la majorité des traitements du secteur privé et il appartiendra à la CNIL de veiller au respect d'un équilibre, par son contrôle a priori ou a posteriori, sans préjudice de l'éventuelle appréciation ultérieure du juge en cas de contentieux* ».
Dans sa délibération, la CNIL a refusé l'application de l'article 7 5° à la société Manpower qui souhaitait ajouter, au sein d'un fichier, le numéro de sécurité sociale pour faciliter la gestion des salariés intérimaires[577]. La société invoquait « *l'intérêt légitime d'identifier de manière fiable les intérimaires afin d'éviter les risques de confusion d'identité dû à des phénomènes d'homonymie et d'erreurs d'orthographe empêchant les intérimaires de faire valoir leur droit, ou ayant des conséquences directes sur l'instruction des dossiers d'embauche ou encore étant susceptible de causer un préjudice tant aux intérimaires qu'aux entreprises utilisatrices* ». La CNIL a reconnu que le risque d'homonymie était une préoccupation justifiée des responsables de traitement, mais qu'il existait d'autres solutions que la collecte de cette donnée.

418. Le chef d'entreprise dispose d'un pouvoir règlementaire envers ses salariés qui lui permet de décider du choix d'une stratégie de gestion de son entreprise. La biométrie est un mode d'identification rapide, plus ou moins coûteux selon les dispositifs, qui assure rentabilité et fiabilité. Néanmoins, une entreprise qui a recours à la biométrie pourrait-elle employer l'intérêt légitime visé par l'article 7 5° de la loi pour contraindre ses employés à utiliser un dispositif biométrique ?

En France, nous pourrions répondre par la négative. La CNIL effectue un contrôle a priori et a posteriori des demandes, elle ne permettrait sans doute pas qu'une entreprise outrepasse le consentement de ses salariés si l'intérêt visé par l'entreprise ne concerne qu'une facilité de gestion, une amélioration de son rendement. Par ailleurs, si une telle restriction échappait au contrôle de la CNIL, les représentants des salariés, voire les salariés eux-mêmes ne manqueraient pas d'engager une action en justice pour faire reconnaître leurs droits et laisser

n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés, p. 57, disponible sur le site internet www.senat.fr

[577] CNIL, Délibération n° 2009-576 du 20 oct. 2009 refusant d'autoriser la mise en œuvre par la société Manpower France d'un traitement automatisé de données à caractère personnel utilisant le numéro de sécurité sociale et ayant pour finalité la gestion des salariés intérimaires, disponible sur le site www.legifrance.gouv.fr

une telle clause à l'appréciation d'un juge. Elle n'a pas changé sa position sur ce sujet puisque des délibérations antérieures aboutissent au même résultat[578].

Peu de litiges devant les tribunaux sont fondés sur cette disposition. Néanmoins, la décision du tribunal de grande instance de Paris statuant en référé peut nous éclairer. La SARL Note2be.com avait créé un site internet dont l'objet était d'inviter les élèves à noter leurs professeurs sur six critères, nominativement désignés, sans le consentement de ces derniers. Certains enseignants visés et leur syndicat ont alors engagé une action en justice visant à faire retirer le site internet. La société, pour se conformer à la loi Informatique et libertés, devait soulever une des exceptions visées à l'article 7. Elle a invoqué l'article 7 5° en vertu duquel le consentement de la personne n'est pas requis, si le responsable de traitement poursuit un intérêt légitime qui consiste à faire valoir la liberté d'expression de ses utilisateurs.

Toutefois, le magistrat a procédé à une étude précise sur la proportionnalité au regard des faits qui lui étaient présentés. Selon lui, les critères observés pour évaluer les enseignants amènent à biaiser l'évaluation. Il ajoute : « *Le simple fait que le site est ouvert à tous est pourtant de nature à rendre bien théorique la possibilité d'un équilibre entre les intérêts des « évaluateurs » et ceux des « évalués ». En effet, rien dans la décision n'indique que le site vérifiait que la personne qui notait avait qualité pour le faire : avait-elle effectivement suivi les cours de l'enseignant concerné ? Dans ces conditions, on pouvait aussi s'interroger sur les modalités de la collecte des données : elle n'était vraisemblablement pas « loyale et licite » au sens de l'article 6, 1°, de la loi de 1978 !* [579] ». La SARL a été condamnée à suspendre sur son site l'utilisation de données nominatives ainsi qu'au paiement d'une somme provisionnelle de un euro pour chaque demandeur. Cette décision a été frappée d'appel, sans succès pour la SARL[580]. Les magistrats ont apprécié l'intérêt légitime par rapport au principe de proportionnalité et des intérêts opposés de chaque partie. Sur cette question, le droit comparé nous paraît particulièrement intéressant.

---

[578] CNIL, Délibération n° 2005-199 du 22 sept. 2005 portant refus d'autorisation de mise en œuvre par la société Volkswagen Finances d'un traitement automatisé de données à caractère personnel ayant pour finalité l'utilisation du numéro de sécurité sociale à des fins de détection d'incohérence dans les demandes de crédit, disponible sur le site www.legifrance.gouv.fr

CNIL, Délibération n° 2006-043 du 23 fév. 2006 portant refus d'autorisation de mise en œuvre par le GIE 50 d'un traitement automatisé de données à caractère personnel portant sur l'utilisation du numéro de sécurité sociale à des fins de "gestion de la relation client en mode multi-canal", disponible sur le site internet www.cnil.fr

[579] TGI Paris, ordonnance des référés du 3 mars 2008, n° 08-51650, disponible sur le site www.dalloz.fr

[580] CA Paris, 25 juin 2008, n° 08-04727, disponible sur le site www.dalloz.fr

419. Au Canada, les solutions varient selon les législations provinciales ou la législation fédérale. Au Québec, il n'y a pas d'exception au consentement exprès préalable au traitement. Par conséquent, il est impossible que l'employeur traite les données d'un salarié si ce dernier n'y a pas consenti. En Colombie britannique, la loi prévoit pour le secteur privé, des exceptions à l'obtention du consentement. Pour certains traitements biométriques, le consentement des salariés n'est pas requis si le dispositif biométrique choisi par l'employeur est raisonnable et légitime, au regard des intérêts économiques de son entreprise[581]. Pour ce faire, il doit démontrer que les inconvénients occasionnés sur la vie privée sont minimes et en relation directe avec les besoins et intérêts économiques de l'entreprise.
La loi fédérale canadienne sur la protection des renseignements personnels et les documents électroniques prévoit dans son article 7, toute une série de situations dans lesquelles le responsable de traitement peut collecter et traiter les données personnelles d'un individu sans obtenir son consentement. Particulièrement si l'entreprise se conforme à l'article 5 3°) de la loi, dont la formulation, relativement vague, laisse une grande place à l'interprétation prétorienne : « *L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances*[582] ».

Dans l'affaire Wansink, c'est ce dernier fondement qui a été invoqué. L'employeur avait obtenu le consentement de la majorité de ses salariés mais quelques réfractaires s'opposaient à la mesure. Le dispositif choisi par l'employeur, consistant à relever des empreintes vocales, était raisonnable au regard de la finalité de gestion des horaires. La cour d'appel fédérale a donné raison à l'employeur[583] car le risque de divulgation des données personnelles était minime et que les voix originales n'avaient pas été conservées. Les salariés ne pouvaient pas raisonnablement s'opposer à la collecte de leurs empreintes vocales pour générer des mots de passe.

Certes, le consentement des salariés peut souffrir de quelques exceptions, mais elles ne sont reconnues en France, comme à l'étranger, que de façon restrictive. Nous n'avons pas de

[581] Office du commissaire à la protection des données et informations de Colombie Britannique, Personal Information Protection Act (PIPA), art. 6 et s., 23 oct. 2003, SBC 2003, disponible sur le site http://www.oipc.bc.ca/
[582] Loi sur la protection des renseignements personnels et les documents électroniques canadienne, 2000, disponible sur le site internet du ministère de la Justice canadien, http://laws.justice.gc.ca/fr/
[583] Affaire *Wansink v. Telus Communications Inc.* (F.C.A.) 2007 FCA 21, disponible sur le lien suivant : http://www.canlii.org/

jurisprudences en ce qui concerne des traitements biométriques, mais nous supposons que la CNIL serait particulièrement vigilante et ne tolèrerait cette exception au recueil du consentement que dans les hypothèses d' « un fort impératif de sécurité ».

420. Si le consentement souffre de quelques exceptions, la loi Informatique et libertés ne prévoit aucune dérogation à l'exercice du droit d'opposition du salarié au traitement des données biométriques (B).

B. La faculté d'opposition du salarié à la collecte des données biométriques

421. La faculté d'opposition, tout comme le consentement préalable, est une manifestation de la volonté du salarié. Néanmoins, comme l'obtention du consentement préalable souffre de quelques dérogations, le droit d'opposition est en pratique plus exercé[584]. C'est la faculté dont dispose une personne, de s'opposer au traitement de ses données personnelles, pour des motifs légitimes, sauf s'il s'agit d'une obligation légale ou règlementaire comme c'est le cas pour les déclarations sociales obligatoires ou le registre du personnel. En principe, toute personne peut exercer son droit d'opposition au traitement de ses données personnelles, dès lors qu'elle a été valablement et préalablement informée du traitement de ces dernières.

422. Sous l'empire de la loi de 1978, ce droit ne pouvait être exercé que sous réserve d'avancer « un motif légitime », sans qu'il soit opéré de distinction selon les catégories de données. A défaut de précisions sur ce que recouvrait ce critère, certains auteurs ont donné quelques pistes permettant d'apprécier le motif légitime. Il s'agirait des « *informations susceptibles de nuire à la vie privée*[585] », « *la personne intéressée pouvant estimer que l'enregistrement porte atteinte à son identité humaine, à ses droits d'homme et de citoyen, à sa vie privée ou à ses libertés individuelles ou publiques*[586] ».

---

[584] Y. Detraigne et A.-M. Escoffier, Rapport d'Information au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques, n°441, 27 mai 2009, p. 40, consultable au www.senat.fr

[585] A. De Laubadère, « loi relative à l'informatique, aux fichiers et aux libertés », ADJA 1978 p. 150

[586] X. Linant de Bellefonds et Hollande A., Pratique du droit de l'informatique, Delmas, 2002, M 1326

Aucune indication supplémentaire n'a été apportée par l'article 38 de la loi 78-17 du 6 janvier 1978 modifiée qui énonce que « *Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.*
Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur.
Les dispositions du premier alinéa ne s'appliquent pas lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement ». La précision apportée par la loi n° 2004-801 du 6 août 2004 concerne la prospection commerciale, pour laquelle le droit d'opposition s'exerce sans perception de frais ni motifs. Toute violation de ce droit constitue une infraction prévue à l'article 226-18-1 du Code pénal[587]. L'article 226-24 du même Code[588] prévoit l'engagement de la responsabilité pénale de la personne morale.

C'est sur ce fondement que la CNIL a engagé la procédure contre l'Eglise de Scientologie en 2004. La Cour de cassation a reconnu la légitimité du droit d'opposition dans un arrêt du 28 septembre 2004. Elle a estimé « *d'une part que le droit d'opposition peut valablement être exercé par l'intermédiaire de la CNIL et d'autre part qu'en matière politique, philosophique ou religieuse, la légitimité de l'opposition est remplie par le seul exercice de cette faculté*[589] », s'agissant de deux personnes qui ont fait l'usage de leur droit d'opposition auprès de la CNIL à ne plus apparaître sur les fichiers de l'ASESIF (Eglise de Scientologie). L'ASESIF avait faussement indiqué l'effacement des données personnelles et a doublement été condamnée pour délit d'entrave et délit de traitement de données nominatives malgré opposition.

---

[587] C. pén. Art. 226-18-1 *(L. n° 2004-801 du 6 août 2004, art. 14)* « *Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende* ».
[588] C. pén. Art. 124 (*Loi n°2009-526 du 12 mai 2009*) « *Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies à la présente section encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par les 2° à 5° et 7° à 9° de 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 ».
[589] Cass. Crim 28 sept. 2004 n°03-86.604, Bull. crim. 2004 n° 224 p. 801

Cette décision nous inspire plusieurs commentaires : le droit d'opposition peut valablement être exercé par l'intermédiaire de la CNIL, même s'il s'agit d'un droit personnel. Par ailleurs, la Cour a estimé que la collecte de certaines données d'ordre politique, philosophique ou religieux constituait un motif légitime. Cette liste ne se veut pas restrictive et peut être élargie aux données biométriques selon le contexte dans lequel ces dernières sont utilisées.

423. En effet, comme rappelé précédemment, les données biométriques, sont des données identifiantes, impliquant le corps humain. Ces données ne sont pas toutes équivalentes, car certaines pourraient être considérées comme portant plus facilement atteinte aux individus, par exemple les empreintes digitales, même si elles ne révèlent, à elles seules, aucune information sur la personne. Nous supposons qu'en biométrie, le motif d'opposition serait légitime dès lors que le dispositif choisi par l'employeur laisserait des traces ou associerait un grand nombre de données identifiantes. Ainsi, le motif légitime serait peut-être rejeté selon les dispositifs envisagés car en pratique, peu de données sont collectées, il s'agit généralement du nom, du prénom et du numéro d'identification de l'employé, voire l'historique de son passage dans les locaux de l'entreprise. Lors de la procédure d'autorisation préalable, la CNIL est particulièrement vigilante sur la nature des données collectées. Les données biométriques, bien qu'identifiantes, ne portent pas plus atteinte à la vie privée que des données bancaires, d'immatriculation ou de sécurité sociale. Elles ne justifieraient pas à elles seules une atteinte à la vie privée qui légitimerait l'exercice du droit d'opposition.

424. A la suite du rapport rendu par deux sénateurs sur la vie privée à l'heure des mémoires numériques[590], une proposition de loi a été déposée au Sénat le 6 novembre 2009. Cette dernière vise à modifier la loi Informatique et libertés afin d'apporter des garanties supplémentaires face aux nouveaux risques que sont les « mémoires numériques », notamment en privilégiant l'exercice du droit d'opposition. A ce titre, les sénateurs souhaitent un renouvellement du droit d'opposition, qui serait appelé droit de suppression. Toute personne soumise à une collecte indirecte de ses données personnelles serait invitée à exercer son droit de s'opposer, sans frais, à ce que ses données soient utilisées à des fins de prospection. Par ailleurs, dans l'hypothèse où les données ont fait l'objet d'un traitement, la

[590] Y. Detraigne et A.-M. Escoffier, Rapport d'Information au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif « au respect de la vie privée à l'heure des mémoires numériques », n° 441, 27 mai 2009, consultable au www.senat.fr

personne qui justifie son identité, a le droit de demander sans frais et pour des motifs légitimes, la suppression de ses données. Par conséquent, l'exercice de ce droit est toujours conditionné à l'existence d'un motif légitime.

425. Sur le principe, le salarié peut initialement consentir ou s'opposer au traitement de ses données biométriques, avec les réserves précédemment évoquées. Lorsqu'il consent au traitement, il a la faculté ultérieure de procéder à la modification des informations le concernant, et même à bénéficier de l'effacement de ses données, ce que nous regroupons dans le droit de regard du salarié sur le traitement de ses données biométriques (section 2).

Section 2. Le droit de regard du salarié sur le traitement de données biométriques

426. En matière de données personnelles, les droits d'accès et de rectification permettent à la personne concernée par le traitement, de se faire communiquer des informations et d'établir des rectifications à ces renseignements fournis par le passé ou collectés à son insu. Ces droits mettent le salarié en position d'acteur qui a un droit de regard sur ses données personnelles sur lesquelles il peut agir pour leur sauvegarde, malgré les informations fournies par le responsable de traitement et la consultation des organes représentatifs. Cette sauvegarde s'exerce tout d'abord par le droit de se faire communiquer les éléments le concernant et ensuite le droit d'accès à ses données afin de procéder à leur modification voire à leur effacement si celles-ci sont incomplètes ou erronées.

Les entreprises ont tendance à négliger la gestion des données personnelles car les salariés eux-mêmes n'usent pas de leurs droits sans doute par défaut de connaissance. Ce constat est issu d'un sondage réalisé par Legal Suite sur l'Internet en mai 2008, sur trois cents personnes (directeurs juridiques, informaticiens, avocats, directeurs des ressources humaines et directeurs des systèmes informatiques) [591]. Il ressort de cette étude, que près de cinquante-six pour cent des sondés « *ne maîtrisent pas ou mal la gestion des données personnelles* ». Les salariés de ces entreprises ne prennent pas toujours conscience de l'étendue des informations détenues et des droits qu'ils peuvent exercer pour limiter cette étendue ou en modifier le

[591] Etude consultable sur le site internet de Legal Suite : http://www.legal-suite.fr/fr/quoi-de-neuf/communiques-de-presse/communiques/enquete-donnees-personnelles.php

contenu. C'est en exerçant les droits qu'ils ont à leur disposition, qu'ils obligent les responsables de traitement à veiller au respect de la loi Informatique et libertés au sein de l'entreprise.

427. Le salarié a un droit d'accès à ses données personnelles biométriques (A) mais il dispose aussi de la faculté de rectifier voire de révoquer l'information qui est faite de ses données personnelles (B).

A. Le principe de libre accès aux données personnelles biométriques

428. L'idée selon laquelle les personnes peuvent exercer des droits sur leurs données personnelles est novatrice au sein de la loi Informatique et libertés n° 78-17 du 6 janvier 1978. D'ailleurs, le Parlement européen a adopté, quelques mois plus tard, une résolution « *sur la protection des droits de la personne face au développement des progrès techniques dans le domaine de l'informatique*[592] » en vertu de laquelle « *toute personne ayant sa résidence habituelle sur le territoire d'un Etat membre a le droit de faire effacer des données illicitement collectées* » et « *de faire procéder à la rectification des données concernant sa personne qui seraient imprécises ou inexactes ainsi qu'à l'information des tiers auxquels elles auraient été communiquées* »

Cette idée se retrouve aussi au sein de la Convention STE n° 108 du Conseil de l'Europe, dans l'article 8 intitulé « *Garanties complémentaires* » qui développe le droit d'accès aux données et de rectification sur ces dernières. Le droit d'accès a été reconnu plus tard dans le domaine de la santé dans la loi n° 94-548 du 1er juillet 1994[593].
Avec la réforme opérée par la loi n° 2004-801 du 6 août 2004, ce droit d'accès n'a pas été modifié dans son état d'esprit mais dans sa mise en œuvre. Ainsi, les salariés peuvent contrôler le contenu et l'exactitude de leurs données personnelles, dont les données biométriques font partie.

[592] JOCE 5 juin 1979 n° C 140, p. 34
[593] loi n° 94-548 du 1er juil. 1994 relative au traitement de données nominatives ayant pour fin la recherche dans le domaine de la santé et modifiant la loi n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés, JO du 2 juil. 1994, p. 9559.

429. Lorsque les données sont collectées en vue de la mise en œuvre d'un dispositif biométrique, le salarié est en droit d'exiger du responsable de traitement l'accès à ses données personnelles et la communication des informations le concernant (1°). Cependant, dans certaines conditions, ce droit peut être soumis à quelques exceptions (2°).

1°. L'accès et la communication aux données biométriques

430. Le droit d'accès est le droit en vertu duquel une personne peut demander et obtenir des informations sur ses données personnelles, contenues au sein d'un fichier. Son exercice se fait en principe librement et sans que le salarié puisse se voir opposer de refus (1-1) sauf exceptions pour certains types de fichiers pour lesquels ce droit est restreint (1-2).

1-1. L'exercice du droit d'accès et de communication

431. Toute personne a le droit d'accéder aux données personnelles qui la concernent (a) et que ces données lui soient transmises dans la mesure où elle satisfait aux conditions de forme (b).

a. Le contenu du droit d'accès et de communication

432. Avant, d'exercer son droit d'accès, le salarié a la faculté de mettre en œuvre son « *droit à la curiosité*[594] ». Baptisé ainsi par monsieur Jean Frayssinet, ce droit permet à toute personne physique d'interroger le responsable de traitement sur ses données personnelles. Ce droit, prévu à l'article 39 I 1° de la loi Informatique, fait partie du droit d'accès, mais diffère de ce dernier car il n'implique pas que le salarié prenne connaissance du contenu des informations nominatives le concernant.

433. Le salarié peut aussi prendre connaissance du contenu des données détenues par le responsable de traitement. L'article 39 I de la loi 78-17 du 6 janvier 1978 modifiée énonce

[594] J. Frayssinet, La protection des données personnelles, in Lucas A., Dezève J. et Freyssinet J., Droit de l'informatique et de l'internet, PUF, 2001, n° 149 et s.

que « ***I.*** *- Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :*

1° *La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;*

2° *Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;*

3° *Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne ;*

4° *La communication, sous une forme accessible, des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;*

5° *Les informations permettant de connaître et de contester la logique qui sous-tend le traitement automatisé en cas de décision prise sur le fondement de celui-ci et produisant des effets juridiques à l'égard de l'intéressé. Toutefois, les informations communiquées à la personne concernée ne doivent pas porter atteinte au droit d'auteur au sens des dispositions du livre Ier et du titre IV du livre III du code de la propriété intellectuelle.*

Une copie des données à caractère personnel est délivrée à l'intéressé à sa demande. Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction.

En cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition. »

Ce droit permet de garantir la protection des libertés individuelles, notamment lorsque des données biométriques ou des données de santé, réputées sensibles, sont collectées.

434. En ce qui concerne les données de santé, cette notion n'a fait l'objet d'aucune définition légale. Le Groupe « Article 29 » précise que ce sont « *toutes les données contenues dans les documents médicaux et les systèmes de dossiers médicaux électroniques (DME)*[595] ». Elles ont un lien clair et étroit avec la description de l'état de santé passé et présent d'une personne. Elles sont particulièrement sensibles, au même titre que les données biométriques et

[595] Groupe de travail « Article 29 », Document de travail 00323/07/FR WP 131 sur le traitement des données à caractère personnel relatives à la santé, contenues dans les dossiers médicaux électroniques (DME), adopté le 15 fév. 2007, consultable sur le site internet du groupe au http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_fr.htm

doivent donc être recueillies avec prudence afin d'éviter tout détournement d'usage. En effet, ces données pourraient intéresser des organismes tiers tels que les compagnies d'assurance ou les autorités répressives et être détournées de la finalité initiale pour laquelle elles ont été collectées. Il ne faut pas que ces données de santé puissent se retrouver associées aux données biométriques au sein d'un seul et même fichier.

L'article 43 de la loi Informatique et libertés modifiée reconnaît au requérant la possibilité d'exercer son droit d'accès sur ses données de santé à caractère personnel. Il doit s'exercer dans les dispositions de l'article L. 1111-7 du Code de la santé publique. Le demandeur a la faculté de se faire communiquer l'ensemble des informations concernant sa santé, de façon directe ou par l'intermédiaire d'un médecin qu'il désigne à cet effet. De nombreux projets dans le domaine de la santé tendent à regrouper les données de santé au sein de dossiers du type dossier médical électronique, dossier médical personnel ou dossier pharmaceutique. Tous ces projets ont pour mêmes finalités d'accroître la qualité des traitements grâce à une meilleure information des patients et de réduire les coûts en matière de santé.

435. En ce qui concerne la biométrie, le salarié peut accéder à ses données ainsi qu'aux données associées comme les données d'identité ou le numéro d'identification fourni par l'employeur. Le salarié a donc tout intérêt à contrôler la validité de son gabarit biométrique et vérifier que ses données n'ont pas été altérées par son vieillissement, une maladie ou un accident qui aurait pu les modifier durablement. Cette vérification est importante car des données erronées ou falsifiées pourraient entraîner des faux rejets et évincer la personne du système.

Pour ce qui a trait aux modalités de consultation, la loi impose au responsable de traitement que la personne concernée puisse consulter ses données sous une « forme accessible ». Les données biométriques ne peuvent pas être consultées comme les données traditionnelles. Lors de la procédure d'enrôlement, le responsable de traitement ne conserve pas l'image initiale de la donnée mais sa conversion en gabarit informatique. Pour que ce gabarit soit consulté, le responsable de traitement doit mettre à la disposition du salarié une machine qui puisse lire les données biométriques. Par ailleurs, au regard de la complexité de ces données, la vérification de leur validité et leur interprétation peut requérir l'intervention d'un expert.

436. Depuis peu, un dispositif biométrique a été implanté dans un établissement de santé. Le Centre régional de lutte contre le cancer Oscar Lambret de Lille a fait une demande auprès de la CNIL, à titre expérimental, d'un traitement de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et le recours à une base centralisée, dans le but de renforcer la sécurité des personnes prises en charge en radiothérapie, prévenant ainsi les erreurs d'identification de ces personnes[596]. L'identité du patient sera contrôlée avant chaque radiothérapie afin de s'assurer que le traitement de radiation administré est bien le bon. Les données de santé ne sont pas associées aux données biométriques, il n'y a pas a priori d'interconnexion entre les fichiers ce qui réduit le risque de voir ces deux catégories de données sensibles s'associer.

437. Le bénéfice du droit d'accès est soumis au respect de plusieurs conditions (b)

b. Les conditions d'exercice du droit d'accès

438. Ce droit d'accès est un droit personnel qui ne peut être exercé que par son titulaire ou son représentant légal, si un mineur ou un majeur incapable est concerné. Seules, en principe, les personnes physiques qui peuvent justifier leur identité, bénéficient de ce droit. En revanche, une seule partie des personnes morales, en l'occurrence les groupements et partis politiques sont autorisés à l'exercer.

En effet, avant 1984, les entreprises n'étaient pas visées par la loi Informatique et libertés. L'avis favorable rendu par la CNIL le 3 juillet 1984[597] en ce qui concerne les mairies d'Arcueil, Gentilly, Ivry-sur-Seine, Villejuif et Vitry-sur-Seine, énonce que « *Si le droit d'accès établi par l'article 34 de la loi du 6 janvier 1978 a un caractère strictement individuel, il convient d'en reconnaître l'exercice aux personnes physiques, représentants légaux des entreprises, dès lors que le nom de ces personnes figure dans le fichier, en tant que dirigeant, actionnaire ou associé* ». Cette solution a pour conséquence, avec les limites posées

[596] CNIL, Délibération n° 2010-033 du 11 février 2010 autorisant la mise en œuvre par le Centre Oscar Lambret de Lille d'un traitement de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale avec base centralisée et ayant pour finalité le contrôle de l'identité des patients pris en charge en radiothérapie, demande d'autorisation n° 1340737, disponible sur le site de Légifrance au www.legifrance.gouv.fr
[597] CNIL, avis 3 juil. 1984, D. 1984, jur., p. 587, note J. Frayssinet

par la décision, de faire tomber dans le champ d'application de la loi, les fichiers d'entreprise et par extension, ceux des associations[598].

439. En ce qui concerne les salariés des entreprises, le droit d'accès s'effectue sur l'ensemble de leurs données personnelles y compris les données d'évaluation professionnelle, comme leur classement annuel « ranking » et leur potentiel de carrière dès lors que ces données peuvent être prises en compte pour statuer sur la carrière de la personne concernée[599].

Pour sa part, la Cour de cassation a précisé sur ce sujet que « *le refus de l'employeur de donner connaissance à la salariée de son appréciation exprimait sa volonté de l'évincer définitivement de tout avancement et que ces faits caractérisaient un comportement discriminatoire à son égard* [600]». Cette décision postule en faveur d'une plus grande transparence des employeurs en ce qui concerne les données issues des méthodes et techniques d'évaluation professionnelle.

La demande de droit d'accès peut être effectuée indifféremment sur place ou par écrit selon la personne mentionnée sur le traitement auprès de laquelle le droit d'accès s'exerce[601]. Le responsable de traitement de l'entreprise a dû valablement informer le salarié dès la création du traitement sur les modalités d'exercice de ce droit.

Par « prolongement[602] » du droit d'accès, le salarié peut se faire communiquer une copie de ses données personnelles. En vertu de l'article 39 I 4° de la loi du 6 janvier 1978, il s'agit, que la personne puisse bénéficier de la « *communication, sous forme accessible, des données à caractère personnel qui concernent ainsi que de toute information disponible quant à l'origine de celle-ci* ». L'intéressé reçoit une copie des données qui apparaissent sur le traitement. Le support doit être accessible, ce qui implique de permettre effectivement au demandeur d'avoir accès au contenu. Il serait impensable d'envoyer une copie électronique sécurisée des données personnelles si la personne ne dispose pas d'un ordinateur.

---

[598] Note précitée
[599] CNIL Rubrique « Actualités », Les salariés peuvent consulter leurs données d'évaluation professionnelle, 13 avr. 2007, disponible au www.cnil.fr
[600] Cass. soc., 23 oct. 2001, n° 99-44.215, disponible au www.legifrance.gouv.fr
[601] Art 39 I de la loi Informatique modifiée
[602] Expression reprise au sein de la revue Lamy de l'Informatique et des réseaux 2009, édition en ligne lamyline reflex, n° 632.

Par ailleurs, le montant acquitté par le demandeur, doit correspondre à celui de la reproduction. Dans un souci d'égalité, il n'est plus question que ce droit donne lieu à redevance, ce qui était le cas sous l'empire de la loi 78-17 du 6 janvier 1978 dans sa rédaction initiale. L'information doit être complète et détaillée ce qui signifie qu'aucune information ne doit être ni évincée ni dissimulée. Sans quoi, un juge des référés pourra être directement saisi. Cela fait partie des changements opérés par la loi 2004-801 du 6 août 2004.
Les données biométriques doivent donc pouvoir être communiquées à la personne titulaire de ces données, de façon intelligible.

440. S'il existe un risque de disparition ou de dissimulation des données personnelles, « *le juge compétent* [603]» peut ordonner toutes les mesures nécessaires qui permettent la sauvegarde de ces données. Cela comprend l'usage d'une procédure en référé.
Sur la compétence matérielle du juge, aucune indication supplémentaire n'apparaît dans la loi, ou dans le décret d'application. Il faut se référer au rapport rendu par Alex Türk au Sénat sur la loi de 2004 qui précise que « *Le juge compétent peut être soit le juge administratif, si le responsable du traitement est l'Etat, une personne morale de droit public ou une personne morale de droit privé gérant un service public, soit le juge judiciaire dans les autres cas*[604] ».
Certains auteurs ont avancé qu'en matière judiciaire, lorsqu'il est question de fichiers du secteur privé, la compétence pour traiter les litiges va au président du tribunal de grande instance[605], mais c'est le président du tribunal de commerce qui est le plus qualifié, s'il s'agit de commerçants[606].

441. Le droit d'accès contenu au sein de la loi Informatique et libertés a inspiré d'autres législations étrangères. Au Québec, par exemple, ce droit a été intégré au sein du Code civil du Québec à l'article 38 qui dispose que « *Sous réserve des autres dispositions de la loi, toute personne peut, gratuitement, consulter et faire rectifier un dossier qu'une autre personne détient sur elle soit pour prendre une décision à son égard, soit pour informer un tiers; elle peut aussi le faire reproduire, moyennant des frais raisonnables. Les renseignements contenus dans le dossier doivent être accessibles dans une transcription intelligible.* »

---

[603] Expression reprise de l'article 39 1° in fine de la loi n° 78-17 du 6 janv. 1978 modifiée.
[604] Sénat, Rapport n° 125 rendu par le rapporteur Alex Türk, session ordinaire 2002-2003, p. 125 http://www.senat.fr/rap/l02-218/l02-2181.pdf
[605] Voir J. Frayssinet et P. Kayser , La loi du 6 janvier 1978, RD pub. 1979, p. 629, n° 88
[606] X. Linant de Bellefonds et Hollande A., Pratique du droit de l'informatique, Delmas, 1998.

Les lois spécifiques sur l'accès aux documents et la protection des données personnelles précisent pour les traitements publics[607] ou privés[608], le droit, pour les personnes concernées, de se faire communiquer des informations sur leurs données personnelles et d'en modifier le contenu.

442. Les salariés sont généralement informés du droit d'accès et de communication au sein de leur contrat de travail mais nous émettons quelques réserves quant à son exercice effectif. En effet, même si l'employeur est débiteur de ce droit et le salarié en est le créancier, le second reste subordonné au pouvoir règlementaire du premier. Cette position hiérarchique peut amener les salariés à craindre que cette demande porte atteinte à la pérennité de leur emploi. Par ailleurs, il est souvent matériellement difficile d'exercer ce droit puisque dans les moyennes et grandes entreprises qui disposent de plusieurs succursales, le responsable de traitement est décentralisé au siège de l'entreprise.

443. Lorsque certains fichiers dépendent de la sûreté de l'Etat ou la défense, l'accès aux données personnelles ne peut s'effectuer directement. La personne concernée conserve toutefois la possibilité de faire valoir son droit d'accès indirect aux données la concernant (1-2).

1-2. Le droit d'accès indirect

444. Le droit d'accès indirect s'exerce sur les traitements qui concernent la sûreté de l'Etat (par exemple les fichiers de la Direction centrale du renseignement extérieur), la défense et la sécurité publique tels que les fichiers de police ou de gendarmerie (Système de traitement des infractions constatées) et les fichiers de police aux frontières comme le Système national d'information Schengen. Certains de ces fichiers sont consultés lors de recrutements ou d'habilitation à diverses professions (gardiennage, emploi dans des zones aéroportuaires etc.). Les informations contenues dans le fichier des comptes bancaires (FICOBA), tenu par la direction générale des Finances publiques, relèvent aussi de cette procédure. En revanche, le Fichier national automatisé des empreintes digitales, ne relève pas du droit d'accès indirect. Les personnes fichées peuvent directement obtenir communication et rectification de leurs données en s'adressant directement au ministère de l'Intérieur.

[607] La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, articles 9 et suivants (L.R.Q., c.A-2.1)
[608] La Loi sur la protection des renseignements personnels dans le secteur privé, art. 27 et s. (L.R.Q., c.P-39.1)

445. Pour des raisons de sécurité nationale (sûreté de l'Etat, de la défense ou de la sécurité publique), certains fichiers ne sont accessibles que par l'intermédiaire d'une personne habilitée à les consulter[609]. Dans ce cas de figure, le droit d'accès est indirect. L'article 41 de la loi du 6 janvier 1978 modifiée dispose que « *par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient ».*

La procédure suit un cheminement spécifique. Le requérant adresse une demande à la Commission afin qu'elle désigne l'un de ses membres compétents pour mener les investigations utiles et faire procéder aux modifications[610]. Ce dernier a la faculté de se faire assister d'un agent. Après avoir effectué les vérifications, une notification est envoyée au requérant. Si les données de ce dernier ne mettent pas en cause les finalités du fichier, elles lui sont communiquées. A propos du projet de décret portant création du fichier d'Exploitation documentaire et valorisation de l'information générale (EDVIGE), la CNIL avait admis que s'exerce un droit d'accès indirect sur les données traitées[611].

Les salariés des entreprises privées concernées par des zones classées « secret défense » ne nous semblent pas concernés par cette procédure[612], tout au moins dans le cadre de leur activité professionnelle. Dans ces cas de figure, les données biométriques et les données associées au traitement ayant fait l'objet d'une autorisation peuvent alors être consultées directement auprès du responsable de traitement.

---

[609] Ces fichiers sont notamment pour les fichiers du renseignement, ceux de la Direction centrale du renseignement extérieur, de la Direction du renseignement militaire, de la Direction générale de la sécurité extérieure. Pour les fichiers de police administrative ou judiciaire il y a le Système de traitement des informations constatées (STIC), le système judiciaire de documentation et d'exploitation (JUDEX) de la Direction générale de la gendarmerie nationale ou le Fichier national des interdits de stade (FNIS).

[610] Ce même art. 41 précise que le membre compétent doit appartenir ou avoir appartenu au Conseil d'Etat, à la Cour de cassation ou à la Cour des comptes.

[611] CNIL, Délibération n° 2008-174 du 16 juin 2008 portant avis sur un projet de décret en Conseil d'Etat portant création au profit de la Direction centrale de la sécurité publique d'un traitement automatisé de données à caractère personnel dénommé « EDVIGE », disponible sur le site internet www.legifrance.gouv.fr

[612] Supra n° 238 et s.

En ce qui concerne les salariés du secteur public comme par exemple ceux du ministère de la Défense ou de l'Intérieur, nous ne sommes pas en mesure de savoir s'ils sont rattachés à ces fichiers de part leur fonction au sein de ces administrations[613].

En 2009, la CNIL a comptabilisé pas moins de neuf cent cinquante (950) demandes de droit d'accès indirect. Ce chiffre est en constante augmentation[614].

446. La demande tendant à accéder aux données peut être acceptée ou rejetée par le responsable de traitement, qui a toute latitude pour répondre à la réclamation du salarié. Cette liberté lui a été concédée avec plus d'aisance depuis la loi n° 2004-801 du 6 août 2004. (2°)

2°. Les exceptions à l'exercice du droit d'accès

447. Le droit d'accès permet au requérant visé par le traitement d'interroger le responsable de traitement sur les données qu'il détient sur son compte. Si les demandes sont manifestement abusives notamment par leur caractère anormalement répété, le responsable de traitement peut lui opposer un refus exprès[615].

Antérieurement à la loi 2004-801 du 6 août 2004, le responsable de traitement ne pouvait refuser de répondre au requérant qu'après avoir préalablement saisi la CNIL. Cette dernière devait lui donner une autorisation de s'opposer à la demande[616]. Par ailleurs, l'opposition à l'exercice du droit d'accès d'une personne à ses données personnelles était passible de poursuites pénales. Désormais le responsable de traitement peut prendre l'initiative du refus. Simplement, il doit prendre garde, car l'autorisation de la CNIL était une sorte de « caution » qu'il n'a plus, puisqu'en cas de litige, il a la charge de la preuve du caractère manifestement abusif de la demande.

---

[613] Nous avons contacté la CNIL afin d'obtenir la confirmation de cette information mais elle n'a pas été en mesure de répondre.

[614] CNIL, 29ième rapport d'activités 2008, Conférence de presse, 13 mai 2009, p. 5, disponible sur le site www.cnil.fr

[615] Art. 39 II de la loi n° 78-17 du 6 janvier 1978 modifiée.

[616] Ancien art. 35 al. 3 de la loi n° 78-17 du 6 janvier 1978, le responsable de traitement pouvait obtenir « *l'autorisation de ne pas tenir compte de certaines demandes manifestement abusives par leur nombre, leur caractère répétitif ou systématique* ».

448. A l'égard du caractère abusif de la demande, quelques indices sont donnés dans la lettre du texte. Ce sont des demandes répétées ou systématiques. Néanmoins, la loi n'apporte aucune précision, chaque situation doit être évaluée personnellement pour juger du caractère abusif. Dans un rapport remis au Sénat, Alex Türk, président actuel de la CNIL précisait qu'une demande pouvait s'avérer abusive « *par son étendue, parce qu'elle porterait, par exemple, sur une période de quinze ans*[617] ».

A défaut de réponse, le responsable de traitement s'expose à des sanctions notamment pécuniaires. Ainsi, la CNIL a sanctionné la société NEUF-CI à une amende de sept mille euros pour avoir répondu partiellement à des demandes répétées d'une abonnée qui n'avaient pas un caractère abusif[618]. Le responsable de traitement avait ignoré les multiples réclamations de l'abonnée et avait fini par répondre de manière insuffisante ou incomplète à sa requête.

Dans le rapport de la Convention 108[619], le Comité a examiné la possibilité d'un recours abusif au droit d'accès pour les données biométriques et admet que les demandes « *excessivement fréquentes* » soient rejetées car « *seules les demandes effectuées à intervalle raisonnable doivent être accordées* [620]». Cette dernière proposition fait appel au bon sens surtout qu'en matière de biométrie l'exercice du droit d'accès requiert la mobilisation de plus de moyens matériels et humains que pour une demande visant d'autres types de données. Nous pensons qu'il est justifié de rejeter les demandes excessivement fréquentes. A contrario, le responsable de traitement doit faire preuve de bonne foi et ne pas éviter les courriers parce que la demande d'accès aux données biométriques est plus coûteuse même si l'on peut regretter que ce droit ne soit pas plus utilisé par les salariés.

---

[617] A.Türk, Rapport du Sénat fait au nom de la Commission des lois, Projet de loi relatif à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, examen des articles, n°218, déposé le 19 mars 2003, disponible sur le site internet du Sénat www.senat.fr

[618] CNIL, Délibération n° 2008-163 du 12 juin 2008 prononçant une sanction pécuniaire à l'encontre de la société Neuf Cegetel, disponible sur le site www.legifrance.gouv.fr

[619] Conseil de l'Europe, Convention STE n°108, Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques, 2005, disponible sur le site www.coe.int/

[620] Ibid.

449. En effet, le salarié est généralement informé de ce droit dans son contrat de travail et dispose d'une créance d'accès à ses données, alors que l'employeur en est le débiteur. Cette position, peut dissuader certains salariés d'exercer ce droit par crainte de représailles. Par ailleurs, comme nous l'avons soulevé précédemment[621], le salarié est souvent géographiquement éloigné du responsable de traitement et ne prend pas l'initiative de le contacter par écrit ou au siège de l'entreprise.

450. Les données biométriques sont des données identifiantes impliquant le corps humain. Alors se pose la problématique de l'application réelle des droits de rectification et d'opposition sur les données biométriques, comme on le ferait avec des données plus « traditionnelles » (B)

[621] Supra n° 365.

B. Le droit à rectification du salarié sur ses données biométriques

451. Le droit de rectification est considéré comme « l'aboutissement[622] » des droits d'accès et de communication aux données personnelles[623]. C'est parce que les données ont été préalablement communiquées et que l'intéressé a pu y accéder, qu'il est en mesure d'agir afin d'en rectifier le contenu. Les données biométriques peuvent être rectifiées quand l'intéressé a constaté, en accédant à ses données, qu'elles étaient entachées d'irrégularités.

Les données biométriques peuvent être inexactes, soit parce qu'elles ont été mal enrôlées, soit par l'altération du temps, de la maladie ou de la vieillesse du salarié. Les conséquences ne sont pas minimes puisque la machine peut afficher de nombreux taux d'erreurs. L'exactitude des données peut être compromise et doit être appréciée au regard de la finalité du dispositif. Ainsi, pour un dispositif de reconnaissance qui a pour finalité le contrôle d'accès sans stockage ultérieur des données, le responsable de traitement peut régler le seuil de sensibilité de la machine et accepter un degré de probabilité de fausses acceptations ou de faux rejets[624] plus élevé pour conserver un dispositif moins coûteux.

En revanche, dès lors que la finalité de contrôle d'accès requiert le stockage des données biométriques au sein d'une base de données centralisée, parce qu'il y a un « fort impératif de sécurité », le responsable de traitement devra effectuer des réglages plus précis par l'extension

---

[622] N. Mallet-Poujol, Lamy Droit de l'Informatique et des Réseaux, Ouvrage collectif sous la direction de M. Vivant, 2009, Partie 1 – Division 2 – Le droit d'accès de la personne concernée, n°633 et suivants, www.lamylinereflex.fr

[623] « *Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.*
Lorsque l'intéressé en fait la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent.
En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord.
Lorsqu'il obtient une modification de l'enregistrement, l'intéressé est en droit d'obtenir le remboursement des frais correspondant au coût de la copie mentionnée au I de l'article 39.
Si une donnée a été transmise à un tiers, le responsable du traitement doit accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa.
Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.
Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent. Art. 40 de la loi 78-17 du 6 janvier 1978 modifiée ».

[624] Supra n° 135.

de l'algorithme de traitement, afin que les taux d'erreurs soient faibles. Il importe de rappeler que les dispositifs biométriques, bien que fiables, reconnaissent les individus par probabilités. La correspondance entre le gabarit enrôlé et la donnée biométrique présentée n'est jamais garantie à un taux de cent pour cent. Par conséquent, l'exactitude des données ne peut jamais être tenue pour acquise et en cas d'inexactitude, cela ne signifie pas forcément que le responsable de traitement a agi illégalement. Le salarié ne peut se retourner contre le responsable de traitement pour ces raisons.

452. Un conflit sur le seuil de probabilité peut intervenir entre le responsable de traitement et le salarié. Ce dernier serait en droit de lui demander de procéder à un second enrôlement, qui en vertu du droit à rectification, ne pourrait lui être refusé. En cas de contestation, le responsable de traitement a la charge de la preuve, sauf s'il est établi que les données contestées ont été communiquées par le salarié ou avec son accord[625].

Cependant, les données biométriques sont enrôlées par le biais du dispositif dont le responsable de traitement a la charge. Par conséquent, les données contestées ne peuvent être communiquées par le salarié. Nous pensons que dans le traitement des données biométriques, la charge de la preuve incombe toujours au responsable de traitement. Si, à l'issue du second enrôlement, les taux d'erreurs sont toujours élevés, le responsable de traitement devra alors proposer au salarié, en vertu du principe de non-discrimination, un moyen alternatif de reconnaissance. Le salarié doit être informé de son « incompatibilité » avec le dispositif, afin qu'il opte pour une autre solution de sécurité proposée par le responsable de traitement et qu'il procède à l'effacement des données biométriques inopérantes.

453. La procédure de rectification ainsi que celle du droit d'accès sont plus complexes à mettre en œuvre quand il s'agit de données biométriques pour les raisons invoquées. Le responsable de traitement doit recourir à des moyens matériels et humains plus importants, ce qui engendre inévitablement un coût plus élevé que pour des données « traditionnelles ».

[625] Art. 40 al. 3 de la loi de 1978 modifiée.

Néanmoins, ce dernier ne peut soulever cette raison pour limiter les droits des salariés à leurs données personnelles. L'entreprise qui fait le choix de recourir à des dispositifs biométriques doit prendre conscience de l'ensemble des changements (matériels, financiers, humains) que cela engendre sur ce type de traitement.

CONCLUSION GENERALE

« L'humanité serait depuis longtemps heureuse
si les hommes mettaient tout leur génie
non à réparer leurs bêtises,
mais à ne pas les commettre[626] ».

« Il est hélas devenu évident
aujourd'hui que notre technologie
a dépassé notre humanité[627] ».

454. Biométrie. Le mot est évocateur. Peu nombreuses sont les personnes sans opinion à son sujet, qu'il s'agisse de progrès scientifique, de passeport, d'enquête policière ou de fiction. Une vision manichéenne du sujet fait débat entre ses partisans et ses opposants. Si nous reprenions cette vision, nous serions amenés à conclure sur cette technologie et son devenir, d'une manière hâtive, simpliste et peu rationnelle. D'une part, dans un optimisme béat, nous serions tentés de ne voir aucune objection à ce que l'identification biométrique d'un individu se généralise progressivement à toutes les tâches de la vie courante. D'autre part, avec une extrême méfiance, nous pourrions céder aux discours alarmistes des détracteurs de la biométrie, lesquels annoncent le chaos et la surveillance totalitaire qui naîtraient de l'imprudence des hommes pour avoir voulu mettre l'individu au cœur de son expérience. La crainte de voir l'homme s'emparer totalement de l'homme se serait réalisée[628].

La construction de l'Europe et la « pax americana » ont abouti à une période globalement prospère, où nos sociétés occidentales sont relativement pacifiées. Pourtant, si l'on compare ce début du XXIe siècle à d'autres pans de l'Histoire de France, nous abordons une époque pleine de contradictions. Alors que nous vivons la période de paix la plus longue de notre Histoire, paradoxalement, les individus ne se sont jamais autant sentis en danger, ou, plus

[626] G. B. Shaw (1856-1950), *Maximes pour révolutionnaire*, éd. Cahiers Libres, 1927
[627] A. Einstein (1879-1955), *Comment je vois le monde*, éd. Flammarion, 1989
[628] Supra n° 1.

justement ont besoin de recourir à des outils de sécurisation dans plusieurs sphères de leur quotidien, en se dotant de « gadgets » biométriques pour protéger leurs biens ou les êtres chers, alors qu'ils manifestent la plus grande méfiance, à accepter sur leur lieu de travail, une technologie analogue. Ce sentiment d'insécurité vient en partie de la médiatisation à outrance des faits divers qui se déroulent dans les zones urbaines et qui attisent la crainte des citoyens pour leur famille, leur personne et leurs biens. Les menaces terroristes n'y sont pas non plus étrangères et conduisent à une identification poussée des individus.

Néanmoins, l'usage de la biométrie ne s'est pas uniquement développé pour des questions de sécurité. Les progrès constants, en matière de découverte de nouvelles technologies, ont eu pour effet un accroissement rapide dans la fabrication de systèmes biométriques, dont ont su se servir les entreprises, car ces nouvelles technologies ont contribué à offrir des outils permettant de pallier le déficit de confiance existant de plus en plus dans les relations de travail. L'accroissement des usurpations d'identité dans les entreprises, mais aussi le désir d'un meilleur rendement et d'une plus grande rigueur dans le travail sont autant de raisons qui amènent les chefs d'entreprise à être de plus en plus méfiants à l'égard de leurs salariés, aboutissant ainsi à leur surveillance.

Ce déficit de confiance peut être élargi aux autres domaines dans lesquels la biométrie intervient comme la biométrie « de confort » où certains appareils du quotidien (serrures, ordinateurs, sac à main etc.) ne fonctionnent plus sans authentification fiable. La biométrie est une technologie qui tend à se développer. Il serait faux de croire qu'en limitant localement les autorisations ou en interdisant un dispositif biométrique, on en freine son expansion. Les règles juridiques présentées tout au long de ces développements ont vocation à encadrer cette technique - et non à l'éradiquer -, afin qu'elle se développe de façon raisonnée, comme un outil de protection améliorant la vie privée[629] et encadrant la vie professionnelle.

455. Du point de vue purement technique, il reste à perfectionner les domaines de la normalisation et de la cryptologie, dont les améliorations contribueront au progrès dans la sécurisation des données biométriques, une fois qu'elles seront collectées et traitées. Grâce à des systèmes de cryptographie pointus et fiables, les dispositifs biométriques se développeront de plus en plus, et avec eux, de manière proportionnelle, la confiance des partenaires

[629] Nommée par les anglo-saxons Privacy Enhancing Technologies (PET)

économiques. Il suffit, pour s'en convaincre, de faire un parallèle avec la signature électronique et les systèmes de cryptographie, utilisés au sein de l'administration française qui ont permis de développer de nombreux services tels que le paiement de la TVA et des impôts en ligne ou même l'engagement de procédures dématérialisées comme la procédure d'injonction de payer par voie électronique.

La loi pour la confiance en l'économie numérique[630] (LCEN) qui règlemente la cryptologie en France, devra peut-être subir des modifications de rigueur afin de s'adapter aux exigences techniques de la biométrie. Au Canada, en Ontario, le Commissaire à la protection des données personnelles reconnaît qu'il est nécessaire d'améliorer les outils cryptographiques afin de pérenniser le développement de la biométrie[631].

Une multitude de dispositifs biométriques voit le jour, dont certains ont un usage industriel comme la reconnaissance de la rétine, la technologie du réseau veineux des doigts de la main et sont employés pour des finalités de contrôle d'accès ou de gestion de l'entreprise. D'autres, plus surprenants, comme la géométrie de l'oreille, la denture, le dessin des lèvres, voire l'odeur, ne dépasseront sans doute pas le stade expérimental, par leur manque de fiabilité ou de facilité d'utilisation pour les individus. Les industriels ne cessent de rechercher de nouvelles techniques car les prévisions montrent un accroissement des ventes de dispositifs biométriques dans tous les secteurs sur les marchés européens, américains et japonais d'ici 2014[632].

456. Du point de vue juridique, pour la biométrie, les principes directeurs de la protection des données personnelles doivent être améliorés et spécifiés. L'intégration de la biométrie soulève de grandes interrogations en matière de droits de l'Homme. Dès lors qu'une technologie touche au corps humain, il importe d'être particulièrement vigilants, car toute décision précitée peut avoir des conséquences irréversibles sur les personnes. Ainsi, dans les entreprises, les responsables de traitement ont l'obligation de veiller au respect de la dignité humaine des salariés lors du processus de collecte et d'utilisation des données personnelles.

---

[630] Loi précitée
[631] A. Cavoukian, M. Snijder, "The relevance of untraceable biometrics and biometric encryption: a discussion of biometrics for authentication purposes", Information of Privacy Commissioner Ontario, European Biometrics Group, August 2009, p. 2.
[632] Supra n° 23.

En ce qui concerne la maîtrise collective dans l'encadrement de la biométrie en entreprise, nous proposerions d'être plus exigeants vis-à-vis du principe de spécification de la finalité et de s'assurer que cette spécification soit effective, c'est-à-dire qu'elle soit plus détaillée par les responsables de traitement lors des demandes d'autorisation. Cela ne doit pas non plus conduire à réduire l'emploi de la biométrie à la sécurisation les lieux. Par ailleurs, la finalité doit être en adéquation avec les besoins de l'entreprise, selon son activité. Le responsable de traitement doit recourir à des solutions alternatives, s'il s'avère que la biométrie n'est vraiment pas requise, notamment pour des raisons environnementales.

Le responsable de traitement, tout comme la CNIL, devront systématiquement choisir entre une technologie basée sur l'authentification ou l'identification[633].
Cette dichotomie authentification / identification permet, en premier lieu, d'établir plus justement la finalité du traitement puisqu'il sera inutile de constituer une base de données biométriques pour contrôler l'accès au restaurant de l'entreprise, par exemple.
En second lieu, ce découpage détermine le seuil de traçabilité de la technologie lorsque les données sont stockées. Si la conservation se fait en identification, au sein d'une base de données, le risque de détournement est présent, même en l'absence de technologie dite « à traces » telle que le contour de la main. C'est d'ailleurs ce qu'a rappelé la CNIL dans l'affaire du GMAC[634]. Elle ne cache pas sa préférence pour l'authentification biométrique qui minimise les risques de détournement et garantit à la personne l'anonymat en lui permettant de détenir ses données personnelles.

En ce qui concerne le principe de proportionnalité, il importe de maintenir le juste équilibre entre le développement des intérêts de l'entreprise et la protection des données personnelles des salariés. Ce principe reste fondamental, il doit être conservé car il permet de poser les bonnes questions en matière « informatique et libertés », lorsque l'attrait de l'installation d'une technique biométrique serait plus justifié par la facilité que par la nécessité.

A propos de la maîtrise individuelle, il reste à faire un important travail de communication et d'information, tant auprès des entreprises que des salariés. Pour ces derniers, la prise de conscience de l'importance de la protection de leurs données personnelles reste progressive et

[633] Supra n° 173.
[634] Supra n° 253.

pour l'instant peu satisfaisante. La consultation des organes représentatifs du personnel doit rester centrale, et le dialogue social intervenir sur ces questions dans le but de permettre un développement de ces applications dans le respect des personnes.

L'information du personnel préalable à l'installation de tout dispositif biométrique dans l'entreprise, doit être améliorée, pour devenir très complète, ce qui n'est pas toujours le cas, notamment sur l'interconnexion des fichiers ou la durée de stockage des données.

Le consentement biométrique, nécessite d'avoir une certaine connaissance technique. Le salarié doit comprendre les implications liées à la collecte d'une donnée biométrique associée à d'autres données d'identité. Cette difficulté se rencontre, par exemple, dans les contrats souscrits en ligne dans la mesure où « le clic » de la souris n'a pas encore le même impact psychologique que la signature papier. Les salariés doivent avoir conscience que le fait d'apposer son doigt sur un lecteur biométrique matérialise son consentement. Un écrit, dans des formes traditionnelles, transmis à la Commission lors de la demande d'autorisation faciliterait sans doute cette prise de conscience[635].

Les droits de regard dont bénéficie le salarié (droit d'accès, d'opposition et de rectification), sont, pour l'instant, cohérents avec l'usage des dispositifs biométriques. Ils garantissent aux salariés un contrôle sur les données biométriques comme c'est le cas pour les autres catégories de données personnelles mais nécessitent un support humain et matériel spécifique qui n'est pas nécessaire pour des données traditionnelles. Ces spécificités ne doivent pas constituer un frein à l'exercice de ces droits.
Les responsables de traitement doivent prévoir et mettre en œuvre des procédures de secours pour les situations d'urgence, particulièrement en cas de refus d'identification d'un salarié ou dans l'hypothèse d'un détournement de données personnelles.

457. Il n'existe pas encore de consensus international quant à l'usage de la biométrie, en dehors de la sphère gouvernementale mais nous espérons vivement que ces questions seront bientôt largement débattues. Déjà, à Madrid, en 2009, quatre-vingts représentants d'autorités de protection, se sont réunis pour adopter une résolution qui vise à instaurer des standards de protection des données personnelles et de la vie privée. La biométrie fera bientôt

[635] Supra n° 413.

partie, sans aucun doute, des technologies pour lesquelles il faudra, aussi obtenir des standards[636].

Sur le plan européen, le projet de réforme de la Directive européenne de 1995 vient d'être amorcé[637]. Il serait souhaitable qu'une discussion soit engagée sur la biométrie dans le secteur privée afin qu'il y ait un consensus sur ces questions. En revanche, il ne serait pas opportun en l'état actuel, d'établir un texte de loi sur la biométrie. C'est une technologie encore nouvelle et nous n'avons pas assez de recul pour mettre en place des règles qui soient à la fois générales pour s'adapter à la multitude de supports et précises pour permettre une protection adéquate des données personnelles des salariés.

Néanmoins, même si le droit du travail s'articule plutôt bien avec les dispositions « informatique et libertés », les règles en la matière pourraient être spécifiées, par exemple, au sein d'un chapitre supplémentaire dans la loi Informatique, comme c'est le cas pour les traitements des données de santé.

Le cas échéant, il serait judicieux de mettre en place une charte ou un code de déontologie, comme l'a fait l'Australie, qui établirait des grands principes entre les industriels, les entreprises privées, les prestataires de cryptographie, les syndicats majoritaires et les organismes de recherche comme le Groupe des Ecoles des Télécommunications. Dans certains pays, tels que le Canada ou l'Australie, des textes de lois ont été établis pour protéger toutes les catégories de données personnelles dans le secteur privé comprenant ainsi à la fois l'usage des nouvelles technologies et la protection des données personnelles des salariés.

458. Nous devons rester particulièrement vigilants à toutes ces questions, car la biométrie ne constitue pas le seul danger. Elle peut interagir dans un avenir proche avec d'autres applications de surveillance, telles que la géolocalisation ou la vidéosurveillance à l'insu des personnes. La propagation de toutes les données que ces appareils génèrent, constitue un risque important pour la protection de la vie privée des individus.

---

[636] CNIL, 30ième Rapport d'activités 2009, « La proposition aux pouvoirs publics », p. 91, disponible sur le site www.cnil.fr

[637] CNIL, La révision de la Directive européenne ne doit pas se faire dans la précipitation, Rubrique actu CNIL, 2 août 2010, article disponible sur le site www.cnil.fr

La Commission nationale de l'informatique et des libertés fait un travail remarquable de sensibilisation, de contrôle et de sanction, malgré la lourdeur de sa charge et la faiblesse de ses effectifs. Elle reste incontestablement, avec le juge judiciaire, le garde-fou en matière de protection des droits et libertés des salariés et plus largement des citoyens français.

Néanmoins, les défis se multiplient, dans le domaine de la protection des données personnelles, au fur et à mesure des découvertes technologiques et la Commission manque toujours plus de moyens matériels et humains pour mener à bien sa mission. En 2011, elle espère enfin que son projet de « label informatique et libertés » verra le jour. Il comprendra à la fois l'assurance de la qualité et la conformité d'un produit biométrique mais pas uniquement et des procédures touchant la protection des données. Prévu par la loi de 2004, ce « label » avait tardé à être mis en œuvre en l'absence de décret d'application.[638]
Enfin, de par la qualité des décisions rendues par la CNIL et son implication dans la protection des données personnelles à l'échelon européen, au sein du groupe « Article 29 », il est permis d'être confiant quant au développement raisonné de la biométrie.

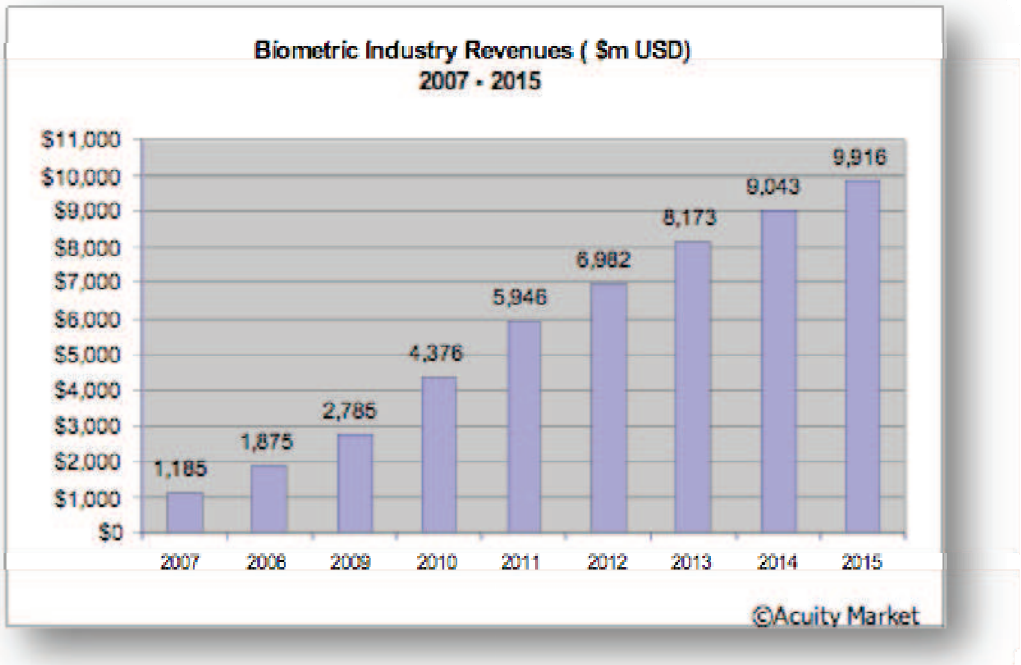
Les entreprises françaises comme Thalès Security Systems ou Sagem ont une reconnaissance internationale dans le domaine de la biométrie. D'autres, de taille plus petite, ne manquent pas de se distinguer, elles aussi, sur la scène internationale, comme la société ID3 Semiconductors qui, en 2009, a atteint les exigences du NIST américain[639] en matière de performances d'algorithmes de comparaison d'empreintes digitales sur des cartes à puce avec son programme nommé « *Fingerprint On-Card Comparison* ». Il serait donc souhaitable que la France profite des atouts de ses entreprises pour bâtir un cadre juridique de la biométrie dans le secteur privé.

[638] CNIL, 30ième Rapport d'activités 2009, « La labellisation », p. 79, disponible au www.cnil.fr, CNIL, « 2011 : objectif labellisation », rubrique article, 17 mai 2010, disponible au www.cnil.fr
[639] National Institute of Standards and Technology

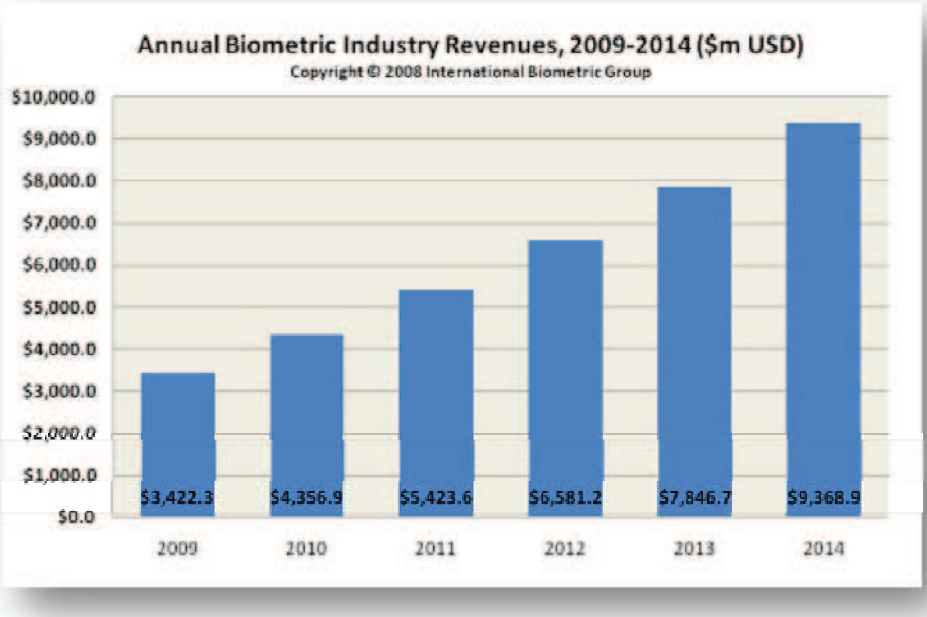
ANNEXES

ANNEXE 1 – REVENUS TOTAL DE LA BIOMETRIE

ET PREVISIONS



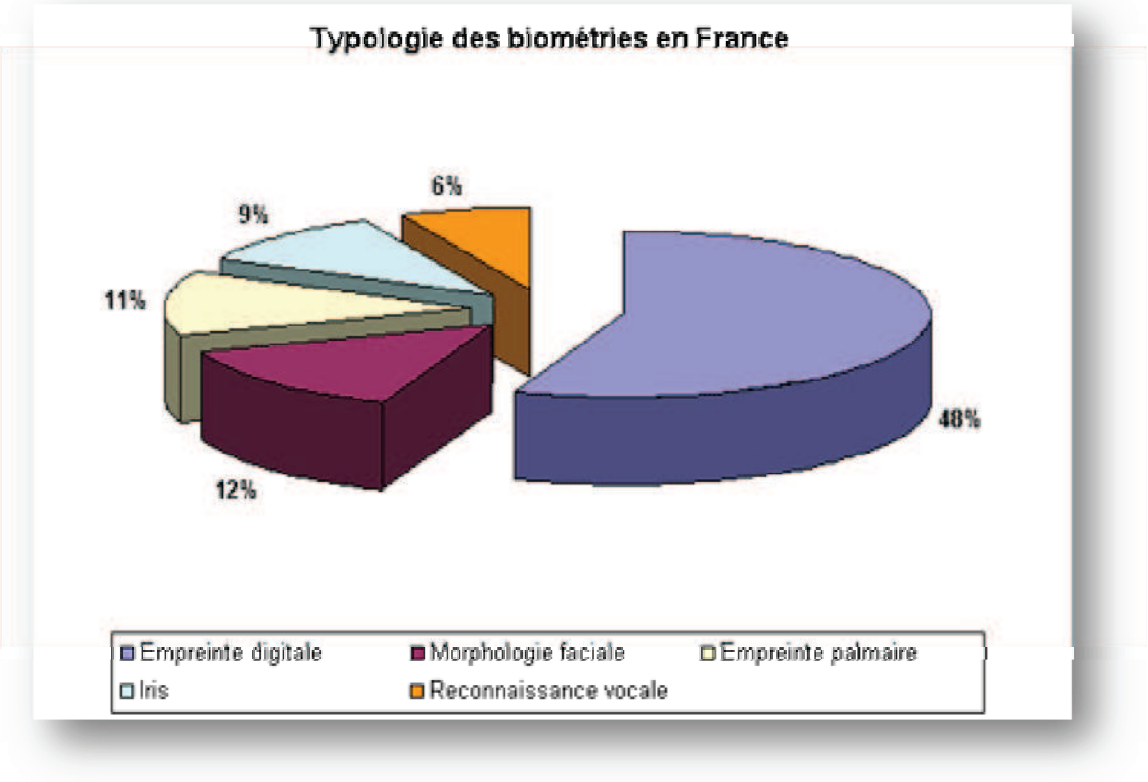
[640]



[641]

[640] International Biometric Group
[641] International Biometric Group

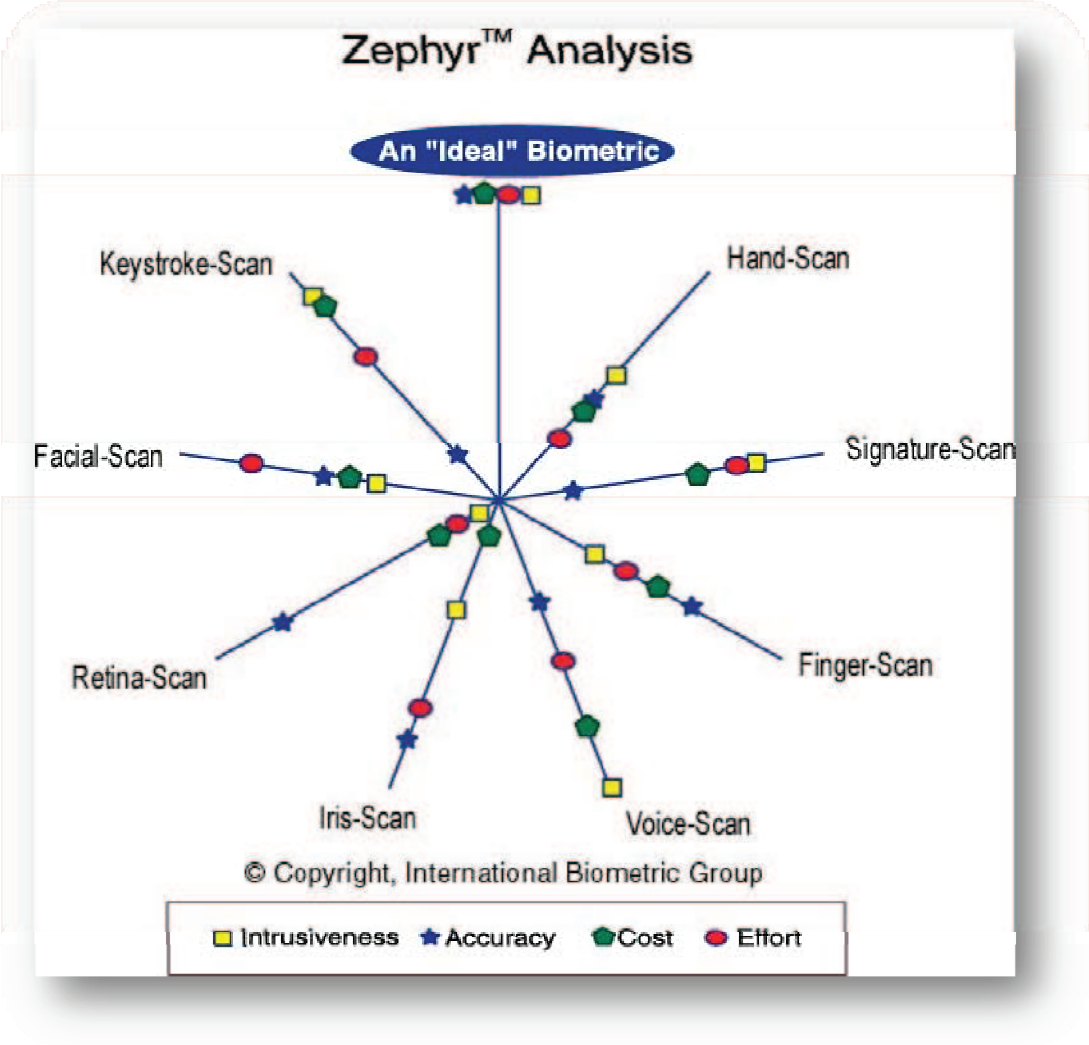
ANNEXE 2- ETUDE COMPARATIVE DU MARCHE FRANCAIS DES SYSTEMES BIOMETRIQUES



642

642 Typologie des biométries en France. Site Internet opticsvalley : http://www.opticsvalley.org/data/lumiere/n31nov06/dossier_biometrie.htm

ANNEXE 3- ETUDE COMPARATIVE DES SYSTEMES BIOMETRIQUES LES PLUS PERFORMANTS



643

Légende :

Intrusiveness : Mesure le caractère intrusif de la technique sur l'utilisateur

Accuracy : Mesure l'efficacité du procédé à identifier une personne

Cost : Mesure le coût de la technique

Effort : Mesure les efforts requis par l'utilisateur

643 Etude de performance des systèmes biométriques réalisée par la société de conseil et d'intégration International Biometric Group. Site Internet Biométrie online.

ANNEXE 4 - EXEMPLE DE FORMULAIRE QUEBECOIS DE CONSENTEMENT A LA CUEILLETTE, L'USAGE ET LA CONSERVATION DE CARACTERISTIQUES OU DE MESURES BIOMETRIQUES

1. Introduction

[Nom de l'organisme public ou de l'entreprise] entend implanter d'ici [indiquer jour, mois et année] un nouveau système de [indiquer le type de système, par exemple paie, contrôle des accès, etc.]. À cet égard, nous désirons obtenir votre consentement afin de prendre des lectures biométriques de [empreintes digitales, empreinte de l'iris, forme de votre main, modulation de votre voix, etc.].

2. [Indiquer le type de caractéristiques physiologiques ou comportementales recueillies] (on y réfère par le terme « Caractéristiques ou mesures biométriques » dans le reste de ce document)

Sur réception de votre consentement, [nom de l'organisme public ou de l'entreprise] procédera à la cueillette de vos données biométriques selon la procédure qui suit. [Indiquer la procédure complète et détaillée. **Voici un exemple dans le cas d'une lecture d'empreintes digitales** : Le lecteur biométrique photographie le doigt, y compris l'empreinte digitale. L'image créée par cette photographie n'est pas conservée. À partir de la photographie, le logiciel place des points à une multitude d'endroits afin que l'ensemble des points puisse constituer l'identification de votre doigt uniquement. Cette étape est effectuée deux fois pour chacun des doigts. La position de chaque point est numérisée et un algorithme transforme ces chiffres en code. Votre identité est ainsi reliée à votre doigt. La procédure est répétée sur trois de vos doigts d'une main seulement (en cas de blessures aux doigts); l'ensemble de ces données biométriques constituent vos caractéristiques ou mesures biométriques]. Vos caractéristiques ou mesures biométriques sont un renseignement personnel aux termes de la loi. [Nom de l'organisme public ou de l'entreprise] s'engage donc à ce que les mécanismes de sécurité en assurent la confidentialité.

Nom de l'organisme public ou de l'entreprise

Nom de l'employé(e)

3. Finalités visées par l'utilisation de la biométrie

Les caractéristiques ou mesures biométriques sont recueillies afin de permettre [indiquer quelles sont les raisons de l'utilisation d'un système biométrique]. Elles font partie de votre dossier d'employé(e) et ne serviront à aucune autre fin.

4. Mesures de sécurité

Vos renseignements personnels sont importants pour [nom de l'organisme public ou de l'entreprise]. C'est pour cette raison que [nom de l'organisme public ou de l'entreprise] s'assure que vos caractéristiques ou mesures biométriques sont adéquatement protégées afin d'assurer leur confidentialité. Vos caractéristiques ou mesures biométriques feront l'objet d'une [indiquer les dispositifs de sécurité, par exemple double cryptage] mis en place pour assurer la confidentialité de vos caractéristiques ou mesures biométriques. Seulement un nombre limité d'employé(e)s de [nom de l'organisme public ou de l'entreprise] auront accès à vos caractéristiques ou mesures biométriques. L'accès aux employé(e)s ne sera permis que s'il est nécessaire pour atteindre les finalités mentionnées au point 3 ci-dessus.

5. Conservation

Vos caractéristiques ou mesures biométriques seront conservées jusqu'à ce que le premier des deux événements suivants survienne : (i) la fin de votre emploi auprès de [nom de l'organisme public ou de l'entreprise]; ou (ii) le moment à compter duquel [nom de l'organisme public ou de l'entreprise] utilise une nouvelle méthode [type de méthode] qui ne correspond pas à la méthode mentionnée au point 1 ci-dessus. Lorsque le premier de ces événements se produira, [nom de l'organisme public ou de l'entreprise] procédera à la destruction sécuritaire de vos caractéristiques ou mesures biométriques dans les plus brefs délais sous réserve d'une demande d'accès ou de rectification en cours faite conformément au point 6 ci-dessous.

6. Droit d'accès et de rectification

Comme pour tous vos renseignements personnels, vous pourrez faire une demande d'accès aux renseignements reliées à vos caractéristiques ou mesures biométriques, une demande de rectification ou toute autre demande d'information en adressant cette dernière par écrit à [nom de l'organisme public ou de l'entreprise], [adresse] à l'attention de [direction responsable, s'il y a]. [Nom de l'organisme public ou de l'entreprise] répondra à votre demande d'accès, de rectification ou d'information dans les 30 jours suivant sa réception.

7. Communication de renseignements personnels

[Nom de l'organisme public ou de l'entreprise] ne communiquera pas vos renseignements personnels, y compris les caractéristiques ou mesures biométriques, à qui que ce soit, à moins que ces renseignements soient nécessaires pour qu'une tierce partie puisse rendre les services requis par [nom de l'organisme public ou de l'entreprise]. Afin d'assurer que vos caractéristiques ou mesures biométriques soient recueillies, utilisées et conservées conformément aux standards de sécurité mentionnés au point 4 ci-dessus, [nom de l'organisme public ou de l'entreprise] a imposé contractuellement à son fournisseur de services biométriques la mise en place et le maintien de mesures de sécurité appropriées. Comme pour tout autre renseignement personnel, [nom de l'organisme public ou de l'entreprise] pourrait avoir l'obligation de divulguer certains renseignements personnels lorsque la loi le requiert ou le permet.

8. Lieu d'entreposage des caractéristiques ou mesures biométriques

Les caractéristiques ou mesures biométriques, comme tous les autres renseignements personnels, sont conservées [type de support et quel endroit].

9. Consentement

Je confirme avoir pris connaissance et avoir compris l'information contenue dans ce formulaire relativement à la cueillette, l'usage et la conservation de mes caractéristiques ou mesures biométriques par [nom de l'organisme public ou de l'entreprise]. Je comprends également que mes caractéristiques ou mesures biométriques ne serviront qu'à [raisons] au, à [nom de l'organisme public ou de l'entreprise].

Je consens à la collecte, à l'utilisation et à la conservation de mes caractéristiques ou mesures biométriques sous réserve des dispositions des présentes.

SIGNÉ à [ville], Québec, le [date]

Signature de l'employé(e) :

ANNEXE 5 – TABLEAU DE LA CNIL REPRESENTANT LES PROCEDURES A SUIVRE SUIVANT LES TECHNIQUES BIOMETRIQUES

Les traitements utilisant un système biométrique : la procédure devant la CNIL

	Finalité du traitement			
Biométrie utilisée	Contrôle d'accès Salariés/visiteurs	Contrôle d'accès clients	Contrôle d'accès à la cantine scolaire	Autre finalité
Contour de la main	Déclaration de conformité (si traitement conforme à l'**AU-007**)	Demande d'autorisation	Déclaration de conformité (si traitement conforme à l'**AU-009**)	Demande d'autorisation
Réseau veineux de la main	Déclaration de conformité (si traitement conforme à l'**AU-019**)	Demande d'autorisation	Demande d'autorisation	Demande d'autorisation
Empreinte digitale	Déclaration de conformité (si traitement conforme à l'**AU-008**) stockage de l'empreinte uniquement sur support individuel	Demande d'autorisation	Demande d'autorisation	Demande d'autorisation
Autre type de biométrie (reconnaissance faciale, de l'iris de l'œil, de la voix, etc.)	Demande d'autorisation	Demande d'autorisation	Demande d'autorisation	Demande d'autorisation

ANNEXE 6 – DELIBERATION DE LA COMMISSION NATIONALE INFORMATIQUE ET LIBERTES (AU- 007) JO N°138 DU 16 JUIN 2006

Délibération n°2006-101 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail.

La Commission nationale de l'informatique et des libertés,

Vu la convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment son article 25-8° ;

Vu le Code du travail et notamment ses articles L 120-2, L 121-8, L 143-14, L 212-1 et suivants, L 236-3; L 412-17, L 424-3, L. 432-2, L 432-2-1, L 434-1, L 611-9, L 620-2;

Vu la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;

Vu la loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat;

Vu la loi n° 84-53 du 16 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale ;

Vu la loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière ;

Vu la loi n° 98-461 du 13 juin 1998 d'orientation et d'incitation relative à la réduction du temps de travail ;

Vu le décret 82-452 du 28 mai 1982 relatif aux comités techniques paritaires ;

Vu le décret 2000-815 du 25 août 2000 relatif à l'aménagement et à la réduction du temps de travail dans la fonction publique de l'Etat ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Après avoir entendu M. Hubert Bouchet, commissaire en son rapport et Mme Pascale Compagnie, commissaire du gouvernement en ses observations.

Formule les observations suivantes :

La gestion des horaires et des contrôles d'accès aux locaux ainsi qu'au restaurant d'entreprise ou administratif et aux prestations associées peut s'effectuer grâce à la mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main. Dès lors, de tels dispositifs relèvent de l'article 25-8° de la loi du 6 janvier 1978 modifiée qui soumet à autorisation les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes.

Il y a lieu, en l'état des connaissances sur la technologie utilisée, de faire application des dispositions de l'article 25-II aux termes duquel les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la Commission.

Le responsable de traitement mettant en œuvre un dispositif reposant sur la reconnaissance du contour de la main dans le respect des dispositions de cette décision unique adresse à la Commission un engagement de conformité de celui-ci aux caractéristiques de la présente autorisation.

Décide que les responsables de traitement qui adressent à la Commission une déclaration comportant un engagement de conformité pour leurs traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à mettre en œuvre ces traitements.

Article 1er : Finalités et caractéristiques techniques du traitement

Seuls peuvent faire l'objet d'un engagement de conformité en référence à la présente décision unique les traitements reposant sur un dispositif de reconnaissance du contour de la main, mis en œuvre par les organismes privés ou publics, à l'exception des traitements mis en œuvre :

pour le compte de l'Etat ;

par les établissements accueillant des mineurs, lorsque les personnes concernées sont des mineurs.

Ces traitements peuvent avoir pour finalités :

le contrôle des accès à l'entrée et dans les locaux limitativement identifiés de l'organisme faisant l'objet d'une restriction de circulation ;
la gestion des horaires et des temps de présence ;
le contrôle de l'accès au restaurant d'entreprise ou administratif et la gestion de la restauration ainsi que la mise en place d'un système de paiement associé ;
le contrôle d'accès des visiteurs.
Le dispositif biométrique de reconnaissance du contour de la main doit présenter les caractéristiques suivantes :
aucune photographie de la main des personnes concernées n'est conservée ;
les éléments pris en compte reposent exclusivement sur la géométrie de la main ;
seul le gabarit du contour de la main, résultat du traitement des mesures par un algorithme, est enregistré dans une base de données où il peut être associé à un numéro d'authentification de la personne ;
lorsque la finalité poursuivie est le contrôle des horaires des employés, le dispositif de reconnaissance du contour de la main peut être interconnecté avec une application de gestion des horaires et des temps de présence ;
lorsque la finalité poursuivie est le contrôle de l'accès au restaurant d'entreprise ou administratif, le dispositif de reconnaissance du contour de la main peut être interconnecté avec une application de gestion de la restauration ainsi qu'avec un système de paiement associé.

Article 2 : Données à caractère personnel traitées

Chacune des finalités précitées peut faire l'objet d'une application mise en œuvre de façon indépendante ou intégrée.
Seules les données à caractère personnel suivantes peuvent être traitées :
a) identité : nom, prénom, photographie, numéro d'authentification et gabarit du contour de la main ;
b) vie professionnelle : numéro de matricule interne, corps ou service d'appartenance, grade ;
c) temps de présence : plages horaires autorisées, cumul des horaires, congés, autorisations d'absences, heures supplémentaires, jours de réduction du temps de travail, décharge d'activité de service et autres absences (motifs, droits et décomptes) ;
d) déplacement des personnes : porte utilisée, zones d'accès autorisées, date et heure d'entrée et de sortie ;

d) en cas d'accès à un parking : numéro d'immatriculation du véhicule, numéro de place de stationnement ;
e) en cas de gestion de la restauration : prix des consommations et moyen de paiement, part patronale ou de l'administration, solde, date du repas et type de consommation (sous la forme exclusive : "hors d'œuvres", "plat", "dessert", "boisson").
S'agissant des visiteurs, outre les catégories de données relatives à l'identité et au déplacement des personnes, l'indication de la société d'appartenance et du nom de l'employé accueillant le visiteur peut être traitée.

Article 3 : Destinataires des informations

Dans la limite de leurs attributions respectives et pour l'exercice des finalités précitées, seuls peuvent être destinataires des données suivantes :

Destinataires	**Données**
personnes habilitées du service du personnel	identité, vie professionnelle, temps de présence, déplacement des personnes et informations en relation avec la gestion du parking
personnes habilitées du service gérant la paie ou les traitements	identité (à l'exception du gabarit du contour de la main et du code d'authentification), temps de présence et vie professionnelle
personnes habilitées du service gérant la sécurité des locaux	identité, plages horaires autorisées, déplacement des personnes, vie professionnelle et informations en relation avec la gestion du parking ou des locaux
personnes habilitées du service ou de l'organisme gérant le restaurant d'entreprise ou administratif	identité (à l'exception du gabarit du contour de la main et du code d'authentification), informations en relation avec la gestion de la restauration

Lorsqu'un accord sur le temps de travail le prévoit et dans la limite des dispositions légales et conventionnelles applicables, certains employés protégés peuvent être destinataires des informations relatives aux heures d'arrivée et de départ des personnes.

Les personnes habilitées du service du personnel ou du service gérant la sécurité ne peuvent avoir accès au gabarit du contour de la main que de façon temporaire et pour les stricts besoins de son inscription dans la base de données ou de sa suppression.

Article 4 : Durée de conservation

A l'exception du gabarit du contour de la main et du code d'authentification associé qui doivent être supprimés dès le départ de l'employé, les catégories de données relatives à l'identité, à la vie professionnelle et à la gestion du parking peuvent, au maximum, être conservés 5 ans après le départ de l'employé.

Lorsque le dispositif a exclusivement pour objet de contrôler l'accès à certaines zones des locaux, la durée de conservation du gabarit du contour de la main et du code d'authentification associé est égale au temps pendant lequel la personne concernée est habilitée à pénétrer dans lesdites zones.

Les éléments relatifs aux déplacements des personnes ne doivent pas être conservés plus de trois mois. Toutefois, les catégories de données relatives aux déplacements des personnes et aux temps de présence des employés peuvent être conservées pendant 5 ans lorsque le traitement a pour finalité le contrôle du temps de travail.

La conservation des données relatives aux motifs d'absence est limitée à une durée de cinq ans sauf dispositions législatives contraires.

En cas de paiement direct ou de pré-paiement des repas, les données monétiques ne peuvent être conservées plus de trois mois. En cas de paiement par retenue sur le salaire, la durée de conservation est de 5 ans.

S'agissant des visiteurs, les catégories de données relatives à l'identité, à la vie professionnelle et à la gestion du parking peuvent, au maximum, être conservés trois mois à compter de la date de la dernière visite.

Article 5 : Liberté de circulation des employés protégés

Les contrôles d'accès aux locaux du responsable de traitement et aux zones limitativement désignées, faisant l'objet d'une restriction de circulation justifiée par la sécurité des biens et des personnes qui y travaillent, ne doivent pas entraver la liberté d'aller et venir des employés protégés dans l'exercice de leurs missions.

Article 6 : Mesures de sécurité

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité et la confidentialité des données traitées et notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance.

Les accès individuels au traitement s'effectuent par un identifiant et un mot de passe individuel, régulièrement renouvelé ou par tout autre moyen d'authentification.

Article 7 : Information des personnes

Le responsable du traitement procède, conformément aux dispositions des articles L. 432-2 et L. 432-2-1 du code du travail et à la législation applicable aux trois fonctions publiques, à l'information et à la consultation des instances représentatives du personnel avant la mise en oeuvre des traitements visés à l'article premier.

L'information des employés est effectuée, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée en août 2004, par la diffusion à chaque personne concernée, préalablement à la mise en oeuvre du traitement, d'une note explicative.

Article 8 : Exercice des droits d'accès et de rectification

Le droit d'accès défini au chapitre V de la loi du 6 janvier 1978 modifiée s'exerce auprès du ou des services que le responsable de traitement aura désignés.

Article 9

Tout traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main qui n'est pas conforme aux dispositions qui précèdent doit faire l'objet d'une demande d'autorisation auprès de la Commission dans les formes prescrites par les articles 25-8° et 30 de la loi du 6 janvier 1978 modifiée.

Article 10

La présente délibération sera publiée au Journal officiel de la République française.

ANNEXE 7 – DELIBERATION DE LA COMMISSION NATIONALE INFORMATIQUE ET LIBERTES (AU- 008) JO N°138 DU 16 JUIN 2006

Délibération n°2006-102 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail.

La Commission nationale de l'informatique et des libertés,

Vu la convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment son article 25-8° ;

Vu le code du travail et notamment ses articles L 120-2, L 121-8, L 143-14, L 212-1 et suivants, L 236-3; L 412-17, L 424-3, L 432-2, L 432-2-1, L 434-1, L 611-9, L 620-2;

Vu la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;

Vu la loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat ;

Vu la loi n° 84-53 du 16 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale ;

Vu la loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière ;

Vu le décret 82-452 du 28 mai 1982 relatif aux comités techniques paritaires ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Après avoir entendu M. Hubert Bouchet, commissaire en son rapport, et Mme Pascale Compagnie, commissaire du gouvernement en ses observations.

Formule les observations suivantes :

La gestion des contrôles de l'accès physique à l'entrée des lieux de travail et dans les zones limitativement identifiées de l'organisme faisant l'objet d'une restriction de circulation peut s'effectuer grâce à la mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des l'empreintes digitales avec enregistrement de celles-ci sur un support individuel.

Dès lors, de tels dispositifs relèvent de l'article 25-8° de la loi du 6 janvier 1978 modifiée qui soumet à autorisation les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes. Il y a lieu, en l'état des connaissances sur la technologie utilisée, de faire application des dispositions de l'article 25-II aux termes duquel les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la Commission.

Le responsable de traitement mettant en œuvre un dispositif reposant sur la reconnaissance de l'empreinte digitale avec enregistrement sur un support individuel dans le respect des dispositions de cette décision unique adresse à la Commission un engagement de conformité de celui-ci aux caractéristiques de la présente autorisation.

Décide que les responsables de traitement qui adressent à la Commission une déclaration comportant un engagement de conformité pour leurs traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à mettre en œuvre ces traitements.

<u>Article 1er : Finalités et caractéristiques techniques du traitement</u>

Seuls peuvent faire l'objet d'un engagement de conformité en référence à la présente décision unique les traitements reposant sur un dispositif de reconnaissance des empreintes digitales avec enregistrement de celles-ci sur un support individuel, mis en œuvre par les organismes privés ou publics, à l'exception des traitements mis en œuvre :

pour le compte de l'Etat ; par les établissements accueillant des mineurs, lorsque les personnes concernées sont des mineurs.

Ces traitements peuvent uniquement avoir pour finalité le contrôle des accès à l'entrée et dans les locaux limitativement identifiés de l'organisme faisant l'objet d'une restriction de circulation, à l'exclusion de tout contrôle des horaires des employés.

Le dispositif de reconnaissance des empreintes digitales doit présenter les caractéristiques suivantes :

seul le gabarit de l'empreinte digitale, clé biométrique résultat du traitement des mesures par un algorithme, est enregistré sur le support individuel et non une image ou une photographie de l'empreinte digitale ;

on entend par support individuel tout support de stockage dont la personne concernée a un contrôle exclusif, tel qu'une carte à puce ou magnétique ;

le gabarit de l'empreinte digitale de la personne concernée est exclusivement enregistré sur un support individuel détenu par elle seule et dont le contenu ne peut être lu à son insu ;

lors de l'enrôlement, un enregistrement temporaire du gabarit de l'empreinte digitale peut être effectué sur le poste informatique servant à l'enrôlement pour les stricts besoins de son inscription dans la mémoire du support individuel et sous réserve qu'il soit effacé à l'issue de cette phase qui ne saurait excéder quelques secondes ;

le contrôle d'accès s'effectue par une comparaison entre le doigt apposé sur le lecteur et le gabarit de l'empreinte digitale enregistré sur le support individuel sans qu'aucune copie de ce gabarit, même temporaire, ne soit effectuée ;

à l'exclusion des gabarits des empreintes digitales, certaines données nécessaires à l'identification de la personne et à la réalisation des contrôles relatifs à la validité du badge peuvent être enregistrées dans un serveur dédié au contrôle des accès.

Article 2 : Données à caractère personnel traitées

Seules les données à caractère personnel suivantes peuvent être traitées :

a) identité : nom, prénom, photographie, numéro de carte et gabarit de l'empreinte digitale ;

b) vie professionnelle : numéro de matricule interne, corps ou service d'appartenance, grade ;

c) déplacement des personnes : porte utilisée, zones et plages horaires d'accès autorisées, date et heure d'entrée et de sortie ;

d) en cas d'accès à un parking : numéro d'immatriculation du véhicule, numéro de place de stationnement ;

S’agissant des visiteurs, outre les catégories de données relatives à l’identité et au déplacement des personnes, l’indication de la société d'appartenance et du nom de l’employé accueillant le visiteur, peuvent être traitées.

Article 3 : Destinataires des informations

Dans la limite de leurs attributions respectives et pour l’exercice des finalités précitées, seuls peuvent être destinataires des données :

les personnes habilitées du service du personnel : identité, vie professionnelle, déplacement des personnes et informations en relation avec la gestion du parking.

les personnes habilitées du service gérant la sécurité des locaux : identité, déplacement des personnes, vie professionnelle et informations en relation avec la gestion du parking.

Les personnes habilitées énumérées ci-dessus ne peuvent avoir accès au gabarit de l’empreinte digitale que de façon temporaire et pour les stricts besoins de son inscription sur le support individuel ou de sa suppression.

Article 4 : Durée de conservation

La durée de conservation du gabarit de l’empreinte digitale est égale au temps pendant lequel la personne concernée est habilitée à pénétrer dans les locaux ou les zones limitativement identifiées de l'organisme faisant l'objet d'une restriction de circulation.

Les catégories de données relatives à l’identité, à la vie professionnelle et à la gestion du parking peuvent, au maximum, être conservées 5 ans après le départ de l’employé.

Les éléments relatifs aux déplacements des personnes ne doivent pas être conservés plus de trois mois.

S’agissant des visiteurs, les catégories de données relatives à l’identité, à la vie professionnelle et à la gestion du parking peuvent, au maximum, être conservés trois mois à compter de la date de la dernière visite.

Article 5 : Liberté de circulation des employés protégés

Les contrôles d'accès aux locaux du responsable de traitement et aux zones limitativement désignées, faisant l'objet d'une restriction de circulation justifiée par la sécurité des biens et des personnes qui y travaillent, ne doivent pas entraver la liberté d'aller et venir des employés protégés dans l'exercice de leurs missions.

Article 6 : Mesures de sécurité

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité et la confidentialité des données traitées et, notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance.

Les accès individuels au traitement s'effectuent par un identifiant et un mot de passe individuel, régulièrement renouvelé, ou par tout autre moyen d'authentification.

Article 7 : Information des personnes

Le responsable du traitement procède également, conformément aux dispositions des articles L. 432-2 et L. 432-2-1 du code du travail et à la législation applicable aux trois fonctions publiques, à l'information et à la consultation des instances représentatives du personnel avant la mise en œuvre des traitements visés à l'article premier.

L'information des employés sera effectuée, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée en août 2004, par la diffusion à chaque personne concernée, préalablement à la mise en œuvre du traitement, d'une note explicative.

Article 8 : Exercice des droits d'accès et de rectification

Le droit d'accès défini au chapitre V de la loi du 6 janvier 1978 modifiée s'exerce auprès du ou des services que le responsable de traitement aura désignés.

Article 9

Tout traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance de l'empreinte digitale avec enregistrement sur un support individuel qui n'est pas conforme aux dispositions qui précèdent doit faire l'objet d'une demande d'autorisation auprès de la Commission dans les formes prescrites par les articles 25-8° et 30 de la loi du 6 janvier 1978 modifiée.

Article 10

La présente délibération sera publiée au Journal officiel de la République française.

ANNEXE 8 – DELIBERATION DE LA COMMISSION NATIONALE INFORMATIQUE ET LIBERTES (AU- 009) JO N°138 DU 16 JUIN 2006

Délibération n°2006-103 du 27 avril 2006 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire

La Commission nationale de l'informatique et des libertés,

Vu la convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, et notamment son article 25-8° et II ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Après avoir entendu M. Francis Delattre, commissaire en son rapport, et Mme Pascale Compagnie, commissaire du gouvernement en ses observations.

Formule les observations suivantes :

Le contrôle de l'accès au restaurant scolaire peut s'effectuer grâce à la mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main.

Dès lors, de tels dispositifs relèvent de l'article 25-8° de la loi du 6 janvier 1978 modifiée qui soumet à autorisation les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes. Il y a lieu de faire application des dispositions de l'article 25-II aux termes duquel les traitements qui répondent à une même finalité, portent sur des

catégories de données identiques et les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la Commission.
Le responsable de traitement mettant en œuvre un dispositif reposant sur la reconnaissance du contour de la main dans le respect des dispositions de cette décision unique adresse à la Commission un engagement de conformité de celui-ci aux caractéristiques de la présente autorisation.
Décide que les responsables de traitement qui adressent à la Commission une déclaration comportant un engagement de conformité pour leurs traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à mettre en œuvre ces traitements.

Article 1er : Finalité et caractéristiques techniques du traitement

Seuls peuvent faire l'objet d'un engagement de conformité en référence à la présente décision unique les traitements reposant sur un dispositif de reconnaissance du contour de la main mis en œuvre par les établissements publics locaux d'enseignement du second degré et les établissements privés d'enseignement du second degré.
Ces traitements ont pour finalité le contrôle de l'accès des élèves et des personnels au restaurant scolaire et sont interconnectés avec une application de gestion de la restauration ainsi qu'avec un système de paiement associé.
Le système envisagé repose d'une part, sur la mise en œuvre d'un fichier de gestion recensant les élèves fréquentant la cantine scolaire et d'autre part, sur un dispositif de contrôle d'accès.
Ce dernier est composé d'une borne d'accès, située à l'entrée du restaurant, reliée à un lecteur biométrique, lequel contient une base de données comportant les gabarits biométriques et les codes d'accès.
Le dispositif biométrique de reconnaissance du contour de la main doit présenter les caractéristiques suivantes :
aucune photographie de la main des personnes concernées n'est conservée ;
les éléments pris en compte reposent exclusivement sur la géométrie de la main ;
seul le gabarit du contour de la main, résultat du traitement des mesures par un algorithme, est enregistré dans la base de donnée où il peut être associé à un code ou numéro d'authentification de la personne.

Article 2 : Données à caractère personnel traitées

Seules les données à caractère personnel suivantes peuvent être traitées :

a) s'agissant des élèves,

les données de gestion utiles pour l'accès au restaurant : identité (nom, prénom), la classe, le numéro d'ordre dans l'établissement, les coordonnées du responsable légal, un code horaire et un code tarif ;

les gabarits biométriques de la main associés à un code d'accès personnel ;

b) s'agissant des personnels,

les données de gestion utiles pour l'accès au restaurant : identité (nom, prénom), les codes horaire et tarif.

les gabarits biométriques de la main associés à un code d'accès personnel.

Article 3 : Destinataires des informations

Peuvent être destinataires des données visées à l'article 2, dans la limite de leurs attributions respectives et pour l'exercice des finalités précitées, le responsable d'établissement ainsi que les seules personnes habilitées qui assurent la gestion du service de la restauration scolaire.

Les personnes habilitées énumérées ci-dessus ne peuvent avoir accès au gabarit de l'empreinte digitale que de façon temporaire et pour les stricts besoins de son inscription sur le support individuel ou de sa suppression.

Article 4 : Durée de conservation

Les données relatives à l'identité de l'élève sont conservées pendant la durée de sa scolarité dans l'établissement. Les données relatives à l'identité des personnels sont conservées pendant la durée de leur affectation au sein de l'établissement.

Les gabarits biométriques du contour de la main associés à un code d'accès personnel sont conservés pendant la durée de l'année scolaire. Si une personne quitte l'établissement ou est désinscrite du service de restauration scolaire en cours d'année, les données biométriques sont effacées dans la semaine suivant son départ ou sa désinscription.

Article 5 : Mesures de sécurité

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité et la confidentialité des données traitées et, notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance.

Les accès individuels au traitement s'effectuent par un identifiant et un mot de passe individuel, régulièrement renouvelé, ou par tout autre moyen d'authentification.

Article 6 : Information des personnes

L'information des élèves majeurs et des représentants légaux des élèves mineurs ainsi que des personnels sur l'identité du responsable du traitement, les finalités poursuivies, le caractère obligatoire ou facultatif des réponses à apporter, les conséquences éventuelles, à leur égard d'un défaut de réponse, les destinataires des données et l'existence d'un droit d'accès et de rectification aux données les concernant est assurée par la diffusion d'une note explicative, préalablement à la mise en œuvre du traitement.

Les élèves majeurs et les représentants légaux des élèves mineurs doivent être individuellement informés du droit de s'opposer, par un moyen simple, à l'informatisation des données biométriques les concernant ou concernant leurs enfants. En cas d'opposition à l'utilisation du dispositif biométrique, les élèves ont la possibilité de se voir délivrer un badge ou tout autre moyen d'accès à la cantine.

L'information des représentants des parents d'élèves, des élèves et des personnels doit également être assurée lors des réunions des instances délibératives de l'établissement.

Article 7 : Exercice des droits d'accès et de rectification

Le droit d'accès défini au chapitre V de la loi du 6 janvier modifiée s'exerce auprès du ou des services que le responsable de traitement aura désignés. Cette information figure sur le formulaire d'inscription au service de restauration scolaire.

Article 8

Tout traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main qui n'est pas conforme aux dispositions qui précèdent doit faire l'objet d'une demande d'autorisation auprès de la Commission dans les formes prescrites par les articles 25-8° et 30 de la loi modifiée du 6 janvier 1978.

Article 10

La présente délibération sera publiée au Journal officiel de la République française.

ANNEXE 9 – DELIBERATION DE LA COMMISSION NATIONALE INFORMATIQUE ET LIBERTES (AU- 019) JO N°142 DU 21 JUIN 2009

Délibération n°2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail

La Commission nationale de l'informatique et des libertés,

Vu la convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données ;

Vu la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel, notamment son article 25-8° ;

Vu le code du travail et notamment ses articles L 1222-4, L 2143-22, L 2315-5, L2323-13 et suivants, L 2323-32, L2325-11 et L8113-4 et suivants ;

Vu la loi n° 83-634 du 13 juillet 1983 portant droits et obligations des fonctionnaires ;

Vu la loi n° 84-16 du 11 janvier 1984 portant dispositions statutaires relatives à la fonction publique de l'Etat ;

Vu la loi n° 84-53 du 16 janvier 1984 portant dispositions statutaires relatives à la fonction publique territoriale ;

Vu la loi n° 86-33 du 9 janvier 1986 portant dispositions statutaires relatives à la fonction publique hospitalière ;

Vu le décret 82-452 du 28 mai 1982 relatif aux comités techniques paritaires ;

Vu le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ;

Sur le rapport de M. Didier Gasse et M. Hubert Bouchet, commissaires, et les observations de Mme Elisabeth Rolin, commissaire du Gouvernement ;

Formule les observations suivantes :

La gestion des contrôles de l'accès physique à l'entrée des lieux de travail et dans les zones limitativement identifiées de l'organisme faisant l'objet d'une restriction de circulation peut s'effectuer grâce à la mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du réseau veineux des doigts de la main. Dès lors, de tels dispositifs relèvent de l'article 25-I-8° de la loi du 6 janvier 1978 modifiée qui soumet à autorisation les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes. Il y a lieu, en l'état des connaissances sur la technologie utilisée, de faire application des dispositions de l'article 25-II aux termes duquel les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la Commission. Le responsable de traitement mettant en œuvre un dispositif reposant sur la reconnaissance du réseau veineux des doigts de la main dans le respect des dispositions de cette décision unique adresse à la Commission un engagement de conformité de celui-ci aux caractéristiques de la présente autorisation. Décide que les responsables de traitement qui adressent à la Commission une déclaration comportant un engagement de conformité pour leurs traitements de données à caractère personnel répondant aux conditions fixées par la présente décision unique sont autorisés à mettre en œuvre ces traitements.

Article 1er : Finalités et caractéristiques techniques du traitement

Seuls peuvent faire l'objet d'un engagement de conformité en référence à la présente décision unique les traitements reposant sur un dispositif de reconnaissance du réseau veineux des doigts de la main, mis en œuvre par les organismes privés ou publics, à l'exception des traitements mis en œuvre :

- pour le compte de l'Etat ;
- lorsque les personnes concernées sont des mineurs.

Ces traitements peuvent uniquement avoir pour finalité le contrôle des accès à l'entrée et dans les locaux limitativement identifiés de l'organisme faisant l'objet d'une restriction de circulation, à l'exclusion de tout contrôle des horaires des employés.
Le dispositif de reconnaissance du réseau veineux doit présenter les caractéristiques suivantes :

- seul le gabarit du réseau veineux du doigt, clé biométrique résultat du traitement des mesures par un algorithme, est enregistré et non une image ou une photographie du réseau veineux ;
- le gabarit du réseau veineux du doigt de la personne concernée est exclusivement enregistré sous une forme chiffrée soit dans la mémoire du terminal de lecture/comparaison qui ne dispose d'aucun port de communication permettant l'extraction de ce gabarit, soit sur un support individuel sécurisé qui reste en possession de la personne devant être authentifiée par le dispositif;
- l'enrôlement des caractéristiques biométriques des personnes s'effectue exclusivement à partir du terminal de lecture/comparaison ;
- le contrôle d'accès s'effectue par une comparaison entre le doigt apposé sur le lecteur et le gabarit du réseau veineux du même doigt enregistré dans la mémoire du terminal de lecture comparaison ;

d'autres données nécessaires à l'identification des personnes peuvent être enregistrées dans la mémoire du terminal de lecture comparaison et associées au gabarit du réseau veineux de leur doigt.

Article 2 : Données à caractère personnel traitées

Seules les données à caractère personnel suivantes peuvent être traitées :
a) identité : nom, prénom, photographie et gabarit du réseau veineux du doigt de la personne ;
b) vie professionnelle : numéro de matricule interne, corps ou service d'appartenance, grade ;
c) déplacement des personnes : porte utilisée, zones et plages horaires d'accès autorisées, date et heure d'entrée et de sortie ; d) en cas d'accès à un parking : numéro d'immatriculation du véhicule, numéro de place de stationnement ;
S'agissant des visiteurs, outre les catégories de données relatives à l'identité et au déplacement des personnes, l'indication de la société d'appartenance et du nom de l'employé accueillant le visiteur peuvent être traitées.

Article 3 : Destinataires des informations

Dans la limite de leurs attributions respectives et pour l'exercice des finalités précitées, seuls peuvent être destinataires des données limitativement les personnes dûment habilitées :

- du service du personnel et du service informatique : identité, vie professionnelle, déplacement des personnes et informations en relation avec la gestion du parking ;
- du service gérant la sécurité des locaux : identité, déplacement des personnes, vie professionnelle et informations en relation avec la gestion du parking.

Les personnes habilitées énumérées ci-dessus ne peuvent avoir accès au gabarit du réseau veineux du doigt de la personne que de façon temporaire et pour les stricts besoins de son inscription sur le support individuel ou de sa suppression, sans qu'il leur soit possible d'accéder directement, de modifier, ou de copier sur un autre support, les gabarits enregistrés.

Article 4 : Durée de conservation

La durée de conservation du gabarit du réseau veineux des doigts de la main est égale au temps pendant lequel la personne concernée est habilitée à pénétrer dans les locaux ou les zones limitativement identifiées de l'organisme faisant l'objet d'une restriction de circulation.

Les catégories de données relatives à l'identité, à la vie professionnelle et à la gestion du parking peuvent, au maximum, être conservées 5 ans après le départ de l'employé.

Les éléments relatifs aux déplacements des personnes ne doivent pas être conservés plus de trois mois.

S'agissant des visiteurs, les catégories de données relatives à l'identité, à l'indication de la société d'appartenance et à la gestion du parking peuvent, au maximum, être conservés trois mois à compter de la date de la dernière visite.

Article 5 : Liberté de circulation des employés protégés

Les contrôles d'accès aux locaux du responsable de traitement et aux zones limitativement désignées, faisant l'objet d'une restriction de circulation justifiée par la sécurité des biens et des personnes qui y travaillent, ne doivent pas entraver la liberté d'aller et venir des employés protégés dans l'exercice de leurs missions conformément aux dispositions du code du travail.

Article 6 : Mesures de sécurité

Le responsable du traitement prend toutes précautions utiles pour préserver la sécurité et la confidentialité des données traitées et, notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance.

Les accès individuels au traitement par l'administrateur du dispositif s'effectuent par un identifiant et un mot de passe individuel ou tout système offrant un niveau de sécurité au moins équivalent. En cas d'utilisation d'un mot de passe, celui-ci doit être régulièrement renouvelé, être d'une longueur d'au moins 8 caractères alphanumériques et comporter au moins un chiffre, une lettre et un caractère de ponctuation. Le dispositif doit permettre l'enrôlement de plusieurs doigts par utilisateur.

Afin d'en garantir la confidentialité, les gabarits enregistrés dans le dispositif doivent être chiffrés en utilisant des algorithmes cryptographiques réputés forts.

Le dispositif doit permettre de détecter toute ouverture ou arrachement du terminal de lecture/comparaison et de le signaler à l'administrateur du système.

Les gabarits traités ne doivent pas permettre de recalculer l'image correspondante du réseau veineux.

Au cas où le dispositif comporte un historique des passages, celui-ci ne doit pas conserver des données au-delà de quatre vingt dix jours.

Article 7 : Information des personnes

Le responsable du traitement procède également, conformément aux dispositions des articles L2323-13 et suivants, L 2323-32 du Code du travail et à la législation applicable aux trois fonctions publiques, à l'information et à la consultation des instances représentatives du personnel avant la mise en oeuvre des traitements visés à l'article premier.

L'information des employés est effectuée, conformément aux dispositions de l'article 32 de la loi du 6 janvier 1978 modifiée en août 2004, par la diffusion à chaque personne concernée, préalablement à la mise en oeuvre du traitement, d'une note explicative.

Article 8 : Exercice des droits d'accès et de rectification

Le droit d'accès défini au chapitre V de la loi du 6 janvier 1978 modifiée s'exerce auprès du ou des services que le responsable de traitement aura désignés.

Article 9

Tout traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du réseau veineux des doigts de la main qui n'est pas conforme aux dispositions qui précèdent doit faire l'objet d'une demande d'autorisation auprès de la Commission dans les formes prescrites par les articles 25-8° et 30 de la loi du 6 janvier 1978 modifiée.

Article 10

La présente délibération sera publiée au Journal officiel de la République française.

ANNEXE 10 – JUGEMENT DU TRIBUNAL DE GRANDE INSTANCE DE PARIS EN DATE DU 19 AVRIL 2005

Vu l'ordonnance du 6 janvier 2005 qui a dit n'y avoir lieu à référé sur les demandes du comité d'entreprise de la société Effia Services et de la Fédération des syndicats Sud Rail et a renvoyé l'affaire à l'audience du 15 mars 2005 pour qu'il soit statué au fond sur le litige opposant les parties ;
Vu les dernières écritures du 14 mars 2005 des demandeurs qui sur le fondement des articles L 120-2, L 121-8 du code du travail et la directive 95/46/CE du 24 octobre 1995 sollicitent de :

dire et juger que le pointage par empreintes digitales mis en place par la société Effia Services, système constitutif d'un traitement automatisé de données personnelles, porte atteinte aux droits et libertés individuels des salariés de l'entreprise et n'est ni adéquat, ni pertinent, ni justifié au regard de l'objectif d'établissement des bulPWW. ns de paye ;

faire interdiction à la société Effia Services de mettre en place le système de badgeage par empreintes digitales ;

condamner la société Effia Services à payer à la Fédération des syndicats Sud Rail la somme de 3000 euros à titre de dommages-intérêts en réparation de l'atteinte portée aux intérêts collectifs de la profession ;

la condamner à payer à chacun d'eux une indemnité de 2000 euros sur le fondement des dispositions de l'article 700 du ncpc ;

Vu les dernières conclusions d'Effia Services aux fins de débouter les demandeurs de l'ensemble de leurs prétentions, de prononcer l'exécution provisoire de la décision à intervenir et de condamner chacun des demandeurs à lui verser 1000 euros sur le fondement de l'article 700 du ncpc ;

DISCUSSION

La société Effia Services, filiale de la société Sncf Participations qui assure dans les gares Sncf, le portage de bagages, l'aide et l'assistance des usagers à mobilité réduite et l'accueil des passagers d'Eurostar a décidé de mettre en place au sein de l'entreprise un nouveau mode de gestion et de contrôle des temps de présence sur l'ensemble des sites de travail en réseau avec un lecteur biométrique utilisant la technologie des empreintes digitales.

Le fonctionnement de ce système comporte deux phases :
l'empreinte digitale du salarié est mémorisée sur une carte à puce, correspondant à un numéro de badge dont la lecture est assurée par une badgeuse à la prise et à la fin du service ;
ce premier contrôle est validé en même temps par l'application du doigt sur un lecteur.

Les demandeurs soutiennent que ce système porte atteinte aux droits et libertés individuelles des salariés résultant des articles L 120-2, L 121-8 et L 432-2-1 du code du travail.

La société Effia Services affirme que le système de pointage par badge est parfaitement justifié et proportionné au but recherché, dans l'exercice du pouvoir réglementaire dont dispose l'employeur dans l'entreprise.

Il n'est pas contesté qu'avant la mise en place du système, un document de présentation a été remis au comité d'entreprise qui, ainsi que cela résulte du point 4 du procès verbal du 21 avril 2004, a été informé et consulté, motif pris des nombreux problèmes liés aux décomptes des heures de présence, sujet notamment évoqué par l'inspection du travail en 2003 et qu'ainsi les dispositions de l'article 432-2-1 ont été respectées.

La déclaration de traitement automatisé d'informations nominatives qui a été transmise le 25 mai 2004 à la Commission de l'informatique et des libertés comporte la mention selon laquelle le traitement en cause a pour but "la gestion des horaires et des temps de présence et la ventilation analytique des activités dans les centres de coûts".

En outre l'article L 121-8 du code de travail, aucune information concernant personnellement un salarié ne peut être sollicitée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ;

le courrier individuel adressé aux salariés le 25 novembre 2004 qui présente le nouveau mode de gestion et contrôle des temps de présence par badgeage à fin de permettre d'éviter toutes les difficultés liées à la gestion du temps, à savoir principalement les bulletins de paye erronés pour cause de feuilles mal remplies, précise que "l'empreinte partielle est stockée uniquement dans la mémoire du lecteur".

Il apparaît ainsi que les conditions préalables de mise en œuvre du système en cause ont été respectées.

Cependant, il ne peut être sérieusement contesté qu'une empreinte digitale, même partielle, constitue une donnée biométrique morphologique qui permet d'identifier les traits physiques spécifiques qui sont uniques et permanents pour chaque individu.

Son utilisation qui met en cause le corps humain et porte ainsi atteinte aux libertés individuelles peut cependant se justifier lorsqu'elle a une finalité sécuritaire ou protectrice de l'activité exercée dans des locaux identifiés.

En effet, selon l'article L 120-2 du code du travail "Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché".

Par ailleurs la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995 considère "que les systèmes de traitement de données sont au service de l'homme ;
qu'ils doivent respecter les libertés et droits fondamentaux de ces personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien être des individus ;
et l'article 6 du chapitre II intitulé : conditions générales de licéité des traitements de données à caractère personnel, stipule que "les données à caractère personnel collectées pour des

finalités déterminées, explicites et légitimes doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées ultérieurement".

Pour justifier la mise en place du système en cause, la défenderesse produit la lettre du 3 février 2003 de l'inspection du travail des transports qui constate que dès 9h20 le matin, les feuilles d'émargement indiquaient déjà l'heure de départ du salarié, ce qui ne permet pas de contrôler la réalité du travail effectif réalisé par les salariés ni de vérifier les temps de coupure repas.

Cependant par lettre du 19 novembre 2004, cette administration a précisé qu'il n'a pas été à l'origine de la mise en place d'une pointeuse à empreintes digitales qui relève du seul choix de l'employeur.
Il convient donc de rechercher si le traitement automatisé des données mis en œuvre par l'employeur, se rapportant au début et à la fin de l'activité professionnelle des salariés tendant à améliorer l'établissement des bulletins de paye est justifié et proportionné au but poursuivi.

Or, il n'est pas prétendu par la société Effia Services que la seule mise en place d'un système de badge ne serait pas de nature à permettre de contrôler efficacement les horaires des salariés sans avoir recours à un procédé d'identification comportant des dangers d'atteinte aux libertés individuelles dont la nécessité n'est pas démontrée.

Il s'ensuit que l'objectif poursuivi n'est pas de nature à justifier la constitution d'une base de données d'empreintes digitales des personnels travaillant dans les espaces publics des gares de la Sncf, le traitement pris dans son ensemble n'apparaissant ni adapté ni proportionné au but recherché.

Il y a lieu de faire interdiction à la société Effia Services de mettre en place le système de "badgeage" par empreintes digitales.

S'il n'est pas contesté que la Fédération des syndicats Sud Rail a qualité à agir pour la défense des intérêts matériels et moraux du personnel et de l'intérêt collectif, elle ne caractérise pas l'atteinte portée à ceux-ci et sera déboutée de sa demande à ce titre.

La société Effia Services, sera condamnée aux dépens et verra sa demande au titre de l'article 700 du NCPC rejetée.

L'équité conduit en revanche à allouer à ce titre à chacun des demandeurs la somme de 1500 euros.

L'exécution provisoire de la décision compatible avec la nature du litige doit être ordonnée.

DECISION

Le tribunal, statuant en audience publique, par jugement contradictoire en premier ressort,

Fait interdiction à la société Effia Services de mettre en place le système de "badgeage" par empreintes digitales ;

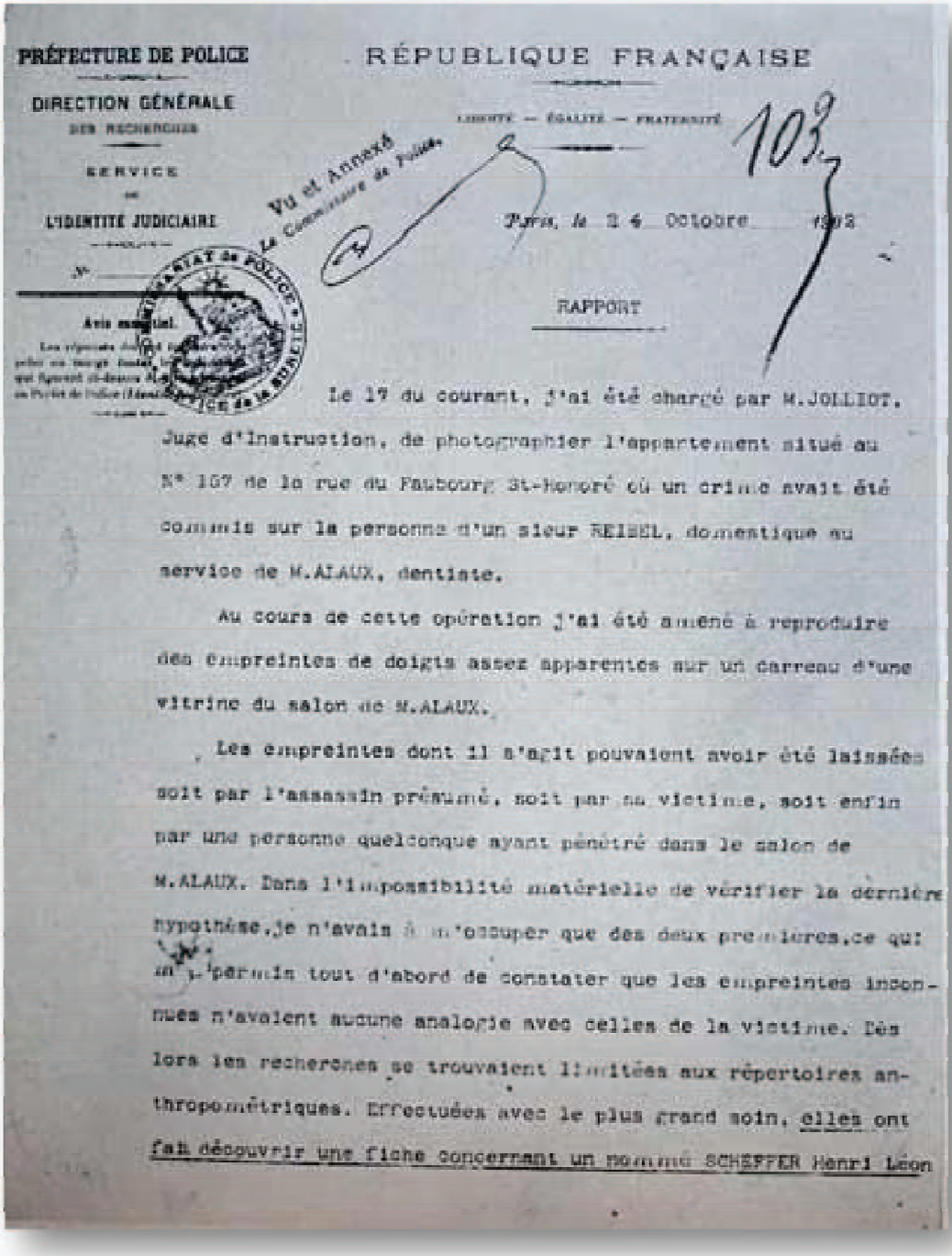
Déboute la Fédération des syndicats Sud Rail de sa demande de dommages-intérêts ;

Condamne la société Effia Services à payer au comité d'entreprise d'Effia Services et à la Fédération des syndicats Sud Rail la somme de 1500 euros à chacun d'eux sur le fondement des dispositions de l'article 700 du ncpc ;

Ordonne l'exécution provisoire de la décision ;

Condamne la société Effia Services aux dépens.

ANNEXE 11 – RAPPORT OFFICIEL DE L'AFFAIRE SCHEFFER REDIGE PAR ALPHONSE BERTILLON[644]



PRÉFECTURE DE POLICE

DIRECTION GÉNÉRALE
DES RECHERCHES

SERVICE
DE
L'IDENTITÉ JUDICIAIRE

N°

Avis mortuaire.

RÉPUBLIQUE FRANÇAISE

LIBERTÉ — ÉGALITÉ — FRATERNITÉ

Vu et Annexé
Le Commissaire de Police,

103

Paris, le 24 Octobre 1893

RAPPORT

Le 17 du courant, j'ai été chargé par M.JOLLIOT, Juge d'Instruction, de photographier l'appartement situé au N° 107 de la rue du Faubourg St-Honoré où un crime avait été commis sur la personne d'un sieur REISEL, domestique au service de M.ALAUX, dentiste.

Au cours de cette opération j'ai été amené à reproduire des empreintes de doigts assez apparentes sur un carreau d'une vitrine du salon de M.ALAUX.

Les empreintes dont il s'agit pouvaient avoir été laissées soit par l'assassin présumé, soit par sa victime, soit enfin par une personne quelconque ayant pénétré dans le salon de M.ALAUX. Dans l'impossibilité matérielle de vérifier la dernière hypothèse, je n'avais à m'occuper que des deux premières, ce qui m'a permis tout d'abord de constater que les empreintes inconnues n'avaient aucune analogie avec celles de la victime. Dès lors les recherches se trouvaient limitées aux répertoires anthropométriques. Exécutées avec le plus grand soin, elles ont fait découvrir une fiche concernant un nommé SCHEFFER Henri Léon

[644] Mémoire de Bertillon, commis auxiliaire au 1er bureau de la division du cabinet, adressé le 1er octobre 1879 au préfet de police Andrieux, site internet crimino corpus : http://www.criminocorpus.cnrs.fr/article133.html. Droits réservés à l'auteur.

âgé de 30 ans, mesuré le 9 Mars dernier comme inculpé de vol et abus de confiance, et dont les empreintes digitales concordent, d'une manière frappante, avec celles relevées sur le lieu du crime.

Afin d'en faciliter la comparaison, j'ai fait agrandir ces documents à une échelle supérieure de 4 fois à la grandeur naturelle et le rapprochement des épreuves apparaît alors avec la plus grande netteté.

Ci-joint une reproduction des pièces mentionnées au présent rapport.

L'examen des pièces sus-énoncées fait ressortir les constatations suivantes: (voir la Planche n° jointe du 31ème 60)

Similitude caractéristique du dessin central de chaque empreinte, soit:

1°: Pour le Pouce, lacets à direction oblique à droite comprenant 12 sillons entre le point central et le triangle d'intersection.

2°: Pour l'Index, lacets à direction oblique à droite comprenant 8 sillons entre le point central et le triangle d'intersection.

3°: Pour le Médium, sillons en forme d'arcs superposés avec, au centre de l'empreinte, un seul lacet oblique à droite renfermant un sillon central.

4°: Pour l'Annulaire, le centre du dessin est formé d'un point enfermé dans un cercle -à remarquer une légère solution de continuité dans la partie supérieure gauche du cercle-. Une spirale entoure ensuite le cercle en commençant par le côté inférieur gauche

et finissant,après une triple révolution,sur le côté supérieur gauche d'autres sillons ou fragments de sillon se greffent sur les côtés de la spirale et la forme générale de l'empreinte se continue en arcs superposés.

A côté de cette similitude de dessins,j'ai également relevé, sur chaque empreinte, un certain nombre de particularités repérées à l'aide de numéros figurant à la fois sur les empreintes relevées sur la vitrine du salon de M.ALAUX et sur celles qui existent sur la fiche du nommé SCHEFFER Henri Léon,retrouvée dans les répertoires anthropométriques.

En voici la nomenclature:

1°: POUCE.

N°1- Sillon bifurqué.
2- Arrêt du sillon central.
3- Echancrure formée par un fragment de sillon se greffant sur la partie supérieure gauche du 4°sillon.
4- Arrêt du 10°sillon.
5- Arrêt de sillon.
6- Sillon bifurqué.
7- Arrêt du 6°sillon.
8- Arrêt de sillon.
9- Arrêt de sillon
10- Bifurcation produite par la réunion des 7°et 8°sillons.
11- Arrêt de sillon.
12- Arrêt de sillon.

2°: INDEX.

N°1- Trace de cicatrice située sur le haut de l'empreinte.
2- Arrêt du sillon central formant boucle.
3- Crochet formé par la base et le côté gauche du triangle d'intersection.
4- Sillon bifurqué.

3°: Médius

3°: MEDIUS.

N°1: Trace très apparente de cicatrice située sur le côté gauche de l'empreinte.
2- Lacet central légèrement échancré dans sa partie supérieure gauche et fragment de sillon se greffant sur la partie supérieure droite.
3- Sillon bifurqué.
4- Arrêt de sillon.

4°: ANNULAIRE.

N°1- Arrêt de sillon.
2- Sillon bifurqué.
3- Arrêt de sillon.
4- Sillon bifurqué.
5- Arrêt externe de la spirale centrale.
6- Arrêt interne de la spirale centrale.

CONCLUSIONS.

Il appert que les empreintes digitales photographiées par nous sur la vitre brisée dans un des salons de M.ALAUX correspondent exactement à celles que le pouce,l'index,le médius et l'annulaire de la main droite du nommé SCHEFFER auraient pu occasionner.

La position respective des traces de doigts imprimées sur les deux faces opposées de cette vitre,savoir: celle du pouce sur la face extérieure, et celles de l'index, du médius et de l'annulaire sur la face intérieure de la vitrine fracturée, démontre incontestablement que l'apposition de ces empreintes a été faite après le bris de la susdite vitre.

LE CHEF DU SERVICE DE L'IDENTITE JUDICIAIRE.

Alphonse Bertillon

ANNEXE 12 – ARTICLES DU CODE DU TRAVAIL CONCERNANT L'EMPLOI DE NOUVELLES TECHNOLOGIES DANS L'ENTREPRISE

Information du Comité d'entreprise

Article L2323-3

- Dans l'exercice de ses attributions consultatives, définies aux articles L. 2323-6 à L. 2323-60, le comité d'entreprise émet des avis et vœux.

L'employeur rend compte, en la motivant, de la suite donnée à ces avis et vœux.

Article L2323-4

- Pour lui permettre de formuler un avis motivé, le comité d'entreprise dispose d'informations précises et écrites transmises par l'employeur, d'un délai d'examen suffisant et de la réponse motivée de l'employeur à ses propres observations.

Article L2323-13

- Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail.

Les membres du comité reçoivent, un mois avant la réunion, des éléments d'information sur ces projets et leurs conséquences sur chacun des sujets mentionnés au premier alinéa.

Article L2323-32

- Le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de celles-ci.

Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci.

Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.

Information du salarié :

Article L1121-1

- Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

Article L1222-4

- Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.

Article L1321-1

- Le règlement intérieur est un document écrit par lequel l'employeur fixe exclusivement :

1° Les mesures d'application de la réglementation en matière de santé et de sécurité dans l'entreprise ou l'établissement, notamment les instructions prévues à l'Article L4122-1 ;

2° Les conditions dans lesquelles les salariés peuvent être appelés à participer, à la demande de l'employeur, au rétablissement de conditions de travail protectrices de la santé et de la sécurité des salariés, dès lors qu'elles apparaîtraient compromises ;

3° Les règles générales et permanentes relatives à la discipline, notamment la nature et l'échelle des sanctions que peut prendre l'employeur.

BIBLIOGRAPHIE

I- TEXTES OFFICIELS

Union européenne

- **Conventions, Charte, Directive, Règlement**

Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales STCE n° 005 du 4 nov. 1950, disponible sur le site www.echr.coe.int

Conseil de l'Europe, STE n° 108, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janv. 1981, disponible sur le site www.coe.int

Directive 95/46 CE du 24 octobre 1995 du Parlement européen et du Conseil 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, JOCE L. 281/31, 23 nov. 1995, disponible au www.cnil.fr

Charte des Droits Fondamentaux de l'Union Européenne, 2000/C 364/01, JOCE du 18 décembre 2000, disponible sur le site www.europarl.europa.eu

Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, disponible sur le site http://europa.eu

- **Décisions de la Commission européenne**

Décision n° 2000/518/EC du 26 juillet 2000 relative à la constatation, conformément à la directive 95/46/CE du Parlement européen et du Conseil, du caractère adéquat de la protection des données à caractère personnel en Suisse notifiée sous le numéro C(2000) 2304.

Décision n° 2002/2/EC du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques notifiée sous le numéro C(2001) 4539.

Décision n° 2003 1731 du 30 juin 2003 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par l'Argentine.

Décision du 21 novembre 2003 constatant le niveau de protection adéquat des données à caractère personnel à Guernesey notifiée sous le numéro C(2003) 4309.

Décision n° 2004/411/CE du 28 avril 2004 constatant le niveau de protection adéquat des données à caractère personnel dans l'île de Man.

Décision n° 2004/535/CE du 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au bureau des douanes et de la protection des frontières des États-Unis notifiée sous le numéro C(2004) 1914.

France

- **Lois**

Loi n° 78- 17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : JO du 7 janvier 1978 et rectificatif au JO du 25 janv. 1978

Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information er relative à la signature électronique, JO du 14 mars 2000 p. 3968

Loi n° 2000-321 du 12 avril 2000 relative aux droits des citoyens dans leurs relations avec les administrations, JO n° 88 du 13 avril 2000 p. 5646

Loi n° 2002-73 du 17 janv. 2002 de modernisation sociale, JO 18 janv. 2002, p. 1008

Loi n° 2003-239 du 18 mars 2003 sur la sécurité intérieure, JO du 19 mars 2003

Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JO du 22 juin 2004

Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO du 7 août 2004.

Loi n° 2007-1631 du 20 novembre 2007 relative à la maîtrise de l'immigration, à l'intégration et à l'asile, JO n° 270 du 21 novembre 2007, p. 18993

- **Décrets**

Décret n° 87-249 du 8 avril 1987, JO n° 84 du 9 avril 1987, p. 4046 modifié par le décret n° 2005-585 du 27 mai 2005 relatif au fichier automatisé des empreintes digitales gérées par le ministère de l'Intérieur, JO n° 124 du 29 mai 2005, p. 9533

Décret n° 2004-1266 du 25 novembre 2004 pris pour l'application de l'article 8-4 de l'ordonnance n° 45-2658 du 2 novembre 1945 relative aux conditions d'entrée et de séjour des étrangers en France et portant création à titre expérimental d'un traitement automatisé des données à caractère personnel relatives aux ressortissants étrangers sollicitant la délivrance d'un visa, JO n° 275 du 26 novembre 2004.

Décret n° 2007-451 du 25 mars 2007 modifiant le décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004, JO 28 mars 2007, p. 5782

Etats-Unis d'Amérique

Department of Homeland Security, Homeland Security Act, Public Law 107-296, 107th Congress, 2002 November 25th

Canada

Loi sur la protection des renseignements personnels L.R.C. 1985, c. P-21, disponible sur le site www.justice.gc.ca

Loi sur la protection des renseignements personnels et les documents électroniques, 2000 ch. 5, p. 8.6, 13 avril 2000, disponible sur www.justice.gc.ca

- **Québec**

Code civil du Québec, L.Q. 1991, c. 64, articles 35 à 41, disponible sur le site www.cai.gouv.qc.ca

- **Alberta**

Personal Information Protection Act, S.A. 2003, c. P-6.5, January 2004, disponible sur le site www.oipc.ab.ca

- **Saskatchewan**

The Freedom of Information and Protection of Privacy Act, S.S. 1990-91, c. F-22.01, current version March 31th 2009, disponible sur le site www.oipc.sk.ca

- **Colombie Britannique**

Personal Information Privacy Act, S.B.C. 2003 c. 63, October 23, 2003, into force on January 1st, 2004, disponible sur le site www.oipc.bc.ca

II- OUVRAGES

Techniques biométriques

Jacques PIERSON, « La biométrie, l'identification par le corps », collection informatique, édition Lavoisier, 2007.

Sciences politiques et sécurité informatique

Big Brother Awards, « Les surveillants surveillés », édition La Découverte, Zones, octobre 2008.

Sous la direction de X. Crettiez et P. Piazza, « Du papier à la biométrie, identifier les individus », édition Presses de la Fondation Nationale des sciences politiques, 2006.

Sous la direction de A. Dahmani, « La démocratie à l'épreuve de la société numérique », édition Gemdev – Karthala, 2007.

Sous la direction de S. Lacour, « La sécurité aujourd'hui dans la société de l'information », actes des séminaires de recherche du programme Asphalès ACI sécurité informatique, 2004-2007, édition l'Harmattan, 2007.

Sous la direction de S. Lacour, « La sécurité de l'individu numérisé : réflexions prospectives et internationales », actes du colloque du programme de recherche Asphalès, ACI informatique, Paris, 22 et 23 novembre 2007, édition l'Harmattan, 2008.

Sous la direction de X. Patier, Regards sur l'actualité n°349, « Sécurité et libertés publiques » La documentation française, Mars 2009.

Informatique et libertés

Christiane Féral-Schuhl, Cyberdroit, le droit à l'épreuve de l'Internet, Praxis Dalloz 5ème édition 2009-2010.

J. Frayssinet, La protection des données personnelles , in Lucas A., Dezève J. et Freyssinet J., Droit de l'informatique et de l'internet, PUF, 2001.

M.-L. Laffaire, Protection des données à caractère personnel, éd d'Organisation, 2005.

X. Linant de Bellefonds et Hollande A., Pratique du droit de l'informatique, Delmas, 2002.
N. Mallet-Poujol, « Traçage électronique et libertés », La documentation française, Collection problèmes économiques et sociaux n° 925, Paris, 2006.

N. Mallet-Poujol, Lamy Droit de l'Informatique et des Réseaux, Ouvrage collectif sous la direction de M. Vivant, 2009.

M.-C. Piatti, Les libertés individuelles à l'épreuve des NTIC, Ouvrage collectif sous la direction de M.-C. Piatti, PUL, 2001.

Droit du travail

S. Allemand, M. Miné, « Siffler en travaillant ? Des droits de l'homme au travail : un état des lieux », Editions Le cavalier Bleu, 2006.

I. de Benalcazar, « Droit du travail et nouvelles technologies », collection Business, Montchrestien, 2003.

B. Géniaut, « La proportionnalité dans les relations du travail, de l'exigence au principe », Nouvelle Bibliothèque des Thèses, Dalloz, 2009.

A. Supiot, « Critique du droit du travail », Quadrige Essais débats, PUF, 2ème édition, Août 2007.

Sous la direction de B. Teyssié, « Les notions fondamentales du droit du travail », Colloques, éditions Panthéon Assas, LGDJ Diffuseur, 2009.

P. Waquet, L'entreprise et les libertés du salarié, collection droit vivant, éditions Liaisons, 2003.

Divers

G. Cornu, Vocabulaire juridique, Association Henri Capitant, PUF, Quadrige, 2003.

J. Domat, « Les lois civiles dans leur ordre naturel », (1689), Paris, veuve Cavelier, t. 1, 1771, p. 204 in ENCINAS DE MUNAGORRI (R.), Introduction au droit, Flammarion, Champs Université, 2002, p. 277.

I. Kant, « Fondements de la métaphysique des mœurs », traduction de Victor Delbos, éd. LGF, 1993.

T. de Koninck, « De la dignité humaine », Essai, PUF, Quadrige, 2002.

III- ARTICLES

Français

L. Acharya, « La biométrie et son usage par l'Etat », Division des sciences et de la technologie, bibliothèque du Parlement, 11 septembre 2006.

G. Agamben, « Non à la biométrie », Journal Le Monde, 6 décembre 2005, p. 25.

E. Barbry, « La biométrie dans les entreprises est permise sous réserve de certaines précautions », Gazette du Palais, 20 octobre 2005 n° 993, p. 14.

E. Barbry, S. Rouillé-Mirza, « La biométrie dans l'entreprise, quand l'innovation se heurte à la culture de l'interdit », Gazette du Palais, 21 juillet 2005, n° 202 p.7.

Ch. Byk, « Biométrie et constitution : est-il trop tard pour les libertés publiques ? », Article publié sur le site internet de l'Association Internationale Droit Ethique et Science, année 2006, http://www.iales.org

E. A. Caprioli et I. Cantero, « Le choix d'un correspondant à la protection des données à caractère personnel. », La Semaine Juridique Entreprise et Affaires n° 25, 22 Juin 2006, 1976.

E. Caprioli, « Traitements utilisant des données biométriques », Communication commerce électronique n°3, mars 2007, p. 40-41.

A. Ceyhan, « La biométrie : une technologie pour gérer les incertitudes de la modernité contemporaine. Applications américaines », in Pierre Piazza (dir.), Police et identification. Enjeux, pratiques, techniques, Les Cahiers de l'INHES, n° 56, premier semestre 2005.

L. Dauxerre, « Le corps, carte d'identité du salarié », La semaine juridique sociale n°46, Lexis Nexis 1578, 11 novembre 2008.

A. De Laubadère, « loi relative à l'informatique, aux fichiers et aux libertés », ADJA 1978 p. 150

B. Dorizzi, « Modalités biométriques : présentation et comparaison » in La sécurité aujourd'hui dans la société de l'information, Programme Asphalès, édition l'Harmattan, année 2007, p. 69-86.

G. Dubey, « Nouvelles techniques d'identification, nouveaux pouvoirs. Le cas de la biométrie », Cahiers internationaux de sociologie 2008/2, n° 125, p. 263-279.

D. Duclos, « Ces industries florissantes de la peur permanente », Le Monde Diplomatique, édition imprimée, p. 16 – 17, Août 2005.

M.-P. Fenoll-Trousseau, « Le correspondant informatique et liberté », La Semaine Juridique Entreprise et Affaires, n°49, 8 décembre 2005, 1771.

D. Forest, « Les procédés sans traces, nouveaux sésames de la biométrie ? », Revue Lamy droit de l'immatériel, n°43, novembre 2008.

J. Frayssinet, « La loi Informatique, fichiers et libertés cuvée 2004 et le droit du travail : constantes et nouveautés », Actes des journées prud'homales d'Aix-en-Provence, Centre de Droit Social, PUAM, 2005.

J. Frayssinet, « La loi relative à l'Informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 : continuité et/ou rupture ? », Revue Droit de l'immatériel, éd. Lamy, décembre 2005, pp. 50 à 55.

S. Gauthronet, « Le devenir des données personnelles dans le cadre des restructurations d'entreprises » 23ème conférence internationale des commissaires à la protection des données, Paris 24, 25 et 26 septembre 2001.

K. Genel, « Le biopouvoir chez Foucault et Agamben », revue Methodos, Penser le corps, n°4, 2004.

X. Guchet, « Big Brother nous regarde-t-il vraiment ? », in La démocratie à l'épreuve de la société numérique, sous la direction d'Ahmed Dahmani, édition Gemdev – Karthala, 2007, p. 359 et suivantes.

Cl. Guerrier, « Protection des données personnelles et applications biométriques en Europe », Communication Commerce Electronique, n°7 juillet 2003, Chroniques p. 17-22.

Cl. Guerrier, « Les enjeux de la biométrie en 2003 », publié dans L'année des TIC 2003, site internet http://www.ostic.info/docs/03_biometrie.pdf

Cl. Guerrier, Immigration et Biométrie, Juriscom.net, 11 septembre 2005, www.juriscom.net

Cl. Guerrier (avec la participation de Laure-Anne Cornelie), Les aspects juridiques de la biométrie, article publié en 2005 par le site internet www.biometrie-online.org

D. Guinier, « Biométrie : classification au vu des nouveaux défis », Expertise des systèmes d'information, n°289, février 2005, p. 62-68.

S. Hadjali, « Droit du travail et nouvelles technologies : de la cybersurveillance à la cyberconfiance », Gazette du Palais, 20 avril 2006 n°110 p. 30.

N. Ivaldi et P. Vincent, « Cybersurveillance des salariés et charte informatique », septembre 2005, site internet de Caprioli et associés, www.caprioli-avocats.com

M.-L. Laffaire et T. Elm, « Biométrie, la première décision d'une longue série » Expertises des systèmes d'information, août/septembre 2005, p. 299 et s.

P. Leclercq, « A propos de la biométrie (quelques réflexions après visite de l'exposition « Biométrie, le corps identité » à la cité des sciences), Communication commerce électronique, n° 3, mars 2006, p. 14-18.

A. Lepage, « La biométrie refoulée de l'entreprise », Communication Commerce Electronique n°10, Octobre 2005, comm 164.

V. Leblanc, « Des salariés en liberté surveillée », Entreprises et Carrières, n° 961, du 30 juin au 6 juil. 2009, p. 12 à 23.

L. Marquet de Vasselot, De l'expression par le comité d'entreprise de son avis, RJS 8-9/00, p. 607

M. Marzouki, « Enjeux des techniques de biométrie, une première approche », Association IRIS, 24 septembre 2001, http://www.iris.sgdg.org

N. Mallet-Poujol, « Protection de la vie privée et des données personnelles », legamedia, 2004, disponible au www.educnet.education.fr

Y. Poullet, « Safe Harbor Principles – une protection adéquate ? », 17 juin 2000, disponible au www.juriscom.net

Rietsch, Caprioli, Kervasdoué et Pépin, « Protection du patrimoine informationnel », FedIsa et fondation CIGREF, année 2007, disponible sur le site www.caprioli-avocats.com

F. Rigaud, « L'élaboration d'un right of privacy par la jurisprudence américaine », Revue internationale de droit comparé, volume 32 n°4, 1980, pp. 701-730.

D. Touchent, « La mise en œuvre d'un système de badgeage par empreintes digitales dans l'entreprise », La semaine juridique entreprises et affaires n°37, Lexis Nexis 1337, 15 sept. 2005.

M. Vivant, Nathalie Mallet-Poujol, Jean-Michel Bruguière, « Droit de l'Informatique », La semaine juridique entreprises et affaires n°27, Lexis Nexis 1674, 2 juil. 2009.

A. Weber, J.-R. Lecerf, « Faut-il avoir peur de la biométrie ? », L'Express, 5 sept. 2005, p. 2-3.

Anglais

M. Crompton, "The end of the world as we know it or the white knight of privacy?", Biometric Institute Conference, Sydney, 20 march 2002, www.privacy.gov.aus

G. T. Clarke, "Biometrics in workplace – Where to draw the line?", Personal Information Protection Act Conference 2006, April 26 and 27, 2006, Calgary, Alberta.
http://www.verney.ca/pipa2006/presentations/a1_gary_clarke_paper.pdf

T. Pilgrim, "Speech to Biometrics Institute, Biometric and Privacy", Conference to Hyatt Hotel Cambera , 21 November 2007, www.privacy.gov.au

J. Stanley and B. Steinhardt, "Bigger Monster, weaker chains: The growth of an American surveillance society", January 2003, ACLU (American Civil Liberties union) http://www.aclu.org/privacy/gen/15162pub20030115.html

B. Yanikoglu and A. Kholmatov, "Combining Multiple Biometrics to Protect Privacy", Sabanci University, Istanbul, Turkey. Site internet de l'Université de Sabanci, http://www.sabanciuniv.edu.tr

A. Cavoukian, M. Snijder, "The relevance of untraceable biometrics and biometric encryption: a discussion of biometrics for authentification purposes", Information of the privacy commissioner Of Ontario, August 2009, disponible sur le site www.biometricgroup.com

IV- THESE ET MEMOIRE

J. Le Clainche, « L'adaptation du droit des données personnelles aux communications électroniques », Thèse de doctorat sous la direction de N. Mallet-Poujol et J. Frayssinet, Université Montpellier I, soutenue le 11 décembre 2008.

D. Auger, « Biométrie : l'équilibre entre libertés individuelles et promesse sécuritaire serait-il possible ? », Mémoire pour l'obtention du DESS, Université Paris I – Panthéon-Sorbonne, sept. 2005

J-B. Thomas, « Identification biométrique, protection des données et droit de l'homme », Mémoire pour l'obtention du Master 2, Université Paris I – Panthéon-Sorbonne, sept. 2007.

V- RAPPORTS, COMMUNICATIONS

France

- **CNIL**

CNIL, « Voix, image et protection des données personnelles », Documentation française 1996.

CNIL, Communication « La Biométrie », 1er juin 2005, site internet www.cnil.fr

CNIL, Communication relative à « Traces actives et sécurité », Philippe LEMOINE, 10 mars 2005, site internet de la CNIL, www.cnil.fr

CNIL, « Le vote par internet aux élections politiques, les éléments du débat », 28 mai 2006, disponible sur le site www.cnil.fr
CNIL, « Affaire SWIFT : la CNIL demande de la transparence », article du 13 juin 2007, disponible au www.cnil.fr

CNIL, Communication relative à « La mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données », 27 nov. 2007, disponible sur le site www.cnil.fr

CNIL, « Etat des lieux en matière de procédés d'anonymisation », direction de l'expertise, étude sur le site internet de la CNIL : http://www.cnil.fr/index.php?id=1536

20° rapport d'activité 1999, « Le commerce électronique : la confiance en jeu », p. 101, disponible sur le site www.ladocumentationfrancaise.fr

21° rapport d'activité 2000, « Les contrôles d'accès par biométrie », p. 101 et s., disponible sur le site www.ladocumentationfrancaise.fr

22° rapport d'activité 2001, « Un siècle de biométrie », p. 157 et s., disponible sur le site www.ladocumentationfrancaise.fr

24° rapport d'activité 2003, « L'impératif de sécurité et ses contreparties », p. 25 et s., disponible sur le site www.ladocumentationfrancaise.fr

26° rapport d'activité 2005, « L'homo informaticus biométrisé », p. 49 et s., disponible sur le site www.ladocumentationfrancaise.fr

27° rapport d'activité 2006, « La convergence des technologies », p. 13, disponible sur le site www.ladocumentationfrancaise.fr

28° rapport d'activité 2007, « Encadrer la biométrie », p. 18 et s., disponible sur le site www.ladocumentationfrancaise.fr

29° rapport d'activité 2008, « Sanctionner », p. 47, disponible sur le site www.ladocumentationfrancaise.fr

30° rapport d'activité 2009, La CNIL en action, « Les initiatives parlementaires pour réviser la loi Informatique et Libertés », p. 45 et s., disponible sur le site www.ladocumentationfrancaise.fr

- **Groupement, Association**

GIXEL (Groupement des Industries de l'Interconnexion des composants et des sous ensembles électroniques), Livre Bleu de l'Industrie « Grands programmes structurants, proposition des industries électroniques et numériques », Juillet 2004.

Ligue des Droits de l'Homme, « Passeport biométrique : IRIS et la LDH demandent au Conseil d'État d'annuler le décret », communiqué du 4 juill. 2008 disponible au www.ldh-france.org

Ligue des Droits de l'Homme, « La biométrie… au risque de nos libertés », article du 10 oct. 2009, disponible au www.ldh-toulon.net

- **Assemblée Nationale et Sénat**

Rapp. min. Travail, emploi et formation professionnelle de G. Lyon-Caen, Les libertés publiques et l'emploi,: La Documentation française, Paris, 1992.

Rapport de Guy Braibant, « Données personnelles et société de l'information », rapport au Premier Ministre sur la transposition en droit français de la directive n° 95/46, le 3 mars 1998.

Office parlementaire d'évaluation des choix scientifiques et technologiques, « La valeur scientifique de l'utilisation des empreintes génétiques dans le domaine judiciaire » par Christian Cabal, député, n° 3121 Assemblée Nationale (11ème législature) et Sénat n°94 (2001-2002), 7 juin 2001.

Office parlementaire d'évaluation des choix scientifiques et technologiques, « les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre », par Christian CABAL, député, n°0938, Assemblée Nationale (12ème législature) et Sénat, 16 juin 2003.

Rapport d'information de Jean-René LECERF, fait au nom de la commission des lois et de la mission d'information de la commission des lois, sur la nouvelle génération de documents d'identité et la fraude documentaire, n° 439 (2004-2005), 29 juin 2005

Office parlementaire d'évaluation des choix scientifiques et technologiques, « La Biométrie », par Christian CABAL, député, n°3302, Assemblée Nationale (12ème législature) et Sénat, Compte rendu de l'audition publique du 4 mai 2006.

Rapport d'information établi par M. Yves DÉTRAIGNE et Mme Anne-Marie ESCOFFIER, « Le respect de la vie privée à l'heure des mémoires numériques », Sénat n°441, Session 2008-2009, déposé le 27 mai 2009.

- **Commissions nationales**

CNCDH, Problèmes posés par l'inclusion d'éléments biométriques dans la carte nationale d'identité, 1er juin 2006.

CCNE, avis n°98, Biométrie, données identifiantes et droits de l'homme, 20 juin 2007, site internet http://www.ccne-ethique.fr/

Union européenne

Groupe de travail Article 29, Avis 8/2003 relatif au projet de clauses contractuelles types présenté par un groupe d'associations professionnelles (« le contrat type alternatif »), GT 8411754/03/FR, adopté le 17 déc. 2003

Groupe de travail Article 29, Avis 3/2005 sur l'application du règlement (CE) n°2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, JO L 385 du 29 décembre 2004 p. 1 - 6

Comité Consultatif du conseil de l'Europe de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Rapport d'étape sur l'application des principes de la convention 108 à la collecte et au traitement des données biométriques, 21ème réunion du 2-4 février 2005

Parlement européen, « SWIFT : les données bancaires européennes doivent être traitées selon les normes européennes, estiment les députés », communiqué de presse, 3 sept. 2009, disponible au www.europarl.europa.eu

Suisse

Préposé fédéral à la protection des données et à la transparence, 9° Rapport d'activités 2001-2002, « Identification biométrique et les risques inhérents à cette méthode », p. 29 et s., disponible sur le site www.edoeb.admin.ch

Préposé fédéral à la protection des données et à la transparence, 12° Rapport d'activités 2004-2005, « Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé », p. 27 et s., disponible sur le site www.edoeb.admin.ch

Préposé fédéral à la protection des données et à la transparence, 13° Rapport d'activités 2005-2006, « Système biométrique de contrôle d'accès à un centre sportif », p. 30 et s., disponible sur le site www.edoeb.admin.ch

Préposé fédéral suisse à la protection des données et à la transparence (PFPDT), 15ème Rapport d'activité 2007-2008 « Introduction de données biométriques dans les documents d'identité. », p. 17, www.edoeb.admin.ch

Préposé fédéral à la protection des données et à la transparence, 16° Rapport d'activités 2008-2009, « Système de reconnaissance faciale dans les stades de sport », p. 22 et s., disponible sur le site www.edoeb.admin.ch

Canada

Consumer Biometric Applications: A Discussion Paper, Ann Cavoukian Ph.D., Information and Privacy Commissioner/Ontario, September 1999.

Commission de l'Ethique de la Science et de la Technologie, document de réflexion sur « L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques », 1er juin 2005, http://www.ethique.gouv.qc.ca

Etats-Unis

Department of Homeland Security: Privacy Impact Assessment for the Biometric Storage System, March 28, 2007 http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_bss.pdf

Organisation Internationale

OCDE

Direction de la Science, Technologie et industrie, Comité de l'information l'informatique et des communications, Groupe de travail sur la sécurité de l'information et de la vie privée, 23 décembre 200, DSTI/ICCP/REG(2003)3/FINAL.

Direction de la science, de la technologie et de l'industrie. Comité de la politique de l'information, de l'informatique et des communications, Groupe de travail sur la sécurité de l'information et de la vie privée, « Technologies fondées sur la Biométrie », 10 juin 2005, références DSTI/ICCP/REG(2003)2/FINAL

VI- DELIBERATIONS ET JURISPRUDENCES

Délibérations CNIL

- **Autorisations unique**

Délibération n° 2006-101 du 27 avr. 2006 portant autorisation unique AU-007de mise en œuvre de dispositif biométrique reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail, J.O n° 138 du 16 juin 2006.

Délibération n° 2006-102 du 27 avr. 2006 portant autorisation unique AU-008 de mise en œuvre de dispositif biométrique reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail, J.O n° 138 du 16 juin 2006.

Délibération n° 2009-316 du 7 mai 2009 portant autorisation unique AU-019 de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle d'accès aux locaux sur les lieux de travail, JO n° 0142 du 21 juin 2009.

- **Demande d'autorisation**

Délibération n°00-056 du 16 novembre 2000 portant avis sur un projet d'arrêté présenté par le ministre de l'Education nationale concernant un traitement automatisé d'informations nominatives ayant pour finalité le contrôle d'accès par la reconnaissance des empreintes digitales de certains personnels de l'Education nationale, pour certains locaux de la cité académique de Lille, www.legifrance.gouv.fr

Délibération n° 00-057 du 16 nov. 2000 portant avis sur un projet d'arrêté présenté par le préfet de l'Hérault concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion du temps de travail des agents de la préfecture, www.legifrance.gouv.fr

Délibération n° 2006-005 du 23 avr. 2002 relative à la demande d'avis présentée par la mairie de Goussainville concernant la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion des horaires de travail des personnels communaux, www.legifrance.gouv.fr

Délibération n° 02-045 du 18 juin 2002 portant avis sur un projet de décision du directeur de l'URSSAF de la Corse relatif à la mise en œuvre d'un dispositif de reconnaissance de l'empreinte digitale destiné à contrôler les accès aux locaux professionnels de l'URSSAF, www.legifrance.gouv.fr

Délibération 2005-035 du 17 fév. 2005. Délibération portant refus d'autorisation de la mise en œuvre par la société MFG Education d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés,www.legifrance.gouv.fr

Délibération 2005-037 du 17 fév. 2005. Délibération portant refus d'autorisation de la mise en œuvre par la mairie des Sables d'Olonne d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés,www.legifrance.gouv.fr

Délibération 2005-036 du 17 fév. 2005. Délibération portant refus d'autorisation de la mise en œuvre par la société Paris Monitoring d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés,www.legifrance.gouv.fr

Délibération 2005-034 du 17 fév. 2005. Délibération portant refus d'autorisation de la mise en œuvre par la société UCOM d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés, www.legifrance.gouv.fr

Délibération 2005-031 du 17 fév. 2005. Délibération portant refus d'autorisation de la mise en œuvre par la société UTEL d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance du contour de la main et ayant pour finalité le contrôle des horaires des employés, www.legifrance.gouv.fr

Délibération n° 2006-005 du 12 janv. 2006 portant refus d'autorisation de la mise en œuvre par la clinique de Goussonville d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle des horaires des employés, www.legifrance.gouv.fr

Délibération n° 2006-069 du 16 mars 2006 portant autorisation de la mise en œuvre par la société Brisach SAS d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalités le contrôle des horaires et le contrôle de l'accès aux locaux, www.legifrance.gouv.fr

Délibération n° 2006-070 du 16 mars 2006 portant autorisation de la mise en œuvre par la société Sagem Défense Sécurité d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, www.legifrance.gouv.fr

Délibération n° 2006-158 du 30 mai 2006 portant autorisation de la mise en œuvre par la société La Mesta Chimie Fine SAS d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, www.legifrance.gouv.fr

Délibération n° 2007-006 du 18 janv. 2007 autorisant la mise en œuvre par l'université d'Evry-Val d'Essonne d'un traitement automatisé de données à caractère personnel ayant pour finalité principale l'évaluation d'algorithmes de reconnaissance du visage et de l'iris, www.legifrance.gouv.fr

Délibération n° 2007-050 du 21 mars 2007 autorisant la mise en œuvre par François Charles Oberthur Fiduciaire d'un traitement automatisé de données à caractère personnel reposant sur

la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles, www.legifrance.gouv.fr

Délibération n° 2007-051 du 21 mars 2007 autorisant la mise en œuvre par Millenium Chemicals Thann SAS d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux sensibles, www.legifrance.gouv.fr

Délibération n° 2007-054 du 21 mars 2007 autorisant la mise en œuvre par la société Brevalex d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, www.legifrance.gouv.fr

Délibération n° 2007-056 du 21 mars 2007 autorisant la mise en œuvre par le port autonome de Bordeaux d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès à un appontement pétrolier et gazier, www.legifrance.gouv.fr

Délibération n° 2007-248 du 13 sept. 2007 autorisant la mise en œuvre par la Manufacture française des pneumatiques Michelin d'un traitement automatisé de données à caractère personnel reposant sur un procédé de reconnaissance vocale et ayant pour finalité la gestion des mots de passe, www.legifrance.gouv.fr

Délibération n° 2007-296 du 4 oct. 2007 autorisant la mise en œuvre par le Groupe des Ecoles des Télécommunications (GET) d'un traitement automatisé de données à caractère personnel ayant pour finalité principale l'évaluation d'algorithmes de reconnaissance de diverses données biométriques, demande d'autorisation n° 1226906, www.legifrance.gouv.fr

Délibération n° 2007-339 du 8 nov. 2007 autorisant la mise en œuvre par la société Hitachi Data Systems d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès au système d'information, autorisation n° 1248197, www.legifrance.gouv.fr

Délibération n° 2008-038 du 7 fév. 2008 autorisant la mise en œuvre par le Centre d'aide au travail - « le Vert Coteau » de Thionville d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux et ayant pour finalité le contrôle de la présence des travailleurs handicapés, autorisation n° 1238037, www.legifrance.gouv.fr

Délibération n° 2008-058 du 6 mars 2008 refusant la mise en œuvre par la SARL Brochage 3000 d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des horaires, autorisation n° 1192992, www.legifrance.gouv.fr

Délibération n° 2008-084 du 27 mars 2008 autorisant la mise en œuvre par la société Thales Security Systems d'un traitement automatisé comportant des données biométriques nécessaires au contrôle de l'identité des personnes, autorisation n° 1239796, www.legifrance.gouv.fr

Délibération n° 2008-098 du 10 avr. 2008 autorisant la mise en œuvre par l'Ecole nationale supérieure d'ingénieurs de Caen (ENSICAEN) d'un traitement de données à caractère personnel ayant pour finalité la création d'une plate-forme de tests biométriques, autorisation n° 1198593, www.legifrance.gouv.fr

Délibération n° 2008-233 du 17 juil. 2008 refusant la mise en œuvre par la société Histoire et patrimoine d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des accès aux locaux, autorisation n°1296677, www.legifrance.gouv.fr

Délibération n° 2008-395 du 6 nov. 2008 refusant la mise en œuvre par la société TAM Airlines d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des horaires, autorisation n° 1281379, www.legifrance.gouv.fr

Délibération n° 2009-025 du 29 janv. 2009 refusant la mise en œuvre par la société Famer Industrie Maintenance d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux et le contrôle des horaires, autorisation n° 1290116, www.legifrance.gouv.fr

Délibération n° 2009-026 du 29 janv. 2009 autorisant la mise en œuvre par le Service Départemental d'Incendie et de Secours de l'Isère (SDIS) d'un traitement de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux, autorisation n° 1303760, www.legifrance.gouv.fr

Délibération n° 2009-311 du 7 mai 2009 autorisant la mise en œuvre par le Centre de culture physique d'Aquitaine d'un traitement de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité la gestion de l'accès à la salle de sport, autorisation n°1309515, www.legifrance.gouv.fr

Délibération n° 2009-360 du 18 juin 2009 autorisant la mise en œuvre par le Graduate Management Admission Council (GMAC) représenté par Pearson Education France d'un traitement de données à caractère personnel reposant sur la reconnaissance du réseau veineux de la paume de la main et ayant pour finalité de contrôler l'accès à des salles d'examen et d'empêcher la substitution de candidat à l'examen GMAT, demande d'autorisation n°1323460, www.legifrance.gouv.fr

Délibération n° 2010-033 du 11 février 2010 autorisant la mise en œuvre par le Centre Oscar Lambret de Lille d'un traitement de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale avec base centralisée et ayant pour finalité le contrôle de l'identité des patients pris en charge en radiothérapie, demande d'autorisation n° 1340737, www.legifrance.gouv.fr

- **Sanctions**

Délibération n° 2006-173 du 28 juin 2006 prononçant une sanction pécuniaire à l'encontre de la SCP X, www.legifrance.gouv.fr

CNIL, Délibération n° 2009-201 du 16 avr. 2009 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la société Jean-Marc Philippe, www.legifrance.gouv.fr

Délibération n° 2010-072 du 18 mars 2010 de la formation restreinte décidant l'interruption d'un traitement mis en œuvre par la Société M., www.legifrance.gouv.fr

- **Autres**

Délibération n° 94-095 du 15 nov. 1994 relative à la proposition modifiée de directive du Conseil de l'Union européenne relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel et à la libre circulation de ces données, www.legifrance.gouv.fr

Délibération n° 96-084 du 1° oct. 1996 portant avis sur le projet de décret pris en application de l'article 18 de la loi du 6 janv. 1978 relatif à l'utilisation du numéro d'inscription au répertoire national d'identification des personnes physiques par le ministère de l'Enseignement supérieur et le CEREQ, 17° rapport 1996, www.ladocumentationfrancaise.fr

Jurisprudences

- **Droit Social**

Cass. crim., 17 juin 1986, Dr. ouvrier 1987 n° 273, note J. G

Cass. soc., 15 oct. 1987, Bull. civ. V, n° 569

Cass. soc. 2 juill. 1987, Bull. civ. V, n° 438

Cass. soc,. 1997 RJS 11/1997 n° 1252; TPS 1997, n° 264, obs. Teyssié

Cass. soc., 3 mars 1988 Bull. civ. V, n° 152, D. 1988, somm. 312, obs. Lyon-Caen

Cass. soc., 20 nov. 1991, n° 88-43.120, Bull. civ. V, n° 519.

Cass. soc., 14 mai 1992, n° 89-45.300, Bull. civ. V, n° 309.

Cass. crim., 11 mars 1993, n° 90-84.931, commentaire de Bernard Bouloc, RSC 1994 p. 101 ; Rec. Dalloz 1994 p. 156.

Cass. crim., 3 mai 1994, Bull. crim. 1994 n° 164 p. 375

Cass. soc., 28 oct. 1996, Dr. soc. 1996 n° 1105

Cass. soc., 12 nov. 1997, Dr. soc. 1998, n° 87, obs. M. Cohen

Cass. soc., 16 juin 1998 : D. 1998. IR. 177.

Cass. soc., 14 mars 2000, n° 1270, n° 98-42.090, Bull. civ. V, n° 101

Cass. Soc., 3 avr. 2001, D. Soc. 2001, p. 675, obs. Gauriau.

Cass. soc., 2 oct. 2001, Arrêt Nikon, pourvoi n° 99-42.942, Bull. 2001. V n° 291, p. 233, RTD Civ. 2002, p. 72, note de J. Hauser.

Cass. crim., 4 juin 2002, n° 01-83.062, disponible au www.legifrance.gouv.fr

CA Aix-en-Provence, 1er ch. A, 25 novembre 2003, n°2003/798.

Cass. Soc., 6 avr. 2004, Société Allied Signal Industrial Fibers, devenue la société Honeywell Longlaville c/ M. Miguel Pacheco, FS- P+B+R+I, D. 2004, p. 2736 note R. de Quenaudon.

Cass. Crim 28 sept. 2004 n°03-86.604, Bull. crim. 2004 n° 224 p. 801

Cass. soc. 7 juin 2006, n° 04-43.866, Girouard c/ Continent France, Bull civ. V, n° 206 ; D. 2006, 1704

Cass. soc., 18 oct. 2006: Juris Data n° 2006-035418; Comm. com. électr. 2007, comm. 61, note A. Lepage.

Cass. soc., 21 déc. 2006, n° 05-41.165, commenté dans la Gazette du Palais, 7 août 2007, n° 219, p. 22.

CA Paris, 25 juin 2008, n° 08-04727, disponible sur le site www.dalloz.fr

Cass. soc., 9 juill. 2008, n° 06-45.800 : Juris Data n° 2008-044801.

Cass. soc., 17 juin 2009, Comm. com. électr. 2009, comm. 106, note É.-A. Caprioli.; Revue de droit du travail 2009 p. 591, comm. L. Marino.

Cass. soc., 21 oct. 2009, pourvoi n° 07-43.877, Bull. 2009. V, n° 226, disponible sur le site au www.legifrance.gouv.fr

- **Biométrie**

TGI Paris section sociale, 1ère chambre, 19 avril 2005, RG n° 05/00382 ou sur le site internet www.legalis.net

- **Conseil d'Etat**

Conseil d'Etat, 10 août 1917, n° 59855, arrêt Baldy, Recueil Lebon 1917, p. 000 ; Rec. CE, p. 638

CE Section, 16 mars 1962, Cie des tramways électriques d'Oran, Rec. p. 176, et JCP 1962 II, 12912, note J. Savatier.

Conseil d'Etat, 1er fév.1980, Dr social 1980, p. 310, concl. Bacquet.

- **Conseil Constitutionnel**

Décision DC n° 2007-557 du 15 novembre 2007, loi relative à la maîtrise de l'immigration, à l'intégration et à l'asile, « Les Cahiers du Conseil constitutionnel n° 24 », disponible sur le site au www.conseil-constitutionnel.fr

- **Autres**

TGI Rouen, 6 juin 1996, Dr. ouv. 1997, p. 24

Civ 1ère, 29 juin 1999, JCP 1999. II. 10187, note R. Martin

TGI Paris, ordonnance des référés, 3 mars 2008, n° 08-51650, disponible sur le site www.dalloz.fr

VII- GUIDES

France

Guide pratique « Déclarez à la CNIL un fichier ou un traitement de données personnelles », Juillet 2006, www.cnil.fr

Guide des transferts de données à caractère personnel vers des pays non membres de l'Union Européenne, Janvier 2007, www.cnil.fr

Guide pour les employeurs et les salariés, édition 2010, www.cnil.fr

Guide du correspondant Informatique et Libertés » édition 2006, www.cnil.fr

Guide du droit d'accès, édition 2010, www.cnil.fr

Suisse

Préposé fédéral à la protection des données et à la transparence, Guide relatif aux systèmes de reconnaissance biométrique, Novembre 2008, www.edoeb.admin.ch

VIII- LIGNES DIRECTRICES

Organisation de Coopération et de Développement Economique

Lignes directrices sur la protection de la vie privée et les flux transfrontalières de données à caractère personnel

Commissariat à la protection de la vie privée du Canada

Commissariat à la protection de la vie privée du Canada, Lignes directrices en matière d'identification et d'authentification, Octobre 2006, disponible sur le site www.priv.gc.ca

Commissariat à la protection de la vie privée du Canada, Lignes Directrices sur le traitement transfrontalier des données personnelles en matière d'identification et d'authentification, Janvier 2009, disponible sur le site www.priv.gc.ca

IX- SITES INTERNET

Français et Européens

- **Français**

Legifrance : http://www.legifrance.gouv.fr/
CNIL : http://www.cnil.fr/index.php?id=1
Conseil Constitutionnel : http://www.conseil-constitutionnel.fr/
Ministère de l'Immigration : http://www.immigration.gouv.fr/
Ministère de l'Economie et des Finances :
http://www.minefi.gouv.fr/dematerialisation_icp/dematerialisation_declar.htm
Commission Nationale d'Ethique : http://www.cne.public.lu/
Comité Consultatif National d'Ethique : http://www.ccne-ethique.fr/
Sénat : http://www.senat.fr/ue/pac/E2532.html
Ligue des droits de l'homme : http://www.ldh-france.org/
Club de la Sécurité de l'Information Français : http://www.clusif.asso.fr/
Cabinet Bensoussan : http://www.alain-bensoussan.com/pages/1/
Cabinet Caprioli : http://www.caprioli-avocats.com/
Groupement des industries de l'interconnexion des composants et des sous-ensembles électroniques (GIXEL) : http://www.gixel.fr/

- **Européens**

Europa: http://europa.eu/index_fr.htm
European Biometrics Portal : http://www.europeanbiometrics.info/
Commission Nationale pour la protection des données du Luxembourg:
http://www.cnpd.lu/fr/index.html
Coopération franco-allemande en matière de sécurité : http://www.france-allemagne.fr/Cooperation-franco-allemande-en,238.html
RISE (Rising Pan European and International awareness of biometrics and security ethics): http://www.riseproject.eu/

Américains

United States Justice Department : http://www.usdoj.gov/
Committee on Homeland Security : http://homeland.house.gov/
Department of Homeland Security : http://www.dhs.gov/index.shtm
Federal Bureau of Investigation: http://www.fbi.gov/
Central Intelligence Agency: https://www.cia.gov/
Integrate Automatic Fingerprint Identification System: http://www.fbi.gov/hq/cjisd/iafis.htm
Philip E. Agre, Department of Information Studies, University of California, Los Angeles:
http://polaris.gseis.ucla.edu/pagre/
American Civil Liberties Union : http://www.aclu.org/
Electronic Privacy Information Center : http://epic.org/privacy/biometrics/

American Payroll Association : http://www.americanpayroll.org/
Biometric Consortium: http://www.biometrics.org/
National Institute of Standards and Technology: http://www.itl.nist.gov/

Canadiens
Ministère de la Justice au Canada : http://www.justice.gc.ca/fr/
Citoyenneté et Immigration Canada : http://www.cic.gc.ca/FRANCAIS/
Commissariat à la protection des données du Canada : http://www.privcom.gc.ca/index_f.asp
Commission d'accès à l'information au Québec : http://www.cai.gouv.qc.ca/
Commission de l'Ethique de la Science et de la Technologie : http://www.ethique.gouv.qc.ca
Bibliothèque du Parlement canadien:
http://www.parl.gc.ca/common/library_prb.asp?Language=F
Canadian privacy law blog : http://www.privacylawyer.ca/

Australiens
Australian National University : http://www.anu.edu.au/index.php
Office of the Privacy Commissioner : http://www.privacy.gov.au/
Roger CLARKE home page : https://www.anu.edu.au/people/Roger.Clarke/
Biometrics Institute : http://www.biometricsinstitute.org/

Divers sites
International Biometric Group : http://www.biometricgroup.com/
International Biometric Industry Association : http://www.ibia.org/
Encyclopédie Wikipedia :
http://fr.wikipedia.org/wiki/Biom%C3%A9trie#Identification_des_personnes_2
Privacy International : http://www.privacyinternational.org/
Crimino Corpus : http://www.criminocorpus.cnrs.fr/article133.html
Biometrie-online : http://www.biometrie-online.net/
Legalis : www.legalis.net

INDEX

A

Accès (droit) :
- Contenu : 428, 432
- Conditions d'exercice : 438
- Exceptions : 447
- Indirect : 444

ADN : 2, 11, 31
Affichage : 361
Amende : 139, 257, 258, 348, 448
Anthropométrie : 6
Authentification, voir finalité
Autorisation préalable (procédure) : 142, 145
- Formalités : 147
- Notification : 152

Autorisation unique : 143, 171, 204

B

Bases de données : 224, 226, 247, 291, 295
Bagde : 176, 224, 228, 234
Besoin général de sécurisation : 227, 286
Biométrie,
- Confort: 22, 118, 126
- Définition: 1
- Gabarit: 63
- Histoire:7
- Multimodale: 100
- Taux: 77, 131, 135

Bulletin de paie: 195

C

Capture Live: 70
CCNE: 30, 264, 328
Clé USB: 204, 295
Charte Internet: 330
CHSCT: 395
Comité d'entreprise,
- Création: 386
- Missions: 387
- Consultation (introduction nouvelles technologies): 388
- Projet: 390, 393

Commissaire à la protection des données
- Australie : 138, 273, 323
- Canada : 282, 301, 322, 419
- Colombie Britannique
- Irlande : 276
- Québec : 32
- Nouvelle-Zélande : 323

Communication (droit de) : 430, 432
Conseil Constitutionnel : 11, 27
Consentement exprès : 402
- Conditions : 405, 410
- Réserves : 417

Conservation des données (durée de) :
Consultation, voir représentant du personnel.
Constitution : 26
Contrat de travail : 181, 233, 250, 261, 344, 377, 417, 442, 449.
Contrôle d'accès,
- Logique : 119
- Physique : 119

Contrôle des horaires, voir Finalité.
Contour de la main, voir reconnaissance
Convention 108: 293, 330
Correspondant Informatique et Libertés,
- Missions : 341, 342, 343
- Indépendance : 344
- Sanctions : 344

CNIL : 5, 139, 186, 457

D

Déclaration de conformité : 169
Délégués du personnel, voir représentant du personnel.
Dialogue social : 327, 339, 456

Dignité humaine : 26, 27, 28, 29, 30, 31, 32, 33
Données à caractère personnel
- Qualité : 267, 269
- Traitements ultérieurs : 272
Droits fondamentaux, Charte de l'Union européenne : 27, 330
Droit à la vie : 26,
Durée de conservation : voir Information
- Sanction : 257.
DUDH : 27,

E

Elections : 112
Empreintes digitales,
- Formation : 61
- Capture : 63, 70
- Enrôlement : 68
- Comparaison : 73
- Leurre : 79
Enjeux majeur,
- Intégrité des personnes : 230
- Biens et installations : 237
- Informations : 240
- Recherche scientifique : 242
Expert en technologies : 397

F

Fiabilité du système : 47, 54, 77, 87, 113, 133, 135, 138, 222, 265, 455
Finalité (principe de), 325
- Authentification : 176, 202
- Détournement : 148, 256
- Identification : 224,
- Empreintes digitales : 179
- Gestion des horaires : 181
  - Libertés individuelles : 184
  - Ethique : 189
- Gestion des contrôles d'accès : 202
Fort impératif de sécurité : 227

G

Gabarit biométrique, voir Biométrie
Géolocalisation : 1, 16, 261
Gestion des horaires, voir Finalité
GMAT : 248, 315

H

Historique de passage : 196, 233.

I

Identité: 14, 47, 103
Identification biométrique, voir Finalités
Information (obligation d')
- Modalités: 361
- Contenu: 364
- Salariés: 358
- Durée de conservation: 377
- Loyale: 261, 355, 358
- Transparente: 402
Interconnexion
- Définition: 370
- Information des salaries: 373
Iris, voir Reconnaissance

J

Juge des référés : 351

L

Loyauté (principe de) : voir information
Libertés individuelles,
- Restrictions : 298

O

OCDE
- Lignes directrices : 330
Opposition (droit d') : 421

P

Passenger Name Record : 18, 138
Passeports : 104
Pouvoir de direction : 418

Préposé Fédéral Suisse à la protection des données
Preuve,
- Définition : 35
- En matière civile : 41
- En matière pénale : 38
Proportionnalité (principe),
- Empreintes digitales : 287
- Fort impératif de sécurité : 289
- Intérêts collectifs : 264
- Usage nécessaire : 277
- Fiabilité du système : 279
- Usage raisonnable : 281

R

Reconnaissance (du)
- Contour de la main : 93
  - Finalités : 213
  - Accès clients : 217
  - Proportionnalité : 301, 306
- Réseau veineux des doigts de la main,
  - Finalité : 219, 252
  - Proportionnalité : 309
- Vocale : 97
  - Finalité : 222, 250
  - Proportionnalité : 318
- Iris : 86
- Faciale : 90

Rectification (droit) : 451
Représentants du personnel, 327
- Avis purement consultatif : 399
- Comité d'entreprise : 387
- Consultation (procédure) : 382
- Information : 385, 389
- Sanctions : 400

Réseaux sociaux : 261
Responsable de traitement
- Délégation : 340
- Mission : 336, 338, 339
- Sanctions : 346
- Procédures : 348, 351, 353
- Responsabilité : 338

S

Safe Harbor, voir Transferts de données
Secret Défense : 238, 240, 445
Sécurisation des paiements : 121, 124
Sécurisation des pensions et salaires : 122
Sous-traitant, voir responsable de traitement.
Stockage (durée), voir Information.
- Proportionnalité : 315

Subordination (lien de) :
Sûreté aéroportuaire : 115
Surveillance des salariés :
SWIFT : 20,

T

Traçabilité : 208, 284, 310
Transfert de données : 155
- Safe Harbor : 158, 157
- Clauses contractuelles type : 163
- Règles contraignantes d'entreprise : 165

Transparence (principe de)

V

Vie privée : 16, 43, 185, 186, 261
Vidéosurveillance : 16, 269
Visa : 23, 108

TABLES DES MATIERES

REMERCIEMENTS **5**

INTRODUCTION GENERALE **7**

Chapitre 1. Le contexte d'implantation de la biométrie 14

Chapitre 2. Les enjeux de la biométrie 21

A- La déroute identitaire de l'emploi de dispositifs biométriques 22

B- L'enjeu politico – stratégique de la biométrie 25

C- Le marché lucratif de la biométrie 29

Chapitre 3. La biométrie source de craintes 31

A- La dignité humaine et le droit à la vie privée 31

1°) La dignité humaine 32

2°) La vie privée 33

B- Le fardeau de la preuve en biométrie 38

1°) La force probante de la donnée biométrique en matière pénale 39

2°) La force probante de la donnée biométrique en matière civile 41

C- La biométrie, technologie au service de la protection de la vie privée 42

Chapitre 4. La position du problème 45

TITRE I – Le contrôle collectif de l'usage de la biométrie en entreprise **49**

Chapitre Préliminaire : Les différentes techniques biométriques 51

Section 1- La propagation contrôlée des outils biométriques 52

A. La technique de reconnaissance par empreinte digitale 54

1°) La formation de l'empreinte digitale 54

2°) La capture de l'empreinte digitale 55

B. Les étapes du traitement de l'empreinte digitale 59

1°) L'enrôlement 59

2°) La capture live 60

3°) La comparaison 61

C. La probabilité d'erreur d'un système biométrique 63

D. Les leurres 64

E. Les autres modalités biométriques 66

1°) La prééminence des caractéristiques biologiques ou morphologiques 67
1-1 La reconnaissance de l'iris 67
1-2 La reconnaissance faciale 72
1-3 La reconnaissance du contour de la main 74
1-4 La reconnaissance vocale 76
2°) La biométrie multimodale 77
Section 2- Les différents usages de la biométrie 79
A. Les usages de sûreté publique ou la « biométrisation de l'identité » 79
1°) La sécurisation des papiers d'identité 79
2°) La sécurisation biométrique des flux migratoires 83
3°) La sécurisation des élections 86
4°) Le marché de la sûreté aéroportuaire 88
B. Les usages de « sécurité de confort » 89
1°) Le marché du contrôle d'accès logique 89
2°) La sécurisation des paiements 91
2-1 La sécurisation des versements de pensions et salaires 91
2-2 La sécurisation des paiements par carte bancaire 92
3°) Les autres utilisations de la biométrie 94
Section 3- Les défaillances potentielles des outils biométriques et les éventuelles conséquences sur la protection des données personnelles 98
A. L'influence du facteur humain sur la fiabilité des systèmes biométriques 98
B. L'influence du facteur statistique sur la fiabilité des systèmes biométriques 101

Chapitre 1- La sujétion du traitement au principe de finalité 104
Section 1- Les procédures de création des dispositifs biométriques en entreprise 108
Sous section 1 : Le contrôle a priori de la CNIL sur les traitements de données biométriques 109
A. Les formalités de déclaration préalable à l'installation de dispositifs biométriques 110
B. La notification et les délais de réponse de la commission nationale de l'informatique et des libertés 113
C. Transfert de données biométriques hors Union Européenne dans le cadre

de la procédure d'autorisation préalable 114
1°) Principe 114
2°) Exceptions 116
2-1 Les clauses contractuelles types 117
2-2 Les règles contraignantes d'entreprise 119
Sous section 2- La déclaration de conformité de l'usage de certains dispositifs biométriques 121
Section 2- L'intégration des finalités d'authentification et d'identification biométrique en entreprise 124
Sous section 1- La finalité d'authentification biométrique intégrée à l'entreprise 126
A. La spécification insuffisante des finalités au regard de la technique de reconnaissance par empreinte digitale 127
1°) La finalité de gestion des horaires 128
1-1 Le contrôle des horaires face aux libertés individuelles 130
1-2 Le contrôle des horaires biométrique sur support individuel évincé par l'éthique 134
a- Le principe du support individuel 134
b- Le jugement du TGI de Paris 136
c- L'autorisation postérieure accordée à la société Brisach 139
2°) La finalité de gestion du contrôle d'accès 143
2-1 Une finalité de contrôle d'accès associée à un processus sécurisé 143
2-2 La finalité du contrôle d'accès en expansion 146
B. L'appréciation de la finalité au regard des autres techniques de reconnaissance biométrique 148
1°) Au regard de la technique de la reconnaissance du contour de la main 148
1-1 Les finalités de contrôle d'accès, de gestion des horaires et de la restauration sur le lieu de travail 149
1-2 La finalité de contrôle d'accès des clients de l'entreprise 152
2°) Au regard de la technique de reconnaissance du réseau veineux des doigts de la main 153
3°) Au regard des autres techniques 155

Sous section 2- La finalité d'identification biométrique avec constitution de bases de données 156
A. La constitution de bases de données d'empreintes digitales 157
1°)- L'enjeu majeur de la protection de l'intégrité physique des personnes 160
2°) - L'enjeu majeur de la protection des biens et des installations 164
3°) - L'enjeu majeur de la protection des informations 167
4°) - L'enjeu majeur des missions de recherche scientifique 168
B. La constitution de bases de données issues d'autres techniques biométriques 172
1°) - La technique de reconnaissance de la voix 174
2°) - La technique de reconnaissance du réseau veineux des doigts de la main 177
Sous section 3 - Les sanctions du détournement de la finalité du traitement de données biométriques 180

Chapitre 2- La sujétion du traitement des données biométriques au principe de proportionnalité 185
Section 1 : L'appréciation de la balance des intérêts collectifs en entreprise 189
A. La qualité des données appréciée au regard du principe de proportionnalité 191
1°) Données adéquates, pertinentes et non excessives 192
2°) Le traitement ultérieur compatible des données 193
B. Les critères de « pondération » des intérêts de l'entreprise 195
1°) L'usage nécessaire de techniques biométriques dans l'entreprise 196
2°) La fiabilité du système envisagé 198
3°) L'usage raisonnable du dispositif biométrique au regard des finalités du traitement 199
Section 2- La prise en compte de la traçabilité de la technologie biométrique 201
A. Les dispositifs de reconnaissance par empreintes digitales remis en cause par le principe de proportionnalité 202
1°) Le fort impératif de sécurité mis à mal par le principe de proportionnalité 203
2°) Le mode de stockage mis à l'épreuve par principe de proportionnalité 208
2-1 Les éléments de réponse sur le plan national 209
2-2 Les éléments de réponse en droit comparé 215
B. Les techniques biométriques « sans traces » proportionnelles 217
1°) Le dispositif de reconnaissance du contour de la main 217

2°) Reconnaissance du réseau veineux des doigts de la main 221
2-1 La traçabilité de la technologie 222
2-2 Le contenu des données collectées 223
2-3 La proportionnalité du dispositif quant au mode de stockage 224
3°) Reconnaissance vocale 227

CONCLUSION TITRE I 231

TITRE II –Le contrôle individuel de l'usage de la biométrie entreprise 236

Chapitre 1- Les obligations d'information et de consultation des salariés dans l'environnement biométrique 239
Section 1 : L'information loyale des salariés 242
A. Les obligations et les sanctions des garants de l'information des salariés 243
1°) Le statut de responsable de traitement 243
1-1- Les Missions du responsable de traitement 244
1-2- La faculté de délégation de certains traitements au Correspondant informatique et libertés 246
2°) Les manquements sujets à sanctions 250
2-1 La procédure normale 251
2-2 La procédure d'urgence 252
2-3 La procédure juridictionnelle 254
B. Le renforcement légal de l'obligation d'information 255
1°) L'information des salariés 256
1-1 L'information loyale des salariés 256
1-2 La transmission de l'information 258
2°) Le contenu de l'obligation d'information 260
2-1- L'information nécessaire mais aléatoire sur l'interconnexion des fichiers 262
a- L'information des salariés 263
b- L'information de la CNIL 264
2-2- La carence de l'information sur la durée de conservation des données biométriques 267

Section 2- La consultation des représentants des salariés 270
A- Les modalités d'information et de consultation des représentants des salariés 272
1°) La consultation du Comité d'entreprise 272
1-1 La présentation d'un projet 274
1-2 Les caractères du projet 275
2°) La consultation du CHSCT 277
3°) L'intervention facultative de l'expert en technologie 278
B- La nature purement consultative de l'avis 279

Chapitre 2 – L'exercice du consentement et des « droits actifs » des salariés 282
Section 1- La manifestation de la volonté du salarié dans l'environnement biométrique 284
A. Le consentement express biométrique 285
1°) Le consentement comme condition de licéité du traitement de données biométriques 285
1-1 Les conditions de fond 285
1-2 Les conditions de forme 288
2°) Les réserves quant à l'exercice d'un consentement exprès 290
B. La faculté d'opposition du salarié à la collecte des données biométriques 294
Section 2 – Le droit de regard du salarié sur le traitement de ses données biométriques 297
A. Le principe de libre accès aux données personnelles biométriques 298
1°) L'accès et la communication aux données biométriques 299
1-1 L'exercice du droit d'accès et de communication 299
a- Le contenu du droit d'accès et de communication 299
b- Les formalités associées au droit d'accès 302
1-2 Le droit d'accès indirect 305
2°) Les exceptions à l'exercice du droit d'accès 307
B. La matérialisation du droit à rectification sur les données biométriques 310

CONCLUSION GENERALE 313

ANNEXES 321

BIBLIOGRAPHIE **361**
INDEX **386**
TABLE DES MATIERES **389**

Vu et permis d'imprimer

Montpellier, le .....

Le Président de l'Université Montpellier I

Philippe AUGE

Résumé en français :

La biométrie regroupe l'ensemble des techniques informatiques qui permettent de reconnaître un individu sur ses caractères biologiques, physiques ou comportementaux. D'abord réservée au domaine judiciaire, elle se démocratise dans toutes les sphères de la vie des individus. Depuis quelque temps, la biométrie est employée dans les entreprises toujours réceptives aux nouvelles technologies. Ainsi, l'insertion de tels dispositifs en entreprise doit faire l'objet d'un dialogue social entre le chef d'entreprise et les représentants du personnel car il s'agit d'une technologie dite de surveillance, souvent comparée à la vidéosurveillance, aux puces RFID, aux données GPS et peut aboutir à l'espionnage des salariés s'ils ne sont pas encadrés. A défaut de législation spécifique, le législateur a confié à la CNIL le soin d'établir les critères d'admissibilité de cette technologie au sein des entreprises. La législation Informatique et libertés se mêle alors à celle du droit du travail, pour faire appliquer des principes communs tels la finalité, la proportionnalité, la loyauté, la transparence de l'information et le consentement des salariés.

Titre et résumé en anglais : The treatments of biometric data in company

Biometry brings together computing techniques that enable the identification of individuals on the basis of their biological, physical appearance and/or behavioral characteristics.

Although firstly reserved for the legal system/judiciary domain, biometry tends to be generalized in all spheres of people life. Recently, biometry has also been used in companies who are always receptive to new technologies.

Thus, the introduction of identifying devices such as these into a company life has to be the subject of corporate discussions between the managing teams and staff representatives. Indeed, such technologies are often compared to video surveillance, RFID chips, GPS data … and they can lead to the spying of employees if their uses are not well supervised. In the absence of specific laws, the legislator has given the CNIL the abilities to establish the requirements of eligibility of this technology usage within the companies. The "liberty and computing" legislation is then combined with the labor laws in order to apply common principles such as the finality, the proportionality, the loyalty, the transparency of information and employee consents.

Discipline :

DROIT PRIVE ET SCIENCES CRIMINELLES

Mots-clés :

Dispositifs biométriques – Authentification – Identification – Données personnelles – Finalité – Proportionnalité – Contrat de travail – Salariés – Dialogue social – Information loyale – Consentement – Droits d'accès et de rectification – CNIL – Responsable de traitement – Traçabilité – Droit comparé

Intitulé et adresse de l'U.F.R. ou du Laboratoire :

ERCIM, UMR 5815 Dynamique du droit – Faculté de droit, UFR Droit – 39, rue de l'Université – 34060 Montpellier cedex 2.