– PANTHÉON - SORBONNE –
UNIVERSITÉ PARIS 1

MASTER 2 Professionnel DROIT DE L'INTERNET PUBLIC

Continuation du programme d'enseignement du DESS Droit de l'internet – Administration – Entreprises

Identification biométrique, protection des données et droits de l'homme

Mémoire soutenu par Jean-Baptiste Thomas-Sertillanges
en vue de l'obtention du Master

Session de Septembre 2007

Président du jury …….....M. Georges CHATILLON,
Directeur du Master Droit de l'Internet Public

Directeur de Mémoire …….....M. Herbert MAISL,
Conseiller d'État

- PLAN -

INTRODUCTION....4
TITRE I. IDENTIFICATION BIOMETRIQUE : POTENTIALITES ET RISQUES JURIDIQUES....8
CHAPITRE 1. Technologies biométriques : vers une identité intelligente ?....9
SECTION 1. L'identification biométrique au service de la sécurité juridique....9
SOUS-SECTION 1. La rationalisation de la preuve de l'identité....9
§1. Procédures traditionnelles d'identification....9
§2. Principes et techniques de l'identification biométrique....14
SOUS-SECTION 2. Une sécurité renforcée ou de nouvelles vulnérabilités ?....16
§1. Un progrès de sécurité dans l'absolu....16
§2. De nouvelles vulnérabilités....20
SECTION 2. Applications actuelles de la biométrie....23
SOUS-SECTION 1. Applications de la biométrie en France....23
§1. Fichiers de police....23
§2. Contrôle des frontières....27
SOUS-SECTION 2. Coopération européenne et internationale....29
§1. Systèmes et fichiers biométriques européens....29
§2. Relations avec les États-Unis....31
CHAPITRE 2. Risques de la biométrie au regard des droits de l'homme....34
SECTION 1. Identification biométrique et protection de la vie privée....34
SOUS-SECTION 1. Un méta-système d'identification....34
§1. Identifiants universels et interconnexion....34
§2. L'évolution du risque : les enjeux de l'interopérabilité....38
SOUS-SECTION 2. Une infrastructure de surveillance....42
§1. Traçage biométrique et surveillance des déplacements....42
§2. Un embryon de « biopouvoir »....45
SECTION 2. Risques au regard des autres droits de l'homme....48
SOUS-SECTION 1. La protection de la personne humaine....48
§1. L'intégrité du corps humain....48
§2. La dignité de la personne humaine....51
§3. La protection de l'identité humaine....53
SOUS-SECTION 2. Le droit à un procès équitable....55
§1. Présomptions de fiabilité et automatisme probatoire ?....56
§2. Portée et limites des gardes fous existants....58
TITRE II. LE REGIME JURIDIQUE DE L'IDENTIFICATION BIOMETRIQUE : EFFICACITE ET LIMITES....61
CHAPITRE 1. Droit positif des dispositifs et des données biométriques....62
SECTION 1. Conditions de licéité du traitement et protection des données....62
SOUS-SECTION 1. Conditions de licéité du traitement....62
§1. Formalités préalables....62
§2. Contrôle de proportionnalité par la CNIL....67
SOUS-SECTION 2. Protection des données biométriques....70
§1. Qualification des données....70
§2. La protection des données biométriques selon la CNIL....75
SECTION 2. Droits des personnes concernées et obligations des responsables du traitement....79
SOUS-SECTION 1. Droits des personnes concernées....79
§1. Droits relatifs à la collecte et au traitement....79
§2. Droits relatifs aux données....80
SOUS-SECTION 2. Obligations des responsables....81
§1. Devoir de loyauté....81
§2. Obligation de sécurité....83
CHAPITRE 2. L'évolution du droit des dispositifs et des données biométriques....85
SECTION 1. Uniformisation, harmonisation ou consolidation ?....85
SOUS-SECTION 1. La convergence des doctrines....86
§1. La convergence des doctrines nationales....86
§2. La convergence des recommandations des autorités supranationales....88
SOUS-SECTION 2. Les tentatives de consolidation....90
§1. Guides et codes de bonne conduite....90
§2. Exemples de consolidations législatives....92
SECTION 2. La signature biométrique, une technologie au renfort de la vie privée ?....95
SOUS-SECTION 1. Un protocole d'identification associant biométrie et cryptographie....95
§1. Principes techniques....95
§2. Étude de cas....97
SOUS-SECTION 2.La résolution de l'antinomie sécurité contre vie privée....98
§1. Évaluation technique....98
§2. Appréciation juridique....99
BIBLIOGRAPHIE....102
ANNEXES....107

- REMERCIEMENTS –

Je souhaite remercier M. CHATILLON,
pour m'avoir permis de suivre cette formation
et pour m'avoir communiqué sa passion pour le droit du numérique.

Je souhaite également remercier M. MAISL,
pour avoir dirigé mes travaux avec intérêt.

Je souhaite enfin remercier ma Mère,
qui m'a appris à parler,
et mon Père,
qui m'a appris à écrire.

« *Cela a posé quelques problèmes techniques pour y fixer les aiguilles, mais après de nombreux essais, on y est arrivé. Eh oui, nous n'avons pas craint de nous donner du mal. Et chacun désormais peut voir, à travers le verre, l'inscription s'exécuter dans le corps. Vous ne voulez pas vous approcher pour regarder les aiguilles ?* »

Franz Kafka, *Dans la colonie pénitentiaire*, 1919

« *La preuve biologique scientifique est une caractéristique imparfaite de la personne humaine et de ses relations sociales et affectives, que seule la vérité juridique, libérée du poids du réalisme biologique est en mesure d'exprimer.* »

Première Chambre civile de la Cour de Cassation
Arrêt du 3 juin 1998

- INTRODUCTION -

1. Sortir d'un débat manichéen

Bien qu'il ne s'agisse pas d'une discipline nouvelle, la biométrie est sur le point de faire une entrée fracassante dans notre vie quotidienne. Dans un contexte international sécuritaire, l'association de l'anthropométrie à l'informatique a ouvert aux gouvernements et aux industriels d'immenses perspectives.

Un des premiers signes de cette évolution s'est manifesté aux États-Unis, dans le cadre du programme d'exemption de visa des visiteurs étrangers. Dans certains aéroports, les autorités américaines procèdent à un relevé des empreintes digitales et à une photographie du visage des voyageurs.

De nombreuses questions résonnent alors dans la tête du citoyen averti. Que deviennent ces données ? Quelle est la légitimité de ce processus ? Le relevé des empreintes digitales n'est-il pas cantonné à l'identification judiciaire ? La suspicion de principe va-t-elle être généralisée ? La question de la lutte contre le terrorisme suffit-elle à justifier le recours à de telles pratiques ? Il faut rappeler que les avions qui se sont écrasés sur les deux tours le 11 septembre étaient partis de Boston ou Washington et non de l'étranger, et qu'en conséquence, le danger venait moins de l'extérieur que de l'intérieur.

L'intuition du citoyen souffle alors à l'oreille du juriste que l'usage de la biométrie recèle des trésors d'ambiguïtés, sur ses finalités avouées ou inavouées, ses limites techniques ou organisationnelles, ses conséquences sociales et politiques, ses risques au regard des droits de l'homme et en particulier de la vie privée. C'est alors au droit de tenter de lever ces incertitudes.

Depuis quelques années, une *intelligentsia* mondiale s'est férocement engagée pour contrer la véritable croisade menée par les industriels et les États du monde entier en faveur de la biométrie. La nature du juriste ne l'incitant traditionnellement pas à prendre pour parole d'évangile l'argumentaire des acteurs économiques et encore moins les justifications gouvernementales restreignant les libertés des citoyens, il n'apparaît pas anormal que nombre d'entre eux se rangent aux côtés des défenseurs des droits de l'homme et des pourfendeurs de l'État omniscient. D'autant que l'introduction de la biométrie se fait dans une certaine forme d'opacité, qui pourrait justifier une opposition de principe.

Cependant, de la même manière que l'argument sécuritaire de l'État ou le lobby des industriels ne suffit par à emporter la conviction du juriste, les cris d'alarmes de la société civile, aussi légitimes soient-ils, ne sont pas toujours fondés sur une démonstration rigoureuse. Il s'agit essentiellement de dénoncer « Big Brother » agité comme un épouvantail. Or, c'est précisément la méthode retenue par les gouvernements, agitant eux-mêmes le spectre du « Terrorisme ».

Dans cette opposition frontale, nul doute que les seconds aient le dernier mot, la majorité des citoyens semblant davantage s'inquiéter des questions de sécurité que des questions de libertés individuelles.

La sérénité et l'efficacité du débat s'en trouvent fortement dégradées, au point que l'on puisse croire que les intérêts en cause soient forcément antinomiques. C'est donc dans un effort d'objectivité et de réalisme, éclairé par les nombreux travaux existants, que ce mémoire tentera d'aider ses lecteurs à prendre position, celle-ci ne pouvant être que provisoire.

2. Définir la biométrie

Dans de nombreuses situations, l'exercice de droits suppose d'apporter la preuve que ces droits sont bien attachés à la personne qui s'en prévaut. M. Georges CHATILLON posait ainsi en 2003 le problème des outils et des procédures d'identification et d'authentification[1] pour l'efficacité de l'administration électronique. Ces procédures passent généralement par la preuve de son état civil, la détention d'un titre, la connaissance d'un code ou d'un mot de passe. Ainsi :

• Le droit de conduire s'exerce par la possession d'un permis de conduire ;
• le droit de vote s'exerce par la détention d'une carte d'électeur et d'une pièce identité ;
• le droit d'accéder à son compte de messagerie suppose un identifiant et un mot de passe ;
• le droit de pénétrer une zone sécurisée s'exerce par la possession d'un badge magnétique ;
• le droit d'accéder à son immeuble suppose la connaissance d'un code d'entrée ;
• le droit de retirer de l'argent à un distributeur nécessite une carte et la connaissance du code ;
• le droit d'utiliser son téléphone portable suppose d'en connaître le code ;
• le droit de prendre le métro ou le train suppose la détention d'un titre de transport validé ;
• le droit d'emprunter un livre à la bibliothèque suppose la détention d'une carte d'abonné ;
• le droit de se présenter à un examen suppose de présenter sa carte d'étudiant.

On peut ainsi multiplier les exemples à l'infini. Par exception et dans les intérêts du commerce, certaines créances bénéficient de facilités légales de transmission. Ainsi, les droits attachés à une lettre de change peuvent être transmis sur simple endossement, sans preuve de l'identité. Seule la signature est en jeu, et donc une identité qui n'est que très faiblement présumée, et qui ne bénéficie d'aucune autre mesure de sécurité que de l'encre sur du papier.

Au final, selon l'étendue du risque de fraude, et la souplesse que l'on souhaite accorder à la procédure, celle-ci sera plus ou moins formalisée, plus ou moins stricte. Ce formalisme constitue à la fois la contrepartie de l'exercice d'une liberté et la garantie de cet exercice, puisqu'il sert aussi à empêcher que l'un ne s'arroge les droits d'un autre.

Les moyens informatiques d'aujourd'hui ne peuvent cependant pas garantir les titulaires de droits contre toute forme d'atteinte, d'usurpation d'identité, de divulgations. Au contraire, ils les facilitent.

C'est à ce stade que la biométrie entre en jeu. Elle est présentée par ses défenseurs comme un moyen de sécuriser le processus d'identification, et par conséquent, l'exercice de droits.

Elle pourrait même aller très loin puisque le droit d'usage d'un produit de propriété intellectuelle (un CD, un DVD) pourrait à terme requérir l'identification biométrique du consommateur pour lutter contre le piratage et limiter la copie privée[2] …

---

[1] Georges CHATILLON, *Simplification, efficacité, bon fonctionnement bon rendement de l'administration électronique, l'expérience française,* Kuwait Conference On Electronic Government 2003. « *Dans les relations entre tout usager et les administrations pour l'application d'une décision individuelle ou la mise en œuvre d'un droit se pose invariablement et ab initio, la question de l'identification du demandeur. Selon le caractère plus ou moins sensible de la demande, l'agent public peut se contenter de l'information alléguée par la personne (identification) ou être amené à vérifier ces informations à l'aide d'un référentiel (papier d'identité, quittance, bulletins de paie)* » http://www.georges-chatillon.eu/spip.php?article51

[2] Institute for Prospective Technological Studies (European Commission Joint Research Center), *Biometrics at the Frontiers : Assessing the impact on Society*, 2005. « *Biometrics might be useful for digital rights management (DRM) to replace code and/or password protected files*»
http://europa.eu.int/comm/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf

Pour la CNIL, 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 »*[3].

Cette définition large recouvre finalement la notion d'anthropométrie et appelle à plusieurs compléments, qui permettent de distinguer les deux disciplines. D'abord, la biométrie implique un traitement automatisé. Ainsi, l'International Biometric Group propose une définition reprise par l'OCDE[4]. Il s'agit de « *l'exploitation automatisée de caractéristiques physiologique ou comportementale pour déterminer ou vérifier l'identité* », définition qui consacre l'incorporation de l'informatique par une discipline millénaire[5].

3. Démystifier la biométrie au regard du droit

Pour beaucoup, la biométrie est le moyen le plus efficace de sécuriser l'identification des individus, et donc de lutter contre la fraude, le crime organisé, le terrorisme, l'immigration clandestine... La variété des applications potentielles de la biométrie laisse présager d'une banalisation sans doute inéluctable.

Les risques qui pèsent sur l'usage de la biométrie sont souvent exprimés en termes généraux et abstraits[6]. Cependant, la délimitation de ces risques et leur portée au regard de la pratique ne sont discernables qu'au prix d'une démystification méthodique de cette technologie au regard du droit.

Le juriste en droit des technologies a en effet la tâche difficile de devoir se plonger au cœur de la technique, pour évaluer en termes juridiques l'impact de ces nouveaux outils sur les rapports de droit. Il s'agit d'un travail de liaison, de connexion, de dialogue perpétuel entre la science et le droit. Il suppose d'aller à la rencontre d'un domaine, d'un état d'esprit et d'un langage, qui ne sont originellement pas les siens, d'en vulgariser certains aspects pour lui-même et pour les autres, avec toutes les limites que l'exercice suppose.

Pour illustrer cette idée, ce mémoire tentera notamment d'expliquer :

pourquoi l'utilisation d'un gabarit n'emporte pas les mêmes effets que l'utilisation d'une donnée biométrique brute ;

pourquoi le stockage des données biométriques dans une base de donnée n'implique pas les mêmes conséquences qu'un enregistrement sur une carte à puce ;

pourquoi le simple chiffrement des données biométriques n'ouvre pas les mêmes perspectives que la cryptologie biométrique ;

pourquoi le risque d'interconnexions de fichiers biométriques n'existe qu'en raison du mouvement

---

[3] CNIL, Document de travail sur la biométrie, 1er juin 2005
http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/LA_BIOMETRIEmai2005.pdf

[4] Organisation de Coopération et de Développement Economiques, Direction de la science, de la technologie et de l'industrie, Comite de la politique de l'information, de l'informatique, et des communications, Groupe de travail sur la sécurité de l'information et la vie privée, *Technologies Fondées Sur La Biométrie*, 10 juin 2005.
http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00186151.PDF

[5] L'empreinte du pouce servait déjà de signature lors d'échanges commerciaux à Babylone (-3000 av. JC) et dans la chine antique (7ème siècle)

[6] Ainsi, dans un avis n° 98 du 7 juillet 2007, « Biométrie, données identifiantes et droits de l'homme » le Comité Consultatif National d'Éthique résume parfaitement les grands enjeux que soulève la généralisation de la biométrie. http://www.ccne-ethique.fr/francais/pdf/avis098.pdf

général d'interopérabilité qui s'annonce ;

pourquoi la biométrie ne remet pas en cause l'intégrité du corps humain, tant que celui-ci ne fait pas l'objet d'une redéfinition du fait des bouleversements informatiques ;

pourquoi l'identification biométrique constitue un pas de plus en direction de l'automatisme probatoire, alors même que la biométrie ne repose que sur des calculs de probabilité ;

pourquoi l'usage de l'empreinte palmaire à l'école comporte moins de risques que l'usage d'empreintes digitales ;

On voit ici que les modalités techniques d'utilisation de la biométrie, jusqu'au paramétrage et à la configuration du système, sont susceptibles d'être analysées différemment au regard de la vie privée.

La biométrie constitue-t-elle par essence une menace pour les libertés individuelles et pour les droits de l'homme ? Peut-elle être considérée comme la contrepartie à l'exercice des certaines libertés ? Les conditions de sa généralisation imminente sont-elles satisfaisantes ? Le cadre juridique actuel permet-il d'en prévenir les effets néfastes ? Faut-il espérer une uniformatisation du droit des dispositifs biométriques ? Est-il temps de se pencher sur les « *privacy enhancing technologies* » ou technologies renforçant la vie privée ?

Voilà quelques-unes des questions auxquelles ce mémoire tentera d'apporter des éléments de réponse, toute conclusion définitive dans ce domaine étant à proscrire.

Une première partie sera consacrée aux risques et aux potentialités de l'identification biométrique, qui se pose à la fois comme un outil au service de la sécurité – sécurité des systèmes d'information, sécurité juridique, sécurité publique - et comme un risque au regard de la protection de la vie privée et des droits de l'homme en général.

Une seconde partie sera consacrée à l'étude du droit des données et des dispositifs biométriques, son efficacité, ses limites, et ses perspectives d'évolution au regard des droits étrangers et des recherches scientifiques.

TITRE PREMIER

IDENTIFICATION BIOMÉTRIQUE
POTENTIALITÉS ET RISQUES JURIDIQUES

Chapitre I
TECHNOLOGIES BIOMETRIQUES, VERS UNE IDENTITE INTELLIGENTE ?

Les technologies biométriques ont aujourd'hui pour domaine de prédilection l'identification des personnes. À ce titre, la généralisation manifestement inévitable de la biométrie constitue l'étape ultime de rationalisation de l'identification, en tant que technique probatoire.

Cette nouvelle méthode d'identification, marquée d'un perfectionnisme certain, n'est ainsi pas cantonnée au renforcement des mesures de sécurité, mais constitue, au même titre que la signature électronique, une technique pouvant renforcer la sécurité juridique. C'est ainsi que la mission d'information de la commission des lois considère que la biométrie, constitue un pas vers « *l'identité intelligente* »[7]. Avant d'étudier les applications actuelles de la biométrie et d'évoquer les règles qui leur sont applicables, il convient d'étudier la biométrie en tant que méthode d'identification.

SECTION 1. L'identification biométrique au service de la sécurité juridique

La biométrie pourrait devenir une technique centrale au regard du droit. Ses qualités techniques alléguées risquent de la rendre indissociable de la notion d'identification. Or, la preuve de l'identité est souvent au cœur des rapports de droit entre les individus et entre les individus et les États. Nous verrons donc dans une première sous-section en quoi la biométrie constitue une petite révolution au regard de l'identification traditionnelle. Dans un second temps, on s'attachera à relever quels sont les nouveaux risques techniques inhérents à cette technologie.

SOUS-SECTION 1. La rationalisation de la preuve de l'identité

§ 1. Procèdures traditionnelles d'identification

• *Finalités de l'identification*

Quelle est l'utilité de pouvoir distinguer un individu de ses semblables ? Peut-on imaginer une société d'individus anonymes ?

L'identité, source de droit. - L'identité[8] se définit comme « *l'ensemble des composantes grâce auxquelles il est établi qu'une personne est bien celle que se dit ou que l'on présume comme telle* »[9]. Il s'agit donc d'éléments connus qui permettent de distinguer une personne de ses semblables. En droit, l'ensemble de ces éléments distinctifs est essentiellement fixé par l'état civil, c'est-à-dire *« la situation d'une personne en droit privé telle qu'elle résulte des éléments pris en considération par le droit en vue de lui accorder des prérogatives juridiques*[10] ».

---

[7] Jean-René LECERF, Identité intelligente et respect des libertés, Sénat, Rapport d'information du Sénat n° 439 (2004-2005) déposé le 29 juin 2005), fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) par la mission d'information (2) sur la nouvelle génération de documents d'identité et la fraude documentaire. http://www.senat.fr/rap/r04-439/r04-4391.pdf

[8] Le mot identité vient (XIVe) du bas latin *identitas*, « qualité de ce qui est le même »

[9] Définition du lexique des termes juridiques 13ème édition, DALLOZ

[10] Définition du lexique des termes juridiques 13ème édition, DALLOZ

Aux termes de cette définition, l'identité est donc attachée à certaines prérogatives juridiques. L'identification serait alors le processus par lequel une personne apporte la preuve de son identité pour pouvoir exercer des droits[11]. Pourquoi, en pratique, les droits seraient-ils attachés à l'identité d'une personne ? Pourquoi ne pourrait-on pas se prévaloir de droits simplement en tant qu'être humain non identifié ?

L'homme anonyme, titulaire de droits naturels. - En 1776, la colonie de Virginie en se détachant de la Grande-Bretagne se dote d'une Constitution qui affirme que « *Tous les hommes sont nés également libres et indépendants ; ils ont des droits certains, fondamentaux et naturels, dont ils ne peuvent par aucun contrat priver ni dépouiller leur postérité ; tels sont le droit de jouir de la vie et de la liberté, avec les moyens d'acquérir et de posséder des propriétés, de chercher et d'obtenir le bonheur et la sûreté.* ». Cette conception, qui attache fondamentalement des droits à la personne humaine, a ensuite été au cœur du développement des démocraties occidentales. En cela, l'individu non identifié est en principe titulaire de droits, dès sa naissance.

Reconnaissance de droits naturels et nécessité d'un contrat social. - Ces droits resteraient à l'état de vœux pieux, de simples assertions animées d'un esprit humaniste, s'il n'existait pas de règles pour les mettre en œuvre. Les droits subjectifs se heurtent à la réalité des rapports sociaux, où l'exercice de droits par les uns est confronté à l'exercice de droits par les autres.

En réalité, ces droits n'ont d'effet que lorsque qu'ils sont consacrés, sanctionnés, régulés, organisés par une autorité légitime, à défaut de laquelle ils n'ont qu'une existence théorique et abstraite. Le premier outil de reconnaissance des droits pourrait donc être le « contrat social » en tant que fiction conceptuelle, créateur de droits et obligations, à la fois entre les individus et entre les individus et un « Léviathan[12] ».

La personnalité juridique, condition d'exercice de droits subjectif. - Le second outil fondamental de l'exercice effectif de droits subjectif est la personnalité juridique, c'est-à-dire « *la qualité de celui qui est titulaire de droits et obligations, et qui de ce fait a un rôle dans l'activité juridique*[13] ».

En France, la personnalité juridique est octroyée par l'État[14] dès la naissance, la naissance devant être constatée dans les trois jours par un officier d'état civil[15], à défaut de quoi l'embryon, l'enfant simplement conçu, ou le fœtus, ne bénéficient pas de la protection juridique des personnes humaines.

L'existence et l'effectivité de droits dépendent donc de l'existence d'une autorité supérieure qui les garantit dans l'absolu et de l'octroi de la personnalité juridique par cette autorité, qui engage implicitement les individus au contrat social. Cela explique dans un premier temps pourquoi le seul

---

[11] Cette définition serait cependant incomplète si on ne prenait en compte l'identification judiciaire, qui a souvent lieu sans la participation de l'intéressé. C'est alors un tiers qui vient apporter la preuve de l'identité d'une personne, identité devient alors source d'obligations pour l'intéressé.

[12] Thomas HOBBES, *le Léviathan, ou Traité de la matière, de la forme et du pouvoir d'une république ecclésiastique et civile*, 1651.

[13] Définition du lexique des termes juridiques 13ème édition, DALLOZ

[14] Au XXème siècle, sous le Code Napoléon, la personnalité juridique pouvait être légalement éteinte, on parlait alors de « *mort civile* ». Cette extinction emportait une privation générale des droits civique et politique. La personne est réputée ne plus exister, bien qu'elle soit vivante physiquement. Elle perdait le droit d'agir en justice, de reconnaître ses enfants naturels, d'être tuteur, de faire ou de recevoir des libéralités. Sa succession était immédiatement ouverte, ses biens lui étaient enlevés pour être aussitôt attribués à ses enfants, son testament annulé, son mariage était dissous, il ne pouvait plus être ni électeur, ni candidat, ni fonctionnaire, ni juré, ni expert, ni témoin.

[15] Article 55 du Code civil.

statut d'être humain ne permet pas, en principe, d'exercer effectivement des droits. Cette reconnaissance passe par l'État, par l'octroi de la personnalité juridique, elle-même nécessitant l'identification.

L'identification, condition de l'exercice effectif des droits. - Cet archétype peut s'appliquer à la majorité des rapports d'obligation : il suffit de remplacer l'idée de contrat social par un contrat de travail, celle d'autorité supérieure par l'employeur, et celle de personnalité juridique par l'habilitation. Cependant, si les conditions du modèle qui vient d'être décrit sont nécessaires, elles sont insuffisantes pour assurer l'effectivité de l'exercice des droits.

En effet, la complexité des relations juridiques nécessite qu'on puisse établir qui est titulaire de quels droits, qui les a déjà exercés, qui ne peut plus les exercer, qui est débiteur de quelles obligations, qui n'est plus débiteur de telles obligations. Il s'agit d'appliquer à chaque sujet de droit un traitement « individuel » correspondant à sa situation juridique particulière.

Dans le cas des rapports de droit entre l'individu et l'État, l'identification a pour objet de permettre à l'État de garantir aux personnes légitimes l'exercice de ces droits, et d'exiger des débiteurs identifiés l'exécution des obligations à leur charge.

Ainsi, l'exercice du droit de vote requiert l'identification des individus pour éviter que certains votent à la place d'autres, ou votent plusieurs fois. C'est également vrai pour le contrat de mariage, qui nécessite l'identification[16] pour éviter qu'un même individu ne se marie plusieurs fois, en d'autres termes pour vérifier qu'un individu a le droit de se marier. C'est encore le cas pour une société d'assurance, proposant des contrats d'adhésion standardisés, qui aura besoin d'identifier les nombreux co-contractants avec lesquels elle doit traiter de manière individuelle.

L'identification, fondement de la personnalité juridique ? - La preuve de l'identité constitue donc en pratique la dernière étape nécessaire à l'exercice d'un droit. Au point qu'à défaut d'apporter la preuve de son identité, la personnalité juridique, et même l'existence du droit sont sans effet. Qui peut espérer pouvoir voter sans carte d'électeur et sans pièce d'identité ? En ce sens, la preuve de l'identité fait sortir la personnalité juridique de son abstraction et de son anonymat pour lui donner une portée concrète.

De sorte qu'on peut en conclure avec le sénateur Michel DREYFUS-SCHMIDT, que l'identité d'une personne est « *ce qui fonde l'existence de sa personnalité juridique* »[17]. Sans identité fixée et avérée, un individu n'a pas de personnalité juridique, ou à tout le moins, les moyens de la mettre en œuvre.

L'identification se situe donc au cœur de nombreuses relations juridiques et constitue un élément de la sécurité des relations de droit. Elle constitue certes une restriction de la liberté, en ce que l'exercice d'un droit nécessite la mise en œuvre d'un processus probatoire contraignant, mettant en jeu une autorité supérieure.

Mais elle est aussi un instrument garantissant l'exercice effectif de ces prérogatives, aussi bien dans la sphère privée que dans la sphère publique, autant pour les personnes physiques que morales. Reste à savoir quelle méthode retenir pour réaliser ce processus probatoire.

---

[16] Article 1er de la Loi n° 2006-1376 du 14 novembre 2006, article « *A la remise, pour chacun des futurs époux, des indications ou pièces suivantes (…) la justification de l'identité au moyen d'une pièce délivrée par une autorité publique* »

[17] Proposition de loi « *tendant à la pénalisation de l'usurpation d'identité numérique sur les réseaux informatiques* », annexe au procès-verbal de la séance du 4 juillet 2005, Sénat. http://www.senat.fr/leg/ppl04-452.html

• Méthodes de fixation de l'identité

L’information, fondement de l’identité. - Nous avons vu que l'identification a pour objet de faire le lien entre un individu et un ensemble de composants distinctifs, éventuellement associés à des droits. Ces composantes peuvent être dans un premier temps le nom, le prénom, la date et le lieu de naissance, la filiation …

L'identité est donc d’abord de l'information sur la personne. En l’absence d’information, l’identité est fragilisée, voire inexistante. Un nouveau-né acquiert un embryon d’identité à partir des informations disponibles sur ses parents, de la détermination du son sexe, de sa date et de son lieu de naissance, du choix d’un prénom. Ainsi, que dire de l’identité d’une personne « née sous X », atteinte d'amnésie, inconnue de tous, et sans papiers ?

Cette relative volatilité de l’identité se vérifie d’autant plus sur le réseau Internet, les informations sur les comportements d’un internaute pouvant au mieux être rattachées à une adresse I.P.

En soi, peu de choses sont susceptibles d'établir un lien fiable entre une personne et de l’information. Une personne peut *a priori* être le support de toute information relative à l’identité. L’identification par le nom peut être délicate en cas d’homonymie. Le sexe, la couleur de peau, même la taille, ne sont plus des éléments intangibles et ne sont plus forcément distinctifs. L’information est transposable d’un individu à un autre, de sorte que l’identification par l’information est par essence aléatoire. Ce n’est que par le jeu de conventions sociales qu’on lui donne un caractère plus ou moins intangible.

La fixation de l’information identifiante. - Il existe des moyens de greffer au corps du sujet le support physique contenant l’information. Dans le domaine de la « traçabilité animale », le tatouage, ou la boucle d'oreille sont des techniques fréquemment utilisées, ainsi que les puces RFID, déjà appliquées aux humains.

Pour les hommes, ce lien est traditionnellement matérialisé par un titre d’identité délivré par les services habilités, sans qu’il soit encore besoin de greffer ce titre au corps de l’individu. Ce titre contient les informations identifiantes. On présume que son détenteur, lorsqu'il correspond aux caractéristiques décrites (âge, photographie, taille, sexe), est identifiable au titre d'un faisceau d'indices concordants. C’est la méthode usuelle du contrôle d’identité. Pour pouvoir s’engager contractuellement, il arrive qu'on demande aussi un justificatif de domicile. Ce justificatif atteste du fait que l’on est identifié de manière stable, sous un certain nom et à une adresse déterminée, par autre un co-contractant comme une compagnie d'électricité ou de téléphone. Mais pour certains contrats, notamment la vente, l’état civil n’est pas nécessaire, tant que des facilités de paiement ne sont pas en jeu (chèque, carte de crédit).

Il s'agit donc là d'une chaîne de présomption qui repose sur la mutualisation de la vérification de l'identité par des parties à différents contrats et dont le premier maillon est la fixation de l’identité par l’État. Cette fixation de l’identité est aujourd’hui encore essentiellement déclarative, et repose donc fondamentale sur la confiance.

Ces chaînes de présomptions interagissent et forment un réseau d'identification sociale présentant une certaine sécurité juridique. Ainsi, chaque chaîne de présomption de l'identité peut être matérialisée par ce que l'on possède, mais aussi par ce que l'on sait, comme un mot de passe ou un code confidentiel. Ce code est attribué de manière confidentielle par une banque, qui se sera elle-même assuré de l'identité de la personne, permettant à un commerçant d'accorder un crédit, sans plus d'identification.

On le voit, ce réseau de certification sociale de l'identité est fondé sur des méthodologies et des appréciations subjectives qui n'offrent pas de garantie absolue. Parfois, elles sont simplifiées au maximum dans les intérêts de la liberté de commerce, à l'image des lettres de change, dont la simple détention confère des droits.

Ces méthodes permettent seulement de faire jouer un certain nombre de présomptions ou d'exposer un faisceau d'indices relatifs à l'identité d'une personne, indices apposés généralement sur un titre que l'on détient. Plus une personne noue de relations juridiques, plus les mailles du filet sont resserrées, de sorte que le changement d'identité, à un certain stade, devient presque impossible.

• Méthodes de preuve de l'identité

Postérieurement à la fixation de l'identité, un sujet de droit aura besoin d'apporter la preuve de son identité, c'est-à-dire du lien entre lui-même et une personne juridique titulaire de droit et obligations, pour de nombreux actes de la vie quotidienne.

Syllogisme. - La plupart du temps, la preuve de l'identité est demandée, directement ou indirectement, par le débiteur des obligations éventuellement représenté par un agent, personne physique ou programme informatique. L'agent procède à deux opérations : il vérifie d'abord le lien entre la personne qui se présente et l'identité déclarée, par exemple à partir d'une carte d'identité ; dans un second temps, il consulte un registre, au sein duquel une identité est associée à des prérogatives. Parfois le titre est lui-même porteur de droit, comme une carte d'accès à une bibliothèque. C'est donc grâce à un syllogisme douteux que l'exercice de droit s'effectue. Si M.X a des droits, que la personne qui se présente est bien M.X, alors cette personne a des droits.

Un processus soumis à l'aléa. - On voit que le processus de fixation de l'identité et le processus d'identification sont soumis à des aléas importants, voire recèlent de véritables carences. Au risque de mettre en cause la sécurité juridique, ils reposent encore beaucoup sur des procédures archaïques, fondées sur une interprétation subjective de la correspondance entre l'identité fixée et l'identité déclarée. Elles sont d'ailleurs souvent issues de la pratique et sources d'erreurs, de malentendus, de fraude … C'est en grande partie le diagnostic[18] de la mission d'information de la commission des lois, rendu dans son rapport « *Identité intelligente et respect des libertés* ».

Si l'on considère que le souci d'ordre et de perfection, facilité par les machines, apporte à l'homme davantage de bénéfices que d'inconvénients, la biométrie pourrait permettre de rationaliser ces procédures, en utilisant les données numériques du corps, indissociable de la personne, comme dénominateur commun entre une personne et des droits.

Cette ambition est encore plus exacerbée avec le développement d'Internet, qui a engendré un retour en force de l'anonymat, souvent considéré comme un risque au regard de la sécurité juridique et de la sécurité en général.

De la même manière que nous avons tenté de disséquer le processus général de la fixation de l'identité et de la vérification de l'identité, il est nécessaire d'examiner la biométrie, moins sous l'angle technique, que sous l'angle des procédures qu'elle met en oeuvre à travers la technique.

---

[18] Jean-René LECERF, Identité intelligente et respect des libertés, Sénat, Rapport d'information du Sénat n° 439 (2004-2005) déposé le 29 juin 2005), fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) par la mission d'information (2) sur la nouvelle génération de documents d'identité et la fraude documentaire. http://www.senat.fr/rap/r04-439/r04-4391.pdf

§ 2. Principes et techniques de l'identification biométrique

• *L'identification par l'informatisation du corps*

Chaque être humain possède des caractéristiques morphologiques et biologiques uniques, qui permettent de le distinguer de ses « semblables ». Ce processus d'identification est inconsciemment effectué par notre cerveau des dizaines de fois par jour, mesurant instinctivement position des yeux, taille du nez, forme du visage des personnes qui nous entourent.

La technologie biométrique repose sur le même principe, mais de façon logique, grâce à la puissance de calcul des ordinateurs. Le système d'identification biométrique conserve en mémoire certaines caractéristiques physiques d'une personne sous forme de données numériques, auxquelles sont comparées celles du « candidat » à l'identification. Lorsque ces données correspondent, le système la « reconnaît ».

On peut donc rapprocher ce système technique de ce qui a été évoqué précédemment. La collecte des données biométriques de référence - l'enrôlement - peut ainsi être assimilée à la fixation de l'identité et éventuellement des droits qui y sont attachés. Ensuite, la comparaison des données - l'appariement - peut être assimilée à l'identification, et donc à la preuve de la titularité de droits.

• *Enrôlement et appariement*

L'OCDE parle de dispositif ou de système biométrique pour désigner *« tout matériel, logiciel associé, microprogrammes, et composantes de réseau nécessaire à la totalité du processus d'enrôlement et d'appariement »*[19].

Procédure d'enrôlement. - Préalable à l'identification, l'enrôlement consiste en pratique à enregistrer les données biométriques de référence auxquelles seront comparées ultérieurement les données du candidat à l'identification. C'est donc une étape d'enregistrement.

Plus techniquement, il s'agit de prélever un échantillon biométrique, c'est-à-dire une donnée brute, comme une image numérisée de l'iris ou de l'empreinte digitale. Cette donnée brute donne ensuite lieu à un traitement informatique. Le programme sélectionne certains points clés pour créer un gabarit qui, par la suite, servira seul de référence. Ce gabarit peut être stocké dans une base de donnée ou sur support externe comme une clé USB. Cette identité biométrique de référence est associée par exemple au droit d'accès à une zone sécurisée, à un identifiant alphanumérique, ou même à l'état civil. En cela, il constitue l'élément technique de l'identité fixée par le système.

Procédure d'appariement. - Au moment de l'identification, on prélève un nouvel échantillon de la personne, une donnée brute qui fait l'objet du même traitement que le gabarit référence, c'est-à-dire un traitement qui repère les points clés de la donnée brute. C'est ensuite par comparaison entre un gabarit référence et le gabarit prélevé *ad hoc* que l'on peut vérifier l'identité d'une personne, lorsque les deux gabarits correspondent, ou lorsque les points clés d'une version partielle de l'empreinte digitale sont superposables.

---

[19] Organisation de Coopération et de Développement Economiques, Direction de la science, de la technologie et de l'industrie, Comite de la politique de l'information, de l'informatique, et des communications, Groupe de travail sur la sécurité de l'information et la vie privée « Technologies Fondées sur la biométrie », 10 juin 2005. http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00186151.PDF

• *Typologie des procédures biométriques*

L'identification au sens générique du terme peut se faire selon plusieurs méthodes dans le domaine de la biométrie. Chaque méthode emporte des conséquences et des risques différents en matière de vie privée et de libertés, c'est pourquoi il est intéressant de se pencher sur les procédures qu'elles mettent en œuvre.

Au préalable, il faut préciser que la typologie habituellement retenue est source de confusion. La création d'un « jargon biométrique » se superpose aux termes du langage courant et créé des néologismes inutiles. Par exemple, le terme d'identification, qui est la finalité générale des procédures biométriques, est utilisé en termes techniques pour désigner une seule de ces procédures, et de manière exclusive. De sorte « l'identification » désigne à la fois une finalité et un des moyens de répondre à cette finalité.

Identification. - La première technique, baptisée « identification » consiste à comparer les données d'une personne inconnue à une base de donnée. Lorsque le système fait apparaître une correspondance avec une donnée préalablement enregistrée, la personne est « identifiée », par distinction au sein d'un lot. Techniquement, cela suppose la constitution d'un fichier préalable c'est-à-dire d'une base de donnée.

Authentification. - D'une certaine manière, on peut comparer cette approche avec le couple « nom d'utilisateur » et « mot de passe ». Le nom d'utilisateur sert à alléguer une identité, le mot de passe sert à vérifier cette identité.

Dans le domaine biométrique, le candidat se prévaut dans un premier temps d'une identité, en soumettant au système les données biométriques de référence, souvent contenues dans une carte à puce. Ensuite, le candidat soumet pour comparaison ses données biométriques, en posant son doigt sur un capteur. Lorsqu'elles correspondent, l'identité alléguée est vérifiée, on parle alors d'« authentification ».

Nous reprendrons cependant autant que possible la nouvelle terminologie[20] du Groupe JS 37 de l'Organisation Internationale de Normalisation qui lui substitue le terme de « vérification »[21], ce dont on ne peut que se réjouir.

Filtrage. - La troisième catégorie de traitement est le filtrage, traduction approximative du « screening ». Il s'agit de la méthode traditionnelle de liste noire. Cette liste contient des données sur des individus à arrêter ou à exclure. Cette application est mise en oeuvre de manière non automatisée par les « physionomistes ». L'usage de la biométrie permet d'automatiser ce processus.

Chaque personne soumise à la procédure de filtrage fournit une donnée biométrique, qui est comparée aux données présentes dans la base de données. L'idée centrale est que toutes les personnes qui passent le test ne sont pas identifiées. Seulement certaines le seront par exception, si

---

[20] http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/JTC_1_SC_37_Agreed_Harmonized_Core_Biometric_Terms_and_Definitions.pdf?nodeid=5675848&vernum=0

[21] En effet, l'utilisation du terme « authentification » est sujette à caution. Ce terme n'est présent dans aucun dictionnaire de référence. Il s'agit d'une transposition du mot anglais « authentication », résultat d'une utilisation abusive y compris dans la langue d'origine. On ne peut authentifier une personne, mais seulement des données, des documents, des éléments d'identité. Or, il est douteux que l'authentification concerne le support de données biométriques. D'autres procédés traditionnels peuvent permettre de s'assurer du caractère officiel d'un document (absence d'azurants optiques, filigrane à deux tons, réactifs chimiques, fibres et impression fluorescentes sous exposition aux UV, fil de sécurité, coloration irisée, motif micro-imprimés, couleurs réactives ...). En soi, la biométrie n'apporte rien à l'authenticité du support ou des données. Ce qu'elle peut éventuellement authentifier, c'est le lien entre une personne et son titre ...

elles figurent au sein de la liste noire. S'il n'y a pas de correspondance dans la base de donnée, l'échantillon biométrique pris à la volée est en principe détruit. Si le système établit une correspondance, un agent décide des mesures à prendre.

C'est typiquement le cas du Système d'Information Schengen pour les contrôles aux frontières au niveau européen, qui contient les données biométriques des personnes recherchées ou faisant l'objet d'une mesure de privation de liberté.

C'est également le domaine de prédilection de la vidéo surveillance biométrique, qui a la particularité de soumettre les individus au test sans qu'ils en aient conscience. L'échantillon biométrique est collecté à la volée pour être comparé à ceux figurant dans une base. Les caractéristiques morphologiques de chaque individu sont analysées par le système, mais seules sont réellement identifiées les personnes présentes dans la base de donnée et faisant l'objet d'une recherche.

Conséquences au regard de la vie privée. - Certes fondée sur une terminologie bancale, cette typologie révèle pourtant une différence d'approche entre chaque procédure, qui n'est pas sans conséquences au regard de la vie privée, comme il sera expliqué dans les chapitres suivants.

Ainsi, l'identification et le filtrage requièrent la constitution d'une base de donnée, là où la vérification permet à l'intéressé de rester maître de ses données, conservées sur un support qui demeure en sa possession. Au final, le choix d'une fonction de vérification, d'identification, ou de filtrage dépend hautement de la finalité envisagée et des circonstances dans lesquelles le dispositif sera employé.

SOUS-SECTION 2. Une sécurité renforcée ou de nouvelles vulnérabilités ?

§ 1. Un progrès de sécurité, dans l'absolu

• *Comparatif des techniques de sécurisation de l'identification*

La vérification de l'identité passe généralement par trois formes, chacune présentant des avantages et des inconvénients de sécurité.

Ce que l'on sait. - Il s'agit en général d'un mot de passe, d'un code confidentiel, d'un *Personal Identification Number*[22]. Ce type de sécurité est utilisé pour l'accès à des services en ligne, à un immeuble, à une pièce ou une chambre d'hôtel, à l'utilisation d'une carte bancaire, à l'utilisation d'un téléphone portable ou d'un ordinateur, d'un réseau d'entreprise ou même à l'ouverture d'un attaché-case. Il est parfois associé à un pseudonyme, celui-ci servant d'identifiant. En terme de sécurité, la faille inhérente à ce système de vérification est aussi sa force. Un mot de passe peut être oublié, perdu, divulgué, subtilisé. En contrepartie, un mot de passe peut aussi être réinitialisé, dès que le secret est corrompu.

Ce que l'on possède. - Il s'agit habituellement d'un titre, d'une carte à puce, d'un badge magnétique, d'un document écrit. Le titre est souvent associé à un mot de passe comme pour la carte bancaire. La sécurité est ici plus forte, mais dépendante des techniques utilisées pour fabriquer la carte et de la qualité technique des programmes qui la compose en termes de sécurités. Dans le cas des cartes bancaires, la sécurité est essentiellement assurée par des procédés de cryptologie à clé

[22] Numéro personnel d'identification

publique, dont le piratage est devenu l'enjeu d'une compétition mondiale entre ingénieurs informatiques de tous âges et de toutes nationalités.

Ce que l'on est. - Il s'agit ici de la reconnaissance visuelle utilisée par exemple dans les relations personnelles, de voisinage, voire professionnelles, mais aussi pour l'identification judiciaire par les témoins oculaires et les physionomistes. Dans ce cas, l'appréciation humaine constitue un aléa trop important pour considérer la reconnaissance visuelle comme parfaitement probante. La sensibilité de l'œil humain pour distinguer les visages n'est pas encore surpassée par la machine, mais c'est ici la rapidité et l'étendue du traitement qui donne l'avantage à la biométrie. L'identification des demandeurs de visa au contrôle des frontières serait tout bonnement impossible par le simple recours à la reconnaissance visuelle.

La rationalisation de l'identification par « *ce que l'on est* ». - La biométrie constitue un renouvellement de l'identification par « *ce que l'on est* ». En associant l'identité à ce qu'il y a de plus permanent chez l'homme, c'est-à-dire des caractéristiques physiques uniques, immuables, et universelles, on fixe au corps une identité à la fois stable et irrévocable. La biométrie garantit l'unicité de la personne en établissant un lien unique entre la donnée biométrique et son porteur, la robustesse de ce lien pouvant en théorie résister à la comparaison de plusieurs centaines de millions d'individus.

Éligibilité à l'enrôlement. - Certains individus ne sont pas éligibles à l'enrôlement. Il existe un pourcentage d'individus exclus de ce type de traitement, du fait de particularités innées ou acquises. C'est le cas des personnes portant le voile, des personnes pratiquant certains métiers ayant pour conséquence de « raboter » les empreintes des doigts, des personnes handicapées. Il semblerait ainsi que le pourcentage de personnes inéligibles aux systèmes biométriques se situe entre 1 et 5%[23].

• Panorama des domaines d'applications de la biométrie

Les apports de la biométrie ouvrent de nombreuses perspectives. Ils permettent d'envisager de nouveaux processus d'identification et de sécuriser davantage les anciennes procédures. Ce bref panorama des domaines d'application des techniques biométriques n'a pas pour objet de présenter leur régime juridique mais d'illustrer les développements précédents.

La gestion des accès physiques. - Il s'agit de vérifier que seules les personnes habilitées peuvent avoir accès à une zone spécifique. Pour effectuer ce contrôle, on associe l'enregistrement de données biométriques d'une personne à une habilitation. Ainsi, on associe un droit d'accès à une identité déterminée, liée à la personne par ses données biométriques. Lorsqu'une personne se présente, en justifiant de son identité via le système biométrique, elle justifiera indirectement de son droit d'accès.

Par identification au sein d'une base de donnée, ou vérification à partir d'une identité fixée sur un titre, on applique cette méthode à la sécurisation des zones « sensibles » (centrale nucléaire, établissement pénitentiaire, salle de serveurs informatiques ...), dont l'accès est réservé à certains responsables.

Dans ce domaine, l'identification biométrique remplace avantageusement les mots de passe, clés, et autres badges magnétiques, susceptibles de vols, reproduction, divulgation, perte, oubli, détérioration ...

[23] Document de travail sur la Biométrie, Commission Nationale Informatique et Libertés, 1er juin 2005. http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/LA_BIOMETRIEmai2005.pdf

La sécurité n'est cependant pas la seule motivation du recours à la biométrie. Il peut s'agir aussi de l'accès à des zones ne présentant pas de risques particuliers (cantines scolaires, restaurants d'entreprise, bibliothèques, parkings ...) et constitue une modalité de gestion de flux ou de gestion des horaires, voire de surveillance.

La gestion des accès logiques. - Il s'agit essentiellement de l'accès à l'utilisation d'applications informatiques, remplaçant l'éternel couple « identifiant et mot de passe ». La multiplication des « logins », du fait du nombre croissant de souscriptions à des services en lignes par les internautes, incite les utilisateurs et les industriels à chercher des solutions moins contraignantes et plus sécurisées. Les certificats électroniques, autre méthode d'identification sécurisée, semblent encore réservés aux initiés, même si le succès de la déclaration des impôts en ligne – un contribuable sur cinq - témoigne de la démocratisation de cette technologie.

L'identification biométrique peut ainsi être utilisée pour l'accès à un compte de messagerie, à un réseau privé d'entreprise, à une application hébergée, à certains serveurs comprenant des données sensibles, à un service de paiement en ligne sécurisé, à l'accès à un service en ligne de l'administration ou du secteur privé. On pourrait imaginer dans quelques années le remplacement des certificats électroniques utilisés pour la déclaration des impôts en ligne par un système de vérification biométrique.

On peut aussi y inclure l'accès à certains outils comme un ordinateur, un téléphone portable, ou encore à l'ordinateur de bord d'une voiture. Le lancement sur le marché d'un nombre croissant de produits grand public intégrant des capteurs biométriques, témoigne d'un intérêt certain des utilisateurs pour une biométrie de « confort », à l'image du Microsoft Print Reader commercialisé pour quelques dizaines d'euros.

En définitive, la biométrie peut remplacer tout système fondé sur une carte à puce ou un PIN, ce qui permet de mesurer l'étendue de ses applications potentielles.

Sécurisation des titres d'identité. - Le rapport du Sénat sur les nouveaux titres d'identité compte sur la biométrie pour les sécuriser, dans le cadre de la lutte contre la fraude et le terrorisme.

En effet, la comparaison entre les données biométriques insérées dans une puce incorporée au titre et les données de son détenteur permettrait de s'assurer que la personne qui détient le titre est bien le détenteur légitime, c'est-à-dire la personne qui s'est enrôlée au moment de la délivrance. Tous les titres officiels sont alors concernés, dont le passeport, la carte d'identité, le permis de conduire, les visas[24] …

Cependant, le fait que l'on puisse s'assurer de la légitimité de la détention du titre est insuffisant. Le procédé biométrique ne se situe qu'au dernier maillon de la chaîne de délivrance. Or c'est en amont que se situent les problèmes principaux, comme le remarquent les rédacteurs du rapport, du fait de la possibilité de bénéficier de vrais titres d'identité au moyen de fausses pièces justificatives.

[24] Un décret n°2007-240 du 22 février 2007 a institué l'ANTS (Agence nationale des titres sécurisés) placée sous la tutelle du ministre de l'intérieur pour répondre aux besoins des administrations de l'État en matière de titres sécurisés. Elle doit notamment définir et évaluer les normes techniques et leur interopérabilité, assurer la gestion des systèmes informatiques, procéder aux achats des titres sécurisés et des équipements nécessaires pour les mettre à disposition des administrations, mettre en oeuvre des actions de communication, promouvoir les savoir-faire nationaux en matière de titres sécurisés. La liste des titres sécurisés est fixée par le décret du 27 février 2007 n°2007-255 et comprend la carte nationale d'identité électronique, le passeport électronique, le passeport biométrique, le titre de séjour électronique, le visa biométrique et les certificats d'immatriculation des véhicules. Sa mission exclut l'instruction des demandes et la délivrance des titres ainsi que l'accès aux données individuelles et la gestion des fichiers correspondants.

Au contraire, l'utilisation d'un procédé biométrique donnerait l'illusion que l'identité, certifiée par la technique, est incontestable. De sorte qu'un faux titre biométrique, obtenu grâce à des justificatifs falsifiés, devient un faux parfait. Le recours à ces données biométriques peut ainsi se retourner contre les personnes qui espéraient y trouver une sécurité renforcée, puisque non seulement les possibilités de fraude en amont ne sont pas réduites, mais en plus la biométrie vient en aval poser sur les titres le sceau de la perfection.

Fondamentalement, une formalisation plus stricte des procédures de délivrance des justificatifs (état civil, justificatif de domicile, intégration d'une photo dans le livret de famille, authentification des actes établis à l'étranger) aurait un impact beaucoup plus significatif en termes de sécurisation des titres d'identité que l'intégration de données biométriques, qui dans ce domaine apparaît aussi efficace qu'un pansement sur une jambe de bois. On peut toutefois se réjouir du maintien de l'aspect simplement déclaratif de l'identité, qui constitue une sorte de garde-fou[25] contre l'éventualité de l'avènement d'un régime anti-démocratique avec la possibilité de pouvoir constituer des faux papiers pour la exemple pour des résistants.

Sécurisation de la délivrance des titres. - Par ailleurs, la biométrie permet d'assurer l'unicité de la délivrance, en empêchant qu'une même personne puisse se voir délivrer plusieurs titres sous plusieurs identités. Cette application nécessite de constituer une base de donnée des personnes ayant fait une demande. Si cette personne apparaît déjà sur la liste, on peut considérer qu'il s'agit soit d'une erreur, soit d'une tentative d'acquérir une seconde identité.

Identification judiciaire. - Il s'agit là de l'application la plus ancienne de la biométrie, parfois appelée « bertillonnage » du nom de son inventeur. Généralement, l'identification d'un criminel peut être effectuée en comparant des traces anonymes, relevées sur les lieux d'un crime, aux empreintes des criminels fichés par les services de police. Dans ce domaine, les apports de l'informatique ont été intégrés depuis longtemps au processus, l'évolution envisagée consistant à étendre le fichier des empreintes digitales à l'ensemble de la population.

Recherches en paternité et en filiation. - Il existe un autre domaine d'identification des personnes en matière judiciaire, pour les recherches en paternité et en filiation. L'expertise judiciaire a aujourd'hui souvent recours à des analyses ADN. Il s'agit là d'un sujet à part en entière que nous évoquerons par la suite, pour en relever les conséquences au regard du droit de la preuve.

Contrôle des frontières. - La biométrie permet déjà de procéder au filtrage des individus dans le cadre des contrôles aux frontières, où toutes les empreintes sont collectées pour les comparer aux bases de données centralisées européenne partagées entre les États (Interpol, SIS, VIS pour les demandeurs de VISA, Eurodac pour les demandeurs d'asile, programme américain d'exemption de visa …). Les personnes identifiées figurant dans les listes noires font alors l'objet des mesures particulières. L'efficacité du contrôle automatisé permet par ailleurs une gestion accélérée des flux des voyageurs dans les aéroports.

Contrôle d'identité. - La vérification sera également possible dans le cadre des contrôles d'identités habituels, obéissant à un cadre juridique et à des conditions propres. La preuve de l'identité auprès des forces de police peut se faire par tout moyen, y compris le témoignage, la carte d'identité n'étant pas obligatoire. Par exemple, lorsque la personne contrôlée possède une carte, la vérification s'opère essentiellement par reconnaissance visuelle, l'agent comparant la photo présente sur le titre et le visage de la personne.

---

[25] Audition de M. Gérard NOIRIEL historien, directeur d'Etudes à l'Ecole des Hautes Etudes en Sciences Sociales (EHESS), Commission Nationale Informatique et Libertés, 15 février 2005.
http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/CRAUDITIONNOIRIEL.pdf

L'intégration d'éléments biométriques dans les passeports, cartes d'identité, permis de conduire, devrait cependant appeler à une réforme des procédures de contrôle de police, notamment en fonction de la constitution ou non d'une base de données centralisée. Dans ce cas, il est probable qu'un contrôle de police consistera à relever les empreintes digitales d'une personne, à les comparer à celles du titre et à celles présente dans la base de donnée ayant servi à la délivrance du titre. Cette collecte pourrait également à terme, permettre de vérifier que la personne contrôlée ne figure pas sur une liste noire.

Traçabilité et gestion des horaires. - Beaucoup de systèmes biométriques sont conçus pour conserver des données concernant l'utilisation du système. On se réfère à ces données sous les noms de « données virtuelles », « données de trafic » ou « données associées ». Elles indiquent en général quand et à quel endroit un individu a été en contact avec le système et donc permettent de recueillir des informations relatives à son parcours, par exemple dans une zone déterminée, à partir de ses différents passages devant la borne biométrique. Ces données peuvent rendre compte des heures d'entrée et de sortie, du temps passé dans une zone sécurisée, de la fréquence de passage, des tentatives de fraudes... Dans le cadre du contrôle des frontières, cette traçabilité permet de déterminer le pays d'origine d'une personne, sa destination, les pays par lesquels il a transité, pendant combien de temps...

Ces données permettent de reconstituer *a posteriori* l'historique d'une personne dans l'espace et dans le temps, éventuellement exploitable dans le cadre d'une enquête ou dans le cadre de la coopération internationale contre le terrorisme.

Elles ont cependant pour effet secondaire de révéler des informations concrètes sur le comportement d'une personne. À chaque fois que la personne concernée soumet ses caractéristiques biométriques, elle laisse des traces plus ou moins précises sur son comportement. La traçabilité biométrique peut donc être à la fois la finalité initiale d'un traitement, mais peut aussi constituer une finalité détournée, lorsque le recours au système biométrique n'a pour objet que le contrôle d'accès, ou la sécurisation d'un titre de voyage.

§ 2. De nouvelles vulnérabilités ?

• *Un système probabiliste*

Probabilités de correspondance entre deux données biométriques. - Une des caractéristiques essentielles de l'identification biométrique est de comparer deux gabarits. Mais le système ne fait qu'évaluer le degré de ressemblance et non l'exacte correspondance entre deux données. En effet, entre l'enrôlement et l'appariement, le candidat ne présente jamais son doigt deux fois de la même façon. La pression sur le capteur, l'orientation dans l'espace, la lumière, ou même le vieillissement du doigt ont une influence sur le résultat du traitement. De sorte qu'il n'y a jamais de correspondance parfaite entre la donnée de référence et la donnée présentée lors de l'identification.

Pour compenser cette différence, le système repose sur un calcul de probabilité. L'administrateur va déterminer un seuil fixe à partir duquel on va considérer que deux données présentent des différences suffisamment négligeables pour qu'on puisse considérer qu'elles correspondent. Ainsi, si les données correspondent à 98%, et qu'un seuil strict a été fixé à 99%, le candidat sera rejeté. Inversement, si le seuil a été fixé de manière souple à 79% et que les empreintes se ressemblent à 91%, on considère la personne comme identifiée.

« **Faux rejets » / « fausses acceptations »**. - Ce seuil correspond en fait à un compromis entre deux objectifs : éviter les faux rejets (une personne habilitée n'est pas reconnue) et éviter les

fausses acceptations (une personne non habilitée n'est pas reconnue). Un seuil fixé à 99% correspond à une politique stricte, permettant d'éviter les fausses acceptations. Il rejettera ainsi toute comparaison qui n'atteindrait qu'un « score de similitudes » de 98%. Mais cette politique stricte a pour inconvénient de multiplier les possibilités de faux rejets, et donc d'interdire l'accès à des personnes habilitées. *A contrario*, un seuil bas fixé à 79% permet au système de reconnaître un candidat, dès que les données se ressemblent à 79%, mais multiplie les possibilités de fausses acceptations.

En définitive, ces deux objectifs sont antinomiques. Éviter les faux rejets suppose une acceptabilité large, et éviter les fausses acceptations suppose une acceptabilité restreinte.

Une science inexacte. - Le caractère probabiliste d'un système biométrique emporte plusieurs conséquences. Il faut se garder de considérer l'identification biométrique comme une science exacte. Ainsi, il revient au responsable de traitement d'assumer le caractère faillible inhérent au système biométrique pour lequel il a opté. C'est à lui d'établir le degré adéquat de probabilité par rapport à la finalité du système.

L'analyse de ces probabilités doit inciter les responsables de traitement à réfléchir sur les applications à grande échelle, notamment pour la gestion des flux de plusieurs dizaines de milliers de personnes, comme dans le cas des contrôles aux frontières.

• Perfectibilité des technologies[26]

Les technologies biométriques peuvent être classées selon deux catégories de données.

Données stables. - Les techniques associées à des données stables reposent essentiellement sur la physiologie et comprennent la reconnaissance faciale et vocale, la reconnaissance de l'empreinte digitale, de la géométrie de la main, de l'iris, de la rétine, de la forme de l'oreille, l'analyse des structures de l'ADN, le réseau veineux, la détection de l'odeur corporelle, l'analyse des pores de la peau.

Données dynamiques. - Les techniques associées à des données dynamiques reposent sur des analyses comportementales et comprennent la vérification de la signature manuscrite, l'analyse de la frappe sur le clavier, l'analyse de la démarche.

Au-delà de leur maturité technique, tous les éléments biométriques ne sont pas équivalents. Chacune de ces technologies présente des avantages et des inconvénients en termes de fiabilité globale, de stabilité, de coût, d'acceptabilité par les utilisateurs, de transparence, de facilité d'emploi, de rapidité d'analyse, d'applications potentielles (identification, vérification). Ces limites techniques se superposent à des limites propres aux types de marqueurs biométriques utilisés. On estime que le taux de différenciation d'une personne par rapport à une autre varie considérablement en fonction des éléments biométriques utilisés.

En résumé, il n'existe à l'heure actuelle aucune technologie offrant un compromis acceptable entre ces différents critères.

Biométrie multimodale. - Il serait inutile de tirer des conclusions trop catégoriques. La recherche devrait à terme parvenir à une solution acceptable.

[26] On trouvera en annexe un tableau récapitulatif des technologies biométriques en fonction des marqueurs utilisés.

Le développement de la biométrie « multimodale », utilisant plusieurs éléments biométriques fait l'objet de nombreux travaux. Elle est déjà indirectement à l'œuvre puisque les recommandations concernant par exemple les passeports biométriques, commandent aux États membres de l'Union Européenne de relever plusieurs types de données biométriques (visage et empreintes digitales).

Cependant, ces différents aspects permettent de se poser la question de l'application éventuelle d'un principe de précaution, lié à l'usage d'une technologie dont on ne connaît pas les effets pour les générations futures, ou à tout le moins, d'éviter de considérer la biométrie comme une panacée universelle, exempte de défauts.

• ***Vulnérabilité de la biométrie à la cybercriminalité***

Comme tout système reposant sur l'informatique, un dispositif biométrique est potentiellement vulnérable à toute forme d'attaque des systèmes d'information.

Méthodes artisanales. - Ces attaques peuvent consister par exemple à contrefaire les marqueurs biométriques. Ainsi, lors d'une récente Conférence de l'Union des Télécommunications internationales sur la Sécurité, un mathématicien japonais, Tsutomo Matsumoto, a décrit en direct, comment fabriquer une maquette de doigt, moulée avec de la gélatine pour confiseries à partir de la trace d'une empreinte digitale laissée sur un verre, elle-même prélevée à l'aide d'un simple bout d'adhésif. Il l'a ensuite photographiée en haute définition, en rehaussé les contrastes avec un logiciel de retouche, et imprimée sur un papier transparent photosensible. Sur les quinze principaux lecteurs biométriques disponibles à l'époque sur le marché, onze ont été piégés. Cette prothèses mise sur le doigt peut même leurrer les systèmes « anti-doigt mort », relevant notamment la circulation sanguine et la chaleur.

Piratage informatique. - Moins exotiques, les techniques traditionnelles des pirates informatiques sont susceptibles d'affecter les systèmes biométriques, particulièrement lorsque les données reposent sur un serveur accessible par un réseau local ou par Internet. Ainsi, il est possible de contourner la capture de l'image biométrique, avant sa conversion en gabarit pour comparaison, en introduisant directement dans le système une image préalablement prélevée (« replay attack »).

Un pirate ayant réussi à accéder au serveur peut aussi remplacer le gabarit stocké par ses propres données, ce qui correspond en fait, à usurper l'identité de l'utilisateur légitime (« substitution attack »).

Il est également possible d'accéder au paramétrage du système et de le régler sur un seuil d'acceptabilité très haut, de manière à ce que toute donnée présentée par le système soit reconnue (« tampering »).

Un autre type d'attaque, à mi-chemin entre méthodes artisanales et piratage, consiste à retracer manuellement l'image approximative d'une empreinte digitale, à la redessiner sur le modèle d'un gabarit copié à partir du serveur qui les stocke (« masquerade attack »).

Certains éléments du programme d'identification peuvent encore être remplacés par un « cheval de Troie » qui affichera systématiquement un haut score de correspondance entre les données enregistrées et les données présentée (« Troy Horse attack »).

La réponse d'un système biométrique étant toujours binaire, soit vraie soit fausse, il est encore possible d'intercepter la communication de cette réponse entre l'application et la capture des données et donner à la réponse la valeur qu'on souhaite. (« overriding Yes/No response).

De ce point de vue, la biométrie de fait que substituer aux procédures d'identification de nouvelles vulnérabilités, liées à l'usage de l'informatique, à d'anciennes vulnérabilités, liées à l'ingénierie sociale et aux défaillances de l'homme. On notera simplement que les premières sont *a priori*, plus difficile à mettre en oeuvre, nécessitant des compétences plus poussées. Il est douteux à cet égard que ce constat constitue un obstacle aux activités terroristes, auxquelles la biométrie est sensée répondre.

SECTION2. Applications actuelles de la biométrie

SOUS-SECTION 1 : Applications de la biométrie en France

§ 1. Fichiers de police

• *Le Fichier National Automatisé des Empreintes Digitales*

« Bertillonage ». - On doit à Alphonse BERTILLON le système d'identification criminelle basé jusqu'alors sur l'anthropométrie et la photographie, introduit en 1894. En 1902, pour la première fois en France, il identifiait l'auteur d'un homicide à partir de traces relevées sur une vitrine fracturée, qu'il avait comparée manuellement avec les empreintes de l'intéressé, classées au fichier anthropométrique dactyloscopique.

L'informatisation de ce fichier a débuté dans les années 1980 pour donner naissance à la première mouture du Ficher National Automatisé des Empreintes Digitales, créé par un décret n° 87-249 du 8 avril 1987 et officiellement mis en service en 1992. Plusieurs textes sont venus étendre son champ d'application par la suite, notamment un décret n° 2005-585 du 27 mai 2005. Au 31 août 2006, 2 398 727 individus étaient fichés au FAED. La CNIL s'est prononcée sur l'utilisation de ce fichier dans deux décisions n° 86-102 du 14 octobre 1986 et n° 04-068 du 24 juin 2004. Outre la CNIL, le fichier est placé sous le contrôle du procureur général de la cour d'appel dans le ressort de laquelle est situé le service gestionnaire.

Champs d'application. - Le FNAED sert à la recherche et à l'identification des auteurs de crimes et de délits, à la poursuite, à l'instruction et au jugement des affaires dont l'autorité judiciaire est saisie, et à la détection des usurpations d'identité ou des identités multiples. Le FNAED permet de s'assurer de la véritable identité des personnes mises en cause dans une procédure pénale ou condamnées à une peine privative de liberté, et plus généralement des personnes « *contre lesquelles il existe des indices graves et concordants de nature à motiver leur inculpation* ». Il s'agit également d'identifier par comparaison les traces de personnes inconnues relevées sur des lieux d'infractions. Dans le cadre de la coopération internationale, les traces transmises par les services de police étrangers sont insérées au fichier.

Habilitation. - L'alimentation et la consultation du fichier sont limitées aux seuls fonctionnaires habilités des services d'identité judiciaire du ministère de l'Intérieur et des unités de recherche de la gendarmerie nationale. Chaque fonctionnaire habilité possède un code d'accès personnel et bénéficie d'un des treize niveaux d'habilitation, accordé en fonction des tâches qu'il est susceptible d'accomplir. Le rapport[27] du groupe de travail de l'Observatoire National de la Délinquance, rendu par Alain BAUER fin 2006, préconise d'ailleurs que l'accès au fichier soit davantage sécurisé en remplaçant le système de mot de passe par des identifiants biométriques…

[27] http://lesrapports.ladocumentationfrancaise.fr/cgi-bin/brp/telestats.cgi?brp_ref=064000885&brp_file=0000.pdf

Enregistrement des données. - Les traces et les données alphanumériques sont insérées dans le FNAED par des personnels qualifiés appelés « traceurs ». Elles sont numérisées et comparées par le système aux empreintes enregistrées dans la base de données. Le « traceur » juge de la pertinence de ces rapprochements et valide une éventuelle identification, lorsque douze points de concordance peuvent être relevés. L'enregistrement des fiches décadactylaires fait l'objet d'un contrôle de légalité (motif de signalisation) ainsi que d'un contrôle qualité (mentions alphanumériques et relevés digitaux), avant toute insertion dans la base de données.

Les relevés d'empreintes donnent lieu à la rédaction d'une fiche comportant l'état civil, le motif, la date et le lieu de signalisation, des éléments de signalement, des clichés anthropométriques et les caractéristiques d'empreintes digitales. Les empreintes sont conservées 25 ans et les traces sont conservées 3 ans pour un délit et 10 ans pour un crime.

Moyens techniques. - Le fichier est en principe accessible sur trois sites centraux situés à Écully (69) pour la Direction centrale de la police judiciaire, à Paris pour la préfecture de police et Rosny-sous-Bois (93) pour la gendarmerie nationale. Dix-neuf sites régionaux sont répartis dans les services territoriaux de la DCPJ. Depuis la fin du premier semestre 2006, 110 bornes de signalisation ont été déployées dans les services de police dans le cadre d'un plan pluriannuel qui prévoit d'en implanter 320 sur tout le territoire d'ici 2009. Les bornes T1 et T4 permettent la numérisation des empreintes et des documents encrés, et la transmission par voie électronique des données alphanumériques et empreintes dans la base du FAED.

• Le fichier national des empreintes génétiques.

Utilisation des données ADN. - Découvert en 1944 comme constituant un élément essentiel du matériel héréditaire, l'ADN détermine toutes nos caractéristiques organiques, morphologiques et parfois pathologiques. Sir Alec JEFFREYS a franchi une étape décisive en 1985, grâce à la mise en œuvre d'une technique d'analyse permettant de déterminer une empreinte génétique à partir de l'ADN d'un individu.

Dans le cadre d'une procédure pénale, la comparaison des empreintes génétiques d'une personne avec celles qui ont été retrouvées sur les lieux de l'infraction facilite l'identification du coupable et offre des perspectives opérationnelles supérieures à la biométrie classique. Pour un délinquant, il est en effet quasiment impossible de ne pas laisser de traces génétiques sur les lieux d'une infraction, alors qu'il suffit de porter des gants pour ne pas laisser d'empreintes digitales.

Assimilation aux données biométriques. - Il existe une tendance à assimiler les données génétiques aux données biométriques. Cette approche vient d'une définition très générale de la biométrie reprise dans le plupart des travaux de réflexion et par la CNIL. Pourtant, la loi 78-17 distingue explicitement les deux catégories de traitements au sein de deux alinéas différents. De même, l'OCDE donne des précisions sur ce qui les différencie. Ainsi, le traitement rapide et informatique que suppose la biométrie, ne permet pas pour l'instant d'assimiler l'usage de ces données à un système d'identification biométrique.

Des risques similaires. - Cependant au plan du droit, les risques qui pèsent sur ce type de données sont les mêmes que pour les données biométriques, voire seraient encore plus prononcés. Il semble que cela ne soit qu'une question de temps pour que ces données deviennent exploitables à grande échelle dans un système biométrique. De plus, l'escalade vers toujours plus de sécurité permet d'envisager que l'ADN devienne la caractéristique biométrique de référence, à tort ou à raison, présentant moins d'inconvénients en termes de fiabilité que les marqueurs biométriques actuellement répandus (empreintes digitales, contours de la main, iris).

Selon l'OCDE, l'utilisation des données génétiques aux fins d'identification comporte un risque particulièrement prononcé de détournement de finalité. Grâce à la recherche sur le génome humain, l'établissement du profil de l'ADN permet de tirer certaines conclusions relatives à la santé du porteur. Si un système d'identité fondé sur l'ADN est créé à grande échelle, il y a fort à parier que de fortes pressions seront exercées par les utilisateurs potentiels de cette information (compagnies d'assurance, institutions financières, chercheurs) pour pouvoir accéder au profil de l'ADN, afin d'effectuer des analyses de risques et des recherches.

Textes applicables. - Créé par la loi n° 98-468 du 17 juin 1998 relative à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, le Fichier National Automatisé des Empreintes Digitales a vu son champ d'application étendu aux principaux crimes d'atteintes aux personnes et aux biens. La loi n° 2003-239 du 18 mars 2003 sur la sécurité intérieure a clairement fait du FNAEG un outil d'identification criminelle « généraliste ». Le fichier est placé sous la responsabilité de la direction centrale de la police judiciaire au ministère de l'intérieur, sous le contrôle d'un magistrat. La CNIL s'est prononcée sur ce fichier dans une délibération n° 99-052 du 28 octobre 1999 et plusieurs fois lors de la modification du régime juridique du fichier. Au 31 octobre 2006, près de 350 000 profils figuraient au FNAEG.

Critères d'inscription au fichier. - La loi prévoit d'abord la centralisation des empreintes génétiques des personnes condamnées dans le cadre d'une des infractions mentionnées à l'article 706-55 du Code de procédure pénale, ainsi que la centralisation des empreintes issues des traces biologiques. Par ailleurs, elle prévoit l'enregistrement de l'empreinte génétique des personnes à l'encontre desquelles il existe « *des indices graves ou concordants rendant vraisemblable qu'elles aient commis l'une des infractions mentionnées à l'article 706-55 du Code de procédure pénale* ». Les personnes habilitées peuvent encore procéder à la comparaison de l'empreinte génétique des personnes à l'encontre desquelles il existe « *une ou plusieurs raisons plausibles de soupçonner qu'elles ont commis un crime ou un délit* ». Enfin, il est possible de procéder à l'enregistrement du profil génétique des personnes disparues ou décédées dans le cadre des procédures de recherche des causes de la mort ou des causes d'une disparition. Elles sont conservées jusqu'à 40 ans pour les personnes définitivement condamnées. Le refus de personnes concernées de se soumettre à un prélèvement destiné à obtenir une empreinte génétique constitue une infraction (article 706-56, II du Code de procédure pénale.)

Habilitation. - Les fonctionnaires de l'unité gestionnaire du FNAEG - rattachée au service central d'identité judiciaire de la sous-direction de la police technique et scientifique - sont seuls habilités à assurer la saisie et l'exploitation des données et à consulter la base à la demande des magistrats et des services d'enquête, avec certaines exceptions[28]. Ils accèdent à l'application, via l'interface CHEOPS, grâce à un code qui leur est propre, en fonction de leur profil d'administrateur ou d'opérateur de saisie. Toute opération effectuée sur la base de données fait l'objet d'une traçabilité dans le système.

Enregistrement des données. - Lorsque le scellé contenant du matériel biologique est transmis au laboratoire, l'Officier de Police Judiciaire ou le magistrat joint un formulaire de demande d'analyse et d'inscription au FNAEG sur lequel sont portées différentes mentions procédurales et administratives, relatives au prélèvement. À l'issue de son analyse, le laboratoire transmet à l'unité gestionnaire le formulaire précité auquel il joint une fiche sur laquelle est consignée l'empreinte génétique extraite. Les profils génétiques, insérés dans le fichier, sont issus

[28] La loi permet à l'officier de police judiciaire de faire procéder à un prélèvement et de demander son inscription au fichier, après avoir requis une personne habilitée aux fins d'analyses (article 706-56 du CPP), et sans autorisation d'un magistrat. Cette possibilité est cependant limitée à l'identification des condamnés et des suspects (article 706-54 alinéas 2 et 3). Le texte autorise également la consultation du fichier (par le seul état civil) afin de s'assurer, avant tout prélèvement, que la personne concernée n'y est pas déjà inscrite.

de l'analyse des segments d'ADN dont la liste est fixée par l'article A38 du Code de procédure pénale (arrêté du 14 février 2002). L'unité procède à l'insertion dans la base du FNAEG. Dès l'insertion dans le fichier, le moteur de recherche de l'application balaie la base et propose d'éventuels rapprochements. À l'issue de cette opération, le résultat (positif ou négatif) est communiqué au requérant sous forme de rapport.

Depuis la loi du 18 mars 2003 et le décret du 25 mai 2004, les magistrats, les personnes habilitées et les OPJ peuvent transmettre les informations destinées à alimenter le fichier par voie électronique, le support papier n'étant plus compatible avec les finalités étendues du FNAEG. Pleinement opérationnel depuis le 17 juillet 2006, le logiciel CHEOPS a été modifié pour permettre aux fonctionnaires de consulter et d'alimenter le fichier à partir de leur poste de travail. Les transmissions des données en provenance des laboratoires, plus complexes, sont encore effectuées sur support physique (CD-ROM).

• Le programme INES et la carte d'identité biométrique.

Le programme INES (identité nationale électronique sécurisée) est un projet global qui consiste à fusionner, simplifier et sécuriser les procédures de demande de passeport et de carte nationale d'identité, à améliorer la gestion de ces titres dans de nouvelles applications, et à délivrer des titres hautement sécurisés conformes aux exigences internationales. Il doit permettre en outre d'offrir aux citoyens les moyens de prouver leur identité sur Internet et de signer électroniquement, afin de favoriser le développement de l'administration électronique.

Une finalité inavouée ? - Le programme INES ne constitue évidemment pas *a priori* un fichier de police. Mais d'aucuns s'inquiètent que la finalité inavouée du projet soit la création d'un « fichier des Français », à l'image du projet SAFARI, qui précisément avait été à l'origine de la loi informatique, fichiers et libertés.

En dehors de la sécurisation du titre par l'insertion d'identifiants biométriques garantissant un lien fort avec son détenteur, il est en effet prévu de constituer un fichier biométrique. Tenu par les services chargés de la délivrance, ce fichier permettrait d'assurer l'unicité de la délivrance et du renouvellement des titres, et ainsi empêcher les demandes multiples venant d'une même personne.

Des pressions se font sentir pour savoir qui aura accès à ce fichier, en dehors des services de délivrance des titres. Doit-on autoriser par exemple les services de police à accéder à ce fichier ? Ce fichier correspondrait-il à une généralisation du fichier FNAED ?

Les auditions de M. Pierre de BOUSQUET DE FLORIAN, directeur de la surveillance du territoire, et M. Marcel FAURE, commissaire divisionnaire et chef de la division nationale de répression des atteintes aux personnes et aux biens, ont révélé la forte demande des services de renseignement et de police de pouvoir disposer d'un fichier national aux fins d'identification. Il existe aussi une forte demande de la part des services en charge de la défense des intérêts fondamentaux de l'État et de la lutte contre le terrorisme à des fins de renseignements. Dans ce cas, il s'agirait ni plus ni moins que de la généralisation du fichier FNAED à l'ensemble des citoyens, présumés suspects.

Débat de société. - De nombreux débats ont eu lieu autour de la carte d'identité électronique. La CNIL a procédé en 2005 à l'audition de nombreuses personnalités (historiens, chercheurs, philosophes, juristes, hauts fonctionnaires, représentant syndicaux). Le Forum des Droits de l'Internet a rendu un rapport[29] le 16 juin 2005 sur le projet[30] du Ministère de l'Intérieur du

[29] http://www.foruminternet.org/telechargement/documents/reco-cnie-20050616.pdf

31 janvier 2005, rapport qui aurait incité les responsables à retirer *in extremis* le projet à l'examen de la CNIL.

Pour certaines personnalités, dont Alain WEBER, président de la Commission Libertés et Informatique de la Ligue des Droits de l'Homme, et Thierry WICKERS, président de la Conférence des bâtonniers, l'utilisation de ce fichier sera amenée à être généralisée. Ainsi, à l'occasion d'affaires criminelles médiatiques, il sera certainement reproché au législateur d'avoir retiré au magistrat un moyen d'enquête ou d'instruction peut-être déterminant.

Dans un article intitulé « *INES, une ennemie qui vous veut du mal* »[31] Alain WEBER écrit : « *il faudrait une sacrée dose d'humour pour rire quand même d'INES, tant ce projet est attentatoire aux libertés et révèle l'outrance d'un pouvoir politique définitivement libéré de toute retenue morale concernant le respect des droits des citoyens.* »

Pour d'autres, à l'image de la mission d'information de la commission des lois du Sénat sur la nouvelle génération de documents d'identité et la fraude documentaire, l'architecture technique du fichier peut aussi permettre d'en limiter les risques. Par exemple, l'anonymisation de la base de données biométriques, non reliée à l'état civil, suffit à éviter les demandes multiples. L'idée de chiffrement en revanche ne paraît pas suffisante puisqu'il suffira à l'administrateur de disposer des clés cryptographiques pour disposer des données en clair. Par ailleurs, les empreintes peuvent n'être que « posées », contrairement aux données fichier FNAED qui sont « roulées » - souvent, seules des traces partielles du doigt de côté ou e biais sont retrouvées. Les empreintes roulées sont uniquement utilisées par la police judiciaire.

De la suspension à la révision du projet. - Le projet est resté en suspens par la suite. Cependant l'intervention au « *E-gov Forum* » d'Issy-les-Moulineaux du 18 octobre 2006 de Fabrice MATTATIA, chargé du projet Place Beauvau, a révélé que le ministère travaillait sur une nouvelle mouture du projet qui devrait voir le jour en 2008. Il devrait notamment être révisé sur le modèle du passeport biométrique, qui avait reçu l'aval de la CNIL le 22 novembre 2005 dans une délibération n°2005-279.

Reste que l'article 9 de la loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme autorise expressément les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales à au accéder système de gestion des cartes nationales d'identité pour les besoins de la prévention et de la répression des actes de terrorisme.

Cette disposition a au moins le mérite de couper court à toute discussion sur le statut du fichier de gestion de la carte d'identité, qui est aujourd'hui légalement un fichier national auquel les services de police peuvent accéder.

§ 2. Contrôle des frontières

• L'expérimentation BIODEV et les visas biométriques

L'article 12 de loi du 26 novembre 2003 n° 203-2119 relative à l'immigration prévoit la possibilité de procéder au relevé, à la mémorisation et au traitement des empreintes digitales et de la photographie des demandeurs de titres de séjour, des étrangers en situation irrégulière et des demandeurs de visas, afin de lutter contre l'immigration irrégulière. Ce système, relié au Système

[30] http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf
[31] http://www.ldh-france.org/media/hommeslibertes/actu132_campagne.pdf

d'Information Schengen au niveau européen, permet de lutter contre les demandes multiples de visas auprès de consulat d'États membres différents.

En application d'un décret du 25 novembre 2004, le gouvernement a lancé, en mars 2005, une expérimentation pour une durée de deux ans dénommée BIODEV, pour relever les empreintes digitales des demandeurs de visas dans 7 consulats, les enregistrer dans une base centralisée et dans une puce intégrée au visa délivré. Le décret précise les destinataires des données, les modalités d'accès et de rectification, l'absence de droit d'opposition, la durée de conservation des données (de 2 à 5 ans).

La CNIL s'était prononcée le 5 octobre 2004 sur ce texte, approuvant l'intégration des données sur un support individuel, mais émettant des réserves sur la constitution de la base de données. La CNIL l'a cependant admis à titre expérimental sous réserve d'une évaluation au regard d'autres procédés.

De l'expérimentation à la généralisation. - Le décret n° 2006-470 du 25 avril 2006 a autorisé l'extension du champ d'application géographique du dispositif (11 nouveaux postes frontières et trente-quatre postes consulaires) et la reconduction de l'expérimentation pour 1 an.

Le nouveau dispositif autorise les services de police urbaine (commissariats centraux de Lille, Lyon, Marseille) à accéder à la base pour connaître la situation d'une personne appréhendée.

Par ailleurs, la base de donnée devait pouvoir être alimentée par les autorités consulaires des autres États-membres, notamment avec les données biométriques de personnes ayant déjà fait l'objet d'une demande de visa dans un autre État.

Dans une délibération n° 2005-313 du 20 décembre 2005, la CNIL avait émis d'importantes réserves sur les modalités envisagées, notamment sur l'accès par les services de police au fichier BIODEV, sur l'absence d'évaluation de l'efficacité de la base de donnée par rapport aux visas intégrant des données biométriques, ou encore sur la conservation des données biométriques de personnes n'ayant pas obtenu de visa.

L'article 9 de la loi n°2006-64 du 23 janvier 2006 autorise aujourd'hui les agents, individuellement désignés et dûment habilités, des services des directions générales de la police nationale, de la gendarmerie nationale ainsi qu'aux agents des services de renseignement du ministère de la défense, à accéder au fichier BIODEV. Ces agents peuvent aussi accéder au fichier national des immatriculations, au système national de gestion des permis de conduire, au système de gestion des cartes nationales d'identité, au système de gestion des passeports, et au système informatisé de gestion des dossiers des ressortissants étrangers en France.

• L'expérimentation PEGASE

Autorisé par un décret n° 2005-556 du 27 mai 2005, le Programme d'Expérimentation d'une Gestion Automatisée et Sécurisée est une expérimentation menée par Air France à l'aéroport Roissy-Charles de Gaulles pour fluidifier les contrôles de police vers la zone privée d'embarquement grâce à un système biométrique. Les formalités de passage étaient simplifiées pour les 10.000 passagers qui y ont participé.

Après s'être inscrits auprès de la police de l'air et des frontières, les passagers se voyaient remettre une carte, comportant différents éléments d'identification dont l'empreinte des deux index. Les passagers entraient alors dans un sas spécifique conçu par la société Sagem. Ils présentaient leur carte devant un lecteur et posaient simultanément l'un de leur index sur un *scanner* pour

identification. Si les deux empreintes concordaient, la porte de sortie du sas s'ouvrait. En cas de problème, le passager était dirigé vers un agent pour se prêter à une identification manuelle.

Le projet a été reconduit pour un an par un décret n°2006-587 du 24 mai 2006, la CNIL s'étant prononcé sur le nouveau décret par une délibération n° 2006-065 du 16 mars 2006. À terme, un nouveau projet « Parafes » devrait être déployé sur ce modèle dans les aéroports internationaux pour le passage aux frontières extérieures Schengen.

SOUS-SECTION 2. Coopération européenne et internationale

§ 1. Systèmes et fichiers biométriques européens

• L'évolution du Système d'Information Schengen (SIS)

Une contrepartie à la suppression des frontières. - Le Système d'Information Schengen, créé par la Convention d'application de l'Accord de Schengen du 19 juin 1990, consiste en une base de donnée centralisée à Strasbourg interconnectant les fichiers « reflets » nationaux des 18 États signataires. Ce fichier est présenté comme une mesure compensatoire à la suppression des contrôles aux frontières intérieures des États participants et à la libre circulation des personnes. Au 31 août 2006, la base nationale comptait 80.620 billets de banque, 164 716 documents vierges, 68 741 armes, 1 890 159 documents d'identité délivrés, 199 819 véhicules, 159 688 personnes recherchées.

Données concernées. Ce fichier regroupe notamment des données sur les personnes physiques disparues comme les mineurs en fugue ou enlevés, les personnes recherchées pour une extradition ou pour comparution devant la justice dans le cadre d'une procédure pénale ou pour exécution d'une peine privative de liberté, les ressortissants des pays tiers non admissibles sur le territoire national, les personnes disparues, selon les finalités prévues par les articles 95 à 100 de la Convention.

Intégration de données biométriques au SIS II. - La mise à jour de ce système doit permettre d'intégrer les données des fichiers des 10 pays qui ont adhéré à l'Union Européenne le 1er mai 2004. L'objectif est également de que le SIS II puisse *« assurer le stockage et le transfert de données biométriques, notamment de photographies et d'empreintes digitales, et la possibilité d'interroger ces données* ».

Dans une communication de décembre 2003, la Commission européenne donne des exemples de situations où le recours aux éléments d'identification biométriques serait utile, lorsque les autorités ont arrêté une personne munie de documents falsifiés, ou lorsque les signalements attachés à un nom font l'objet de contestations, les cas d'homonymie et surtout d'usurpations d'identité étant fréquents dans ce domaine. De nombreux signalements peuvent ainsi être associés à une mauvaise personne.

Les règles spéciales de protection. - Des règles spéciales de protection des données à caractère personnel sont définies au Chapitre 3, articles 102 à 118 de la Convention d'application. Le contrôle de ce fichier en matière de protection de donnée est assuré par l'Autorité de Contrôle Commune Schengen, qui s'est prononcée dans un avis du 19 mai 2004 sur le nouveau dispositif et l'intégration de données biométriques comme identifiant au sein du SIS II. Elle a ainsi jugé nécessaire la définition d'un « *cadre juridique clair* » du fait des risques plus importants « *d'élargissement de la finalité du système* ».

En France, le fichier reflet N-SIS est encadré par le décret n° 95-577 du 6 mai 1995, sous la responsabilité du ministère de l'intérieur (direction générale de la police nationale). La CNIL a

publié un guide de 48 pages sur les modalités d'exercices du droit d'accès (article 109 de la Convention). Il peut s'exercer dans n'importe quel pays, les données des fichiers décentralisés étant les mêmes que celles du système central, mais conformément au droit national de l'État saisi. En France, le droit d'accès est mixte. Il est direct par exemple pour les personnes enregistrées dans l'intérêt des familles ou les mineurs fugueurs (article 97). En dehors des cas prescrits, c'est le droit d'accès indirect qui s'applique, aux termes de l'article 39 de la loi informatique, fichiers et libertés.

• Système d'Information sur les Visas (VIS)

Création d'un système européen d'information sur les visas. - Ce système d'information a pour objectif de prévenir les demandes multiples de visas auprès de consulats d'État membres différents. Il s'agit de collecter en plus des données alphanumériques des données biométriques (photo et empreintes digitales) à des fins d'identification des demandeurs de visa. Les consulats et autres autorités compétentes des États membres procèderont à la saisie ou la consultation de données aux fins de délivrance ou le refus de délivrance d'un visa.

Le système VIS repose sur une base centrale placée auprès de la Commission européenne, reliée par une interface commune aux systèmes nationaux nécessaires aux décisions nationales de délivrance ou de refus de délivrance d'un visa.

Fin des négociations. - La discussion sur la proposition de règlement concernant le système est entrée dans sa phase finale en vue d'une adoption par le Parlement européen. Très contestée, notamment par le groupe de l'article 29, la clause passerelle prévoit que les données collectées au titre des finalités du VIS, et donc du premier pilier, sont mises à disposition des autorités du troisième pilier, compétentes pour prévenir et lutter contre les infractions criminelles.

Avis du groupe 29 sur l'intégration de données biométriques. - Selon le groupe de l'article 29, le recours à la biométrie sur une échelle sans précédent requiert l'adoption de garanties supplémentaires et des modalités de contrôle renforcées.

Ainsi, le texte devrait tenir compte des cas d'impossibilité d'une collecte biométrique pour certaines personnes sans que cela ne les pénalise. Les comparaisons automatisées fondées sur les données biométriques devraient être effectuées *« d'une manière qui garantisse un très bas taux de faux rejet* ». En cas de rejet, les personnes doivent pouvoir être informées des motifs et des moyens d'obtenir *« une réévaluation à l'aide de moyens non automatiques* ».

Par ailleurs, le texte devrait prévoir l'effacement des données biométriques des étrangers ayant obtenu un permis de séjour de longue durée ou ayant obtenu la nationalité d'un État membre. Un âge minimum pour la collecte des données biométriques devrait également être fixé. Les données des personnes « invitantes » (personnes morales ou physiques qui s'engagent à prendre en charge des frais de subsistance pour la durée du séjour) ne devraient pas être conservées au-delà de la durée nécessaire à la finalité du traitement ; la collecte aux données doit se limiter à ce qui est nécessaire à l'octroi du visa. Enfin, la formation des personnels aux règles de protection et l'existence de matrices d'habilitations strictes doivent être garanties.

• Eurodac et la gestion des demandes d'asile.

Le système Eurodac est une base de données centralisant les fichiers des États-membres contenant les empreintes digitales des demandeurs d'asile et des immigrants clandestins. En comparant les empreintes lors du contrôle aux frontières, les États membres peuvent vérifier si un demandeur d'asile a déjà formulé une demande dans un autre État membre et déterminer ainsi l'État

responsable de l'examen d'une demande d'asile. Cela permet aussi d'identifier les demandeurs d'asile entrés irrégulièrement sur le territoire de l'Union.

Textes applicables. - Ce système a été institué en application de la convention de Dublin[32] signée le 15 juin 1990, le Règlement n°2725/2000 du Conseil du 11 décembre 2000 et le Règlement (CE) n° 407/2002 du Conseil du 28 février 2002 qui en fixe les modalités d'application.

Conservation. - Les données des demandeurs d'asile sont conservées dix ans, mais peuvent être effacées avant si la personne obtient la citoyenneté d'un des États membres. Les données des immigrants clandestins sont conservées deux ans et peuvent être effacées avant si l'intéressé obtient un titre de séjour ou quitte le territoire des États membres.

Contrôle. - Le Groupe de coordination de contrôle d'Eurodac est une autorité de contrôle commune indépendante, placée sous la responsabilité du contrôleur européen de la protection des données. Cette autorité est chargée notamment de contrôler l'activité de l'unité centrale afin de s'assurer que les droits des personnes concernées soient respectés et de répondre aux problèmes de mise en œuvre liés au fonctionnement d'Eurodac.

Le Groupe a publié le 7 juillet 2007 son premier rapport[33] d'inspection sur la base de donnée européenne. Le groupe constate par exemple que 6% des empreintes prélevées par les États membres étaient rejetées à cause de leur mauvaise qualité. En principe, les empreintes digitales d'Eurodac ne peuvent être utilisées que pour déterminer le pays responsable de la demande d'asile. Si aucun abus n'a été constaté, le groupe de coordination remarque malgré tout que certaines unités nationales d'Eurodac sont gérées par les forces de police et que le principe de l'accès des autorités policières à ces différentes bases de données est de plus en plus reconnu. Il existe également des pays où le responsable du traitement au plan national est difficilement identifiable.

Fichier INEREC en France. - En France, l'Office français de protection des réfugiés et apatrides, établissement public placé sous tutelle du Ministère des Affaires étrangères, est chargé d'appliquer la Convention de Genève du 28 juillet 1951, relative au statut des réfugiés et la Convention de New-York du 28 septembre 1951 qui définit le statut des apatrides.

L'OFPRA est notamment chargé de la gestion du fichier INEREC[34] qui contient les empreintes digitales des demandeurs du statut de réfugié, utilisé en lien avec la base Eurodac. Les données sont conservées 10 ans. Dans une décision du 22 avril 1997, le Conseil Constitutionnel avait censuré une disposition de la loi du 25 avril 1997, qui prévoyait la possibilité, pour les services du ministère de l'Intérieur et de la gendarmerie, de consulter le fichier dactyloscopique de l'OFPRA. Pour le Conseil, *« la confidentialité des éléments d'information tenus par l'OFPRA et relatifs à la personne sollicitant en France la qualité de réfugié est une garantie essentielle du droit d'asile, principe de valeur constitutionnelle* ».

§ 2. Relations avec les États-Unis

• *Programme américain de dispense des visas*

[32] La Convention de Dublin a été remplacée par le Règlement Dublin le 18 février 2003, s'appliquant à tous les États membres sauf le Danemark, ainsi qu'à la Norvège et l'Islande. Depuis le 1 avril 2006, le règlement Dublin s'applique aussi au Danemark et la Convention de Dublin est dès lors devenue obsolète.

[33] http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Eurodac/07-07-17_Eurodac_report_EN.pdf

[34] Arrêtés du Ministère des Affaires étrangères du 5 décembre 1990, du 6 novembre 1995 et du 9 décembre 1999.

Lutte contre le terrorisme. - Depuis le 11 septembre, le *Department of Homeland Security* (Département pour la sécurité intérieure) des États-Unis met en oeuvre une politique de recours généralisé à la biométrie, qui s'est d'abord manifesté par le programme d'exemption de visa (USA Visa Waiver Program). Ce programme s'inscrit dans le cadre de la lutte contre le terrorisme par le contrôle aux frontières de l'identité des personnes, afin de repérer les terroristes notoires. Les autorités ont annoncé que le dispositif avait également permis de repérer des trafiquants de drogue et des fraudeurs à la carte bancaire.

Depuis janvier 2004, les voyageurs ayant besoin d'un visa pour se rendre aux États-Unis doivent se soumettre à la collecte de deux empreintes digitales et à une numérisation du visage. Cette mesure a été étendue à 27 pays supplémentaires (15 États de l'Union Européenne dont la France, le Royaume-Uni, l'Italie, le Luxembourg, l'Autriche, ainsi que le Japon, l'Australie, la Nouvelle-Zélande, Brunei et Singapour). Le dispositif est en cours de déploiement et déjà opérationnel sur les principaux points d'entrée sur le territoire. Il est également en voie de généralisation à l'ensemble des frontières, aéroports, ports, points de passage terrestre.

Mesures techniques de protection des données. - En l'absence d'un corpus juridique particulier, les mesures de protection de la vie privée sont essentiellement techniques (matrices d'habilitations, sécurité physique des locaux, mots de passes et identifiants, clés cryptographiques réinitialisées quotidiennement, audits techniques). Ces spécificités sont référencées en fonction des risques de détournement, dans un rapport d'impact sur la vie privée[35] du 15 juin 2005, publié sur le site du DHS et régulièrement mis à jour.

Recommandations du « *Chief Privacy Officer* ». - Dans une déclaration[36] générale du 14 septembre 2004, le *Privacy Officer*, la seule autorité fédérale américaine affectée au domaine de la protection des données et de la vie privée, définit un certain nombre d'obligations à la charge des agents du DHS, des administrateurs des systèmes et des autorités tierces, obligations qui rejoignent plus ou moins certaines règles européennes de protection des données.

Les personnes habilitées devront respecter notamment un principe de proportionnalité des données collectées *(« Ensure that only personal information that is necessary and relevant for legally mandated or authorized purposes is collected*[37] »). Elles devront aussi respecter un principe de finalité (« *Use personal information collected only for the purposes for which it was collected, unless other purposes are explicitly mandated or authorized by law*[38] »). Elles ont également une obligation de sécurité (« *conduct a risk assessment to identify privacy risks and determine the appropriate security controls to protect against the risk*[39] »). Il est cependant difficile d'évaluer le caractère contraignant des recommandations et des guides publiés par le DHS.

• Passeports biométriques

Une exigence américaine. - La Section 303 du « *Enhanced Border Security and Visa Entry Reform Act of 2002* » fait obligation aux États qui ont été désignés pour participer au *Visa Waiver Program* de démontrer qu'ils ont un programme destiné à délivrer à partir du 26 octobre 2005 des

---

[35] United-States Visitor and Immigrant Status Indicator Technology Program Office, *US-VISIT Program : Privacy Impact Assessment Update International Live Test*, 15 juin 2005 et mis à jour au 22 décembre 2005. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_livetest.pdf
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_update_12-22-2005.pdf

[36] http://www.dhs.gov/xlibrary/assets/privacy/privacy_stmt_usvisit.pdf

[37] « s'assurer que seules les informations pertinentes et nécessaires à la finalité sont collectées »

[38] « utiliser des informations personnelles uniquement pour les finalités pour lesquelles elles ont été collectées »

[39] « mener une étude d'impact pour identifier les risques au regard de la vie privée, et déterminer des contrôles de sécurité appropriés pour prévenir les risques »

passeports incluant des éléments d'identification biométriques authentifiés conformes aux standards de l'Organisation de l'Aviation Civile Internationale.

Ainsi, le règlement (CE) n° 2252/2004[40] du 13 décembre 2004 impose aux États-membres de prévoir un passeport biométrique pour leurs ressortissants et établit des normes de sécurité pour les éléments biométriques intégrés dans les passeports délivrés par les États membres.

Failles de sécurité. - Dans un avis[41] du 30 septembre 2005, le groupe de l'article 29 demande que les passeports ne puissent pas être lus par des lecteurs qui ne sont pas compatibles avec la norme *Extended Access Control* – contrôle d'accès étendu. Cette norme empêche, par un mécanisme de clés combinées, tout interception non autorisée des données biométriques.

La sécurité des passeports est en effet sujette à caution. Ainsi, le quotidien britannique *The Guardian* révélait fin 2006 que les puces intégrées aux passeports pouvaient être piratées en quelques heures et révéler ainsi leur contenu.

De même, des chercheurs de l'Université catholique de Louvain (UCL), Gildas AVOINE, Kassem KALACH et Jean-Jacques QUISQUATER, spécialistes en cryptographie, ont mis en lumière[42] les failles de sécurité des passeports électroniques belges, grâce à un simple lecteur de puces RFID[43]. Les failles des passeports délivrés après juillet 2006 sont par ailleurs les mêmes que celles dont souffrent les passeports anglais, néerlandais, allemands et suisses, ces différents modèles s'appuyant sur le standard de l'Organisation de l'Aviation Civile Internationale.

Application en France. - En France, c'est le décret n° 2005-1726 du 30 décembre 2005 qui crée le passeport électronique. La CNIL s'est exprimée sur ce décret dans une délibération n° 2005-279 du 22 novembre 2005. Le décret modifie ainsi le champ d'application de l'ancien traitement DELPHINE[44] institué par l'arrêté du 22 novembre 1999.

La production et la délivrance des passeports biométriques étaient suspendues en raison d'un recours exercé par l'Imprimerie nationale devant le Conseil d'État. Le Ministère de l'Intérieur avait en effet attribué ce marché à la société Oberthur Card Systems, lors même que cette mission relève du monopole de l'établissement public en vertu de la loi 93-1419 du 31 décembre 1993. Le Conseil d'État a confirmé l'ordonnance du 23 novembre 2006 rendue par le juge des référés du tribunal administratif de Paris qui s'était prononcé pour une suspension de la fabrication des passeports par la société privée.

Il existe un traitement parallèle, dénommé PHILEAS[45], placé sous la responsabilité du Ministère des Affaires Etrangères. Ce traitement est relatif à la fabrication et la gestion des passeports biométriques d'urgence et des laissez-passer. La CNIL s'est exprimée sur ce traitement dans une délibération n°2006-85 du 21 mars 2006.

---

[40] Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres. http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/oj/2004/l_385/l_38520041229fr00010006.pdf

[41] Avis n°3/2005 sur l'application du règlement (CE) no 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_fr.pdf

[42] http://www.01net.com/editorial/350471/la-securite-des-passeports-electroniques-prise-en-defaut/

[43] *Radio Frequency Identification* : identification par radio fréquence.

[44] Délibération CNIL n° 99-23 du 8 avril 1999

[45] Arrêté du 21 mars 2006 portant création d'un système informatisé de fabrication et de gestion des titres de voyage PHILEAS et modifiant l'arrêté du 30 mars 2005 relatif au système informatique de traitement des données relatives aux Français établis hors de France.

Chapitre 2
RISQUES DE LA BIOMÉTRIE AU REGARD DES DROITS DE L'HOMME

SECTION1. Identification biométrique et protection de la vie privée

SOUS-SECTION 1. Un « méta-système d'identification »

§ 1. Les données biométriques, clés universelles d'interconnexions

• La problématique des identifiants uniques

Le 9 avril 1973, Adolphe TOUFFAIT, procureur général de la Cour de cassation affirmait, devant l'Académie des sciences morales et politiques que « *la dynamique tendant à la centralisation des fichiers risque de porter gravement atteinte aux libertés et même à l'équilibre des pouvoirs politiques* »[46]. Ces quelques mots résumaient l'ensemble des inquiétudes que suscitait déjà l'informatique au regard de la vie privée et des principes démocratiques. Ce risque, pressenti et exprimé de manière visionnaire il y a maintenant trente-cinq ans, demeure et s'amplifie aujourd'hui à la mesure des avancées technologiques.

En quoi consiste précisément ce risque ? En quoi la biométrie peut-elle être perçue comme un facteur aggravant ?

De l'informatique aux technologies de la communication. - Dans les années 70, l'informatique est encore fortement centralisée, environ 500 grandes administrations et entreprises concentrant 80% des dépenses informatiques. Les systèmes volumineux centralisés ne supportent alors que des terminaux passifs et des fichiers à structure fixe, dont l'en-tête des enregistrements joue le rôle d'index.

Pour Philippe LEMOINE[47] de la CNIL, deux évolutions transforment ce paysage. D'une part, le passage d'une « logique de fichiers » à une « logique de base de données relationnelles », permet d'échapper aux structures fixes, grâce aux relations dynamiques établies entre un sujet et ses attributs. D'autre part, l'apparition d'une notion « d'administration des données » permet d'attribuer aux différents types de données une définition et une structure homogène, communes aux différentes bases de données qui les utilisent. On passe alors de l'organisation de l'information à la communication de l'information.

Ainsi, les notions d'identifiants uniques vont s'affirmer en substituant aux anciens « index » une administration homogène de données. L'identifiant unique est alors une clé commune d'accès aux fichiers, une sorte de dénominateur commun, permettant les fameuses interconnexions.

De ce point de vue, l'interconnexion suppose simplement de s'accorder sur un langage commun. C'est précisément cette approche qui a permis l'avènement du protocole TCP/IP et donc

---

[46] Cité par Philippe BOUCHET, « *SAFARI ou la chasse aux Français* », Le Monde, 21 mars 1974. http://perso.orange.fr/perso.web/hebergement/biometrie/doc/LEMONDE_Chasse_aux_francais.pdf

[47] Communication de M. Philippe LEMOINE sur les identifiants, les réseaux et l'espace public, Commission Nationale de l'Informatique et des Libertés, 10 juin 2004 http://www.cnil.fr/fileadmin/documents/approfondir/dossier/technologies/Com-phl-identifiants-VD-MEF.pdf

de l'Internet, de l'hypertexte et de l'html, langage codés qui permettent de naviguer de façon fluide dans des applications hétérogènes, pilotées par des machines elles-mêmes hétérogènes sur l'ensemble de la planète. En soi, l'interconnexion constitue une modalité technique d'échange entre deux entités, transposant dans le monde numérique, la faculté des hommes à communiquer, c'est-à-dire à « s'assurer que l'autre a entendu et qu'une réaction est possible ».

De l'interconnexion au fichage généralisé. - Les fichiers en question portent très souvent sur les personnes. On parlait de fichiers nominatifs, on parle aujourd'hui de fichiers de données à caractère personnel.

La loi du 6 janvier 1978 a été adoptée en réaction au projet SAFARI. Ce projet stigmatisait alors l'idée de faire du numéro INSEE, c'est-à-dire du Numéro d'Inscription au Répertoire des personnes physiques, un identifiant unique, une clé d'accès universelle à tous les fichiers structurés en fonction de cette donnée.

Le NIR comme identifiant unique est encore aujourd'hui au centre de nombreux débats, par exemple au sujet de son utilisation par l'administration fiscale pour s'assurer de l'identité des contribuables ou au sujet du dossier médical personnel. En application du principe de finalité, la CNIL surveille l'utilisation du NIR jouant le rôle d'identifiant transversal dans des domaines administratifs répondants à des finalités homogènes, tout en encourageant la création d'identifiants sectoriels, empêchant les interconnexions.

Le regroupement d'un maximum d'informations sur une personne permet en effet d'en établir le profil, les comportements, la personnalité, les modes de consommation d'un individu. Ainsi, pour un même individu, ou toute une population, des fichiers interconnectés pourraient regrouper état civil, situation de famille, casier judiciaire, état de santé physique et psychologique, situation professionnelle, déclaration de revenu, état du patrimoine, état des transactions économiques, historique des déplacements, modes de consommation, habitudes alimentaires, préférences sexuelles, origine ethnique, opinons politiques, philosophiques, de ses croyances religieuses.

Ce fichage met en oeuvre une sorte d'informatisation de l'individu et crée, d'une certaine manière, un double virtuel de la personne, qui échappe à son contrôle et se dissocie même la réalité. Pour reprendre la terminologie de BAUDRILLARD, ce « simulacre » de la personne est amené à se substituer à la personne réelle, de sorte que les individus sont moins traités en tant que tels, mais en tant que supports d'informations objectives. Et plus l'information est étayée, plus ce simulacre a vocation à se substituer à la réalité.

Il suffit de superposer cette réflexion aux heures les plus sombres de notre histoire pour en mesurer les dangers, aux heures où certains individus furent traités moins comme des personnes qu'en tant que supports d'une croyance religieuse, d'une opinion politique, ou d'une origine ethnique. Il suffit alors de garder à l'esprit que l'histoire peut se répéter, ou se plonger dans la contemplation de certaines oeuvres d'anticipation, comme l'excellent « Gattaca[48] ».

• La problématique appliquée à la biométrie

Les données biométriques, des données identifiantes. - Ce n'est évidemment pas un hasard si, comme nous le verrons, le régime juridique de la biométrie est calqué sur celui du NIR. Ainsi, l'article 27 de la loi de 1978 soumet deux types de traitements opérés pour le compte de l'État à autorisation par décret en Conseil d'État pris après avis motivé de la CNIL. Il s'agit des «

[48] http://www.imdb.com/title/tt0119177/

traitements qui portent sur des données parmi lesquelles figure le numéro d'inscription des personnes au répertoire national d'identification des personnes physiques » et « *des traitements qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes* ». La soumission des deux types de traitement à la même procédure de contrôle *a priori* atteste clairement de leur lien de parenté.

Ce n'est pas non plus un hasard si la définition des données à caractère personnel a été modifiée pour y inclure, de manière implicite la biométrie. « *Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ». Avant la réforme de 2004, la définition était moins précise que « *Sont réputées nominatives au sens de la présente loi les informations qui permettent, sous quelque forme que ce soit, directement ou non, I'identification des personnes physiques auxquelles elles s'appliquent* ».

Les données biométriques sont ainsi reconnues implicitement par le droit comme permettant l'identification des individus, au même titre que le NIR, les données s'y rapportant étant constitutives de données à caractère personnel.

La problématique des interconnexions renouvelée. - Le 16 décembre 2005, au cours de la 27ème Conférence internationale des Commissaires à la protection des données et à la vie privée, a été adoptée une résolution[49] sur l'utilisation de la biométrie dans les passeports, cartes d'identité et documents de voyage.

Les Commissaires à la protection des données déclarent ainsi que « *les informations biométriques pourraient être utilisées en tant qu'identificateur unique universel* ». Comme pour le NIR, lorsque deux bases sont structurées par des données biométriques, il est possible de faire un rapprochement entre plusieurs fichiers et de compiler des données nominatives séparées à l'origine.

C'est aussi le diagnostic de l'OCDE dans son rapport[50] sur les technologies biométriques, aux termes d'un paragraphe intitulé « infrastructure de surveillance/ identificateur unique ».

« *Sans doute parce qu'elle incarne la forme ultime d'identification personnelle, la biométrie peut être considérée comme facilitant tous les aspects inquiétants et déshumanisants d'une société d'information – une société dans laquelle une somme d'informations personnelles jamais égalée auparavant peut être recueillie et exploitée de façon systématique. Le risque existe effectivement que l'authentification biométrique devienne la forme par défaut de l'authentification et de l'identification humaines, même dans des situations où une méthode moins intrusive suffirait, simplement parce qu'une empreinte biométrique peut être prise de tout le monde et aussitôt utilisée.* »

Au niveau mondial, on reconnaît donc depuis quelques années l'existence de cette problématique des identifiants uniques, dénominateur commun aux bases de données, clés universelles d'accès aux interconnexions. Le risque pourrait devenir endémique, du fait de la

---

[49] 27ème Conférence internationale des Commissaires à la protection des données et à la vie privée, Montreux, 16 septembre 2005, Résolution sur l'utilisation de la biométrie dans les passeports, cartes d'identité et documents de voyage. http://www.statewatch.org/news/2005/sep/Biometrie-Resolution-f.pdf

[50] Organisation de Coopération et de Développement Economiques, Direction de la science, de la technologie et de l'industrie, Comite de la politique de l'information, de l'informatique, et des communications, Groupe de travail sur la sécurité de l'information et la vie privée, « Technologies Fondées Sur La Biométrie », 10 juin 2005. http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00186151.PDF

possible généralisation de la biométrie à tous les gestes, activités, procédures nécessitant un tant soit peu de sécurité, de l'entrée aux frontières des États-Unis à l'ouverture d'un réfrigérateur ou d'une télévision dotée d'un contrôle parental.

Comme l'a fait remarquer M. George TOMKO, expert en protection de la vie privée et concepteur de systèmes biométriques, « *la biométrie, si elle est utilisée telle qu'elle est commercialisée actuellement, portera atteinte à la vie privée et mettra en péril nos libertés. En deux mots, la biométrie fondée sur un gabarit ne respecte pas la vie privée. Chaque fois que la vérification ou l'identification reposent sur la comparaison avec un gabarit stocké, cela crée des conditions qui, au fil du temps, compromettront la vie privée, que ce soit du fait d'une entreprise ou des pouvoirs publics, notamment lorsqu'il faudra faire face à la prochaine situation de crise nationale* ».

Ainsi, la biométrie est donc à ce point considéré comme l'étape ultime de la rationalisation du processus d'identification, qu'il apparaît aujourd'hui que cet identifiant corporel, intangible, irrévocable, et unique, constitue la clé d'accès idéale à toute les bases de données à caractère personnel existantes et ayant vocation à exister.

Cette démonstration reste cependant éminemment théorique. Il convient de se plonger encore davantage dans la technique biométrique pour comprendre exactement quelle est la portée de ce risque, et comment il peut être atténué.

• Les gabarits, freins ou moteur des interconnexions *?*

Les systèmes d'identification biométriques mettent en jeu deux types de donnée comme décrit dans le chapitre précédent : les données brutes et le gabarit. Leur utilisation pour procéder à des interconnexions dépend de conditions techniques propres à chacune. Il convient donc de les analyser séparément pour saisir la portée du risque de détournement de finalité.

Vers l'interdiction de conserver les données brutes ? - En principe, les données brutes, issue de la numérisation d'un marqueur biométrique, ne sont pas conservées. Elles sont simplement analysées à l'étape de l'enrôlement pour constituer le gabarit de référence, puis à l'étape d'identification pour constituer un gabarit de comparaison. En ce sens, elles n'ont pas vocation à être conservées dans la mémoire du système. Les autorités de protection des données prennent d'ailleurs en compte la conservation des données brutes par un système d'identification pour en contrôler la proportionnalité. En soi, rien ne nécessite de les conserver. On pourrait même s'interroger sur un principe d'interdiction pur et simple de conserver les données biométriques brutes.

Si toutefois elles étaient conservées, le rapprochement de deux bases de données à partir de données brutes est difficile à mettre en oeuvre. Évidemment, il faut au préalable que les responsables de traitement de deux fichiers souhaitent s'entendre sur une interconnexion et prennent le risque des sanctions pénales applicables, ou partir de l'hypothèse d'une tentative de piratage.

En pratique, les données brutes d'une personne créée au sein d'un système A ne permettront pas *a priori*, d'accéder à des informations sur la même personne, contenues dans un fichier B. Les captures numériques ont des caractéristiques propres (résolution, lumière, contraste, saturation des couleurs, dimensions, résistance aux parasites), de sorte que les captures du système A ne seront pas forcément exploitables ou convertibles en gabarits par le système B. Le risque existe, au gré du hasard, que deux systèmes différents soient compatibles, ou tout simplement qu'il s'agisse de deux produits issus du même fabriquant. Le risque demeure, grâce à l'éventualité d'une comparaison

visuelle des données, mais qui correspond à une spécialité professionnelle à part entière. Comme souvent en matière de technologies, c'est moins la biométrie elle-même qui est en cause que les usages qui peuvent en être fait.

Absence relative d'interopérabilité des gabarits. - En principe, une donnée brute ne peut être reconstituée à partir d'un gabarit, le processus d'extraction des caractéristiques étant irréversible.

Sur le plan informatique, seuls les points-clés des minuties d'une empreinte digitale constituent le gabarit, de sorte qu'il est impossible de reconstituer une donnée brute complète et exploitable à partir d'« extraits » partiels. C'est comme si on tentait de reconstituer une musique à partir du tempo, ou un film à partir d'images prises à une minute d'intervalle. Il serait seulement possible de redessiner à la main une minutie approximative à partir des points-clés du gabarit, mais cette opération délicate n'est pas applicable à une masse de fichiers biométriques et ne créerait qu'un risque ponctuel. Ainsi, les gabarits échappent aux éventuels risques qui pèsent sur les données brutes.

Les gabarits comportent en revanche des risques spécifiques. En effet, dans un système d'identification déterminé, un gabarit a par essence, pour fonction d'être rapproché des données du candidat à l'identification pour l'opération de comparaison. On pourrait donc croire qu'un gabarit biométrique est forcément similaire d'un système à l'autre, pour un même marqueur biométrique comme une empreinte digitale.

Or il n'en est rien. Les gabarits ne sont pas interopérables par défaut. Les algorithmes des systèmes biométriques créés par les sociétés privées constituent la véritable valeur ajoutée d'un produit, et la fiabilité du système dépend étroitement de la qualité des programmes en cause. De sorte qu'il s'agit de secrets de fabrique, véritable enjeu de concurrence entre les industriels.

Ainsi, sauf hasard extraordinaire, volonté préalable de pouvoir rendre interopérables deux produits, ou encore utilisation du même produit configuré selon les mêmes paramètres, le gabarit d'un système A ne peut permettre d'accéder aux données associées au gabarit du système B. De même, le gabarit créé par le système A ne permet pas de créer un gabarit exploitable par le système B. À l'inverse du numéro NIR ou même de l'état civil, par définition et par essence interopérables en tant que suites alphanumériques, les données biométriques ne pas sont interopérables par défaut. Ce défaut d'interopérabilité relatif entre la majorité des systèmes actuels constitue techniquement un frein aux interconnexions. On voit alors que le risque véritable est celui de la normalisation des procédés biométriques.

§ 2. L'évolution du risque : les enjeux de l'interopérabilité

• *Le mouvement en faveur de l'interopérabilité*

Les techniques biométriques reposent encore largement sur des formats propriétaires et dispersés, ce qui garantissait une certaine protection contre les détournements de finalité et les interconnexions abusives. Mais un mouvement général de normalisation est en train de remettre en cause cette protection.

Travaux de l'OACI. - L'illustration la plus saisissante de la normalisation de la biométrie aux fins d'interopérabilité, et donc d'interconnexions, est relative aux travaux[51] de l'OACI pour les

[51] Organisation de l'Aviation Civile Internationale, Document 9303, *Machine Readable Travel Documents* (Documents de voyage lisible à la machine), 6ème édition, septembre 2006.

passeports biométriques.

Le Conseil de l'Europe, sous l'impulsion autoritaire des États-Unis, a rapidement adopté un règlement[52] se référant aux normes de l'OACI pour les titres d'identité et les documents de voyage. Cette interopérabilité permettra de rapprocher les données présentes dans les passeports et celles présentées par les voyageurs aux listes noires utilisées dans le cadre du contrôle des frontières et de la coopération policière et judiciaire internationale, finalités auxquelles adhèrent les autorités de protection des données.

Organismes internationaux. - Le JTC 1/ SC 37, un des sous-comité du Joint Technical Comittee de l'ISO, spécialement chargé des questions de biométrie, a pour mission explicite la normalisation des technologies biométriques « *en vue de faciliter l'interopérabilité et l'échange de données entre applications et systèmes* ». Le JTC 1/ SC 37 a ainsi la charge de définir des formats de fichiers communs, des interfaces de programmation des applications (API), des modèles biométriques, des techniques de protection des modèles, des profils d'application et de mise en oeuvre et des méthodologies appliquées à l'évaluation de la conformité. Chacun de ces domaines est pris en charge par un groupe de travail spécifique.

L'ISO/CEI JTC 1/SC 17 s'occupe plus particulièrement depuis 1999 de l'intégration de la biométrie dans les cartes et les documents officiels, dans le cadre de l'amélioration de la sécurité de frontières qu'il considère comme l'un de ses principaux objectifs.

Organismes français. En France, l'organisme spécialisé dans la normalisation et qui coopère notamment avec l'ISO est l'AFNOR (Agence française de normalisation). L'AFNOR a créé un comité de normalisation FTS 40 au sein de la Commission générale CG CSA41.

Ce comité de normalisation FTS est chargé d'étudier plusieurs secteurs en conjonction avec les cartes d'identification : biométrie, signature électronique, protocoles sécurisés sur réseaux ouverts. Par ailleurs, une nouvelle commission AFNOR sur la biométrie CN37 a été instituée en janvier 2004, au sein de laquelle deux groupes de travail ont été créés : GT1 (Techniques biométriques) et GT2 (profils d'utilisation de la biométrie).

Définition de normes communes[53]. - Trois normes ISO/IEC 19785-2:2006, ISO/IEC 19794-1:2006, ISO/IEC 19785-1:2006 définissent un cadre commun d'échange des données biométriques. D'autres définissent un format d'échange et de programmation communs :

• ISO/IEC 19794-2:2005 format commun d'échange des minuties d'empreintes digitales ;

• ISO/IEC 19794-4:2005 format commun d'échange des images d'empreintes digitales ;

• ISO/IEC 19794-5:2005 format commun d'échange des image faciales ;

• ISO/IEC 19794-6:2005 format commun d'échange des images de l'iris.

• ISO/IEC 19784-1:2006 Biometric application programming interface

• Utilité et dangers de la standardisation

Projet de standards intégrant la protection de la vie privée. Sous plusieurs aspects, la

[52] Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres. http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/oj/2004/l_385/l_38520041229fr00010006.pdf

[53] Une liste plus complète des normes existante est consultable en annexe.

normalisation peut avoir un intérêt juridique et aller de pair avec le droit pour mettre en œuvre les règles de protection des données.

Ainsi, les Commissaires à la protection des données se sont montrés favorables à un projet de normalisation porté par l'ISO sur des standards relatifs aux principes de protection de la vie privée. Ils ont ainsi adopté une résolution[54] au cours de leur 26ème conférence, souhaitant être associés activement à l'élaboration de celles-ci et prescrivant plusieurs orientations pour qu'elles n'aient pas qu'une finalité technique.

Évaluation des systèmes. - En dehors des normes citées, la définition d'un cadre commun pour l'évaluation des technologies, comme la norme ISO/IEC 19795-1:2006 sur les tests de performances des systèmes biométriques, est incontestablement un progrès, dans la mesure où est pris en compte le caractère perfectible des systèmes biométriques.

Harmonisation terminologique. - De même, le JTC 1/ SC 37, un des sous-comités du Joint Technical Comittee de l'ISO, spécialement chargé des questions de biométrie, a adopté un document[55] qui définit l'ensemble des termes techniques relatifs à la biométrie, et des recommandations sur l'usage de tel ou tel terme. Par ailleurs, le 6ème groupe de travail (WG6) du SC 37 est chargé de « *questions sociétales et juridictionnelles* » - expression qui traduit le niveau d'expertise qu'on peut en attendre, mais cela part d'une bonne intention...

Ainsi dans un de ses derniers rapports, le groupe de travail indique aux chefs de projet que la mise en conformité avec la loi peut aider à rassurer les personnes concernées, qu'il doivent être conscient des enjeux relatifs à l'utilisation des empreintes digitales, y compris lorsqu'ils souhaitent vérifier le casier judiciaire d'un candidat !

Publication des normes. - On peut cependant se poser la question des dangers de publier les normes techniques utilisées par le secteur public, publication qui rend les systèmes particulièrement vulnérables à toute forme d'attaque, en mettant à disposition de tous, y compris les personnes mal intentionnées, les caractéristiques techniques des dispositifs de sécurité utilisés par les gouvernements.

L'interopérabilité : un risque majeur. - Le véritable enjeu au regard de la protection de la vie privée est donc moins la biométrie elle-même, que la volonté des responsables de traitements, de rendre tous les dispositifs biométriques interopérables, au mépris du principe de finalité. Comme il a été décrit précédemment, c'est essentiellement par la volonté exprès des parties en présence de rendre leurs systèmes interopérables que les gabarits peuvent être utilisés pour une interconnexion de fichier.

De sorte que les réserves techniques sur le défaut d'interopérabilité des systèmes biométriques pourraient à terme être remis en cause, à défaut d'un changement d'approche, d'une prise de conscience, ou de dispositifs légaux.

Une standardisation totale, impliquant secteur privé et secteur public, autorités européennes et nationales, services de proximité et services en lignes, ouvre alors la perspective d'un « méta-système d'identification », rendant potentiellement « interconnectables » tous les fichiers

---

[54] Résolution sur le projet de normes ISO de protection de la vie privée, 26ème Conférence internationale de protection de la vie privée et des données Personnelles Wroclaw, 14 septembre 2004,.
http://26konferencja.giodo.gov.pl/data/rezolucje/fr/rezolucja1.doc

[55] http://isotc.iso.org/livelink/livelink/fetch/2000/2122/327993/2262372/JTC_1_SC_37_Agreed_Harmonized_Core_Biometric_Terms_and_Definitions.pdf?nodeid=5675848&vernum=0

biométriques nominatifs existants, quelles que soient leurs finalités.

Cette méta-identité à la fois éclatée et centralisable, échappant au contrôle de son titulaire, tant dans l'utilisation qui en est faite que de son exactitude, est en train de devenir un instrument de pouvoir sans réel contre-pouvoir. Encore une fois, il n'y a plus qu'à espérer que cette identité volatile ne tombe pas entre des mains mal intentionnées, le cadre juridique actuel ne permettant pas de contrer ce mouvement en faveur de l'interopérabilité.

• L'encadrement juridique des interconnexions

Interdire les moyens ou encadrer les finalités ? Au final, seul le droit peut encore tenter de répondre à ces inquiétudes. La biométrie interopérable reste un moyen mis aux services de différentes finalités. Lorsque cette finalité est l'interconnexion, analysée précédemment comme la véritable source du danger, le réalisme et la logique indique d'en encadrer les conditions de mise en oeuvre et non d'interdire les outils de sa mise en oeuvre. En France et ailleurs, la possibilité de commettre un crime au moyen d'une arme blanche n'empêche pas la commercialisation des couteaux à pain. C'est également l'approche retenue aux États-Unis pour la délivrance des armes à feu, à la différence près que les armes à feu n'ont pas d'autre finalité que de tuer...

Il convient donc de s'en référer au régime juridique des interconnexions, tel qu'il est prescrit par le droit positif, ainsi que celui des transferts de données et de leurs destinataires.

Autorisation de la CNIL pour le secteur privé et public. - Aux termes de l'article 25 de la Loi de 1978, sont mis en oeuvre après autorisation de la Commission nationale de l'informatique et des libertés, « *les traitements automatisés ayant pour objet l'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents* » ainsi que « *l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes* ».

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 € d'amende aux termes de l'article 226-16 du Code pénal.

Communication de données à des tiers. - Le principe de la communication à des tiers de données issues d'un traitement dûment autorisé ou déclaré n'est pas interdit par la loi.

Elle prévoit simplement que les destinataires ou catégories de destinataires soient mentionnés et communiqués aux personnes concernées par le traitement, le destinataire devant s'entendre comme « t*oute personne habilitée à recevoir communication de ces données autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leurs fonctions, sont chargées de traiter les données ».*

Toutefois, la loi précise que les autorités légalement habilitées, dans le cadre d'une mission particulière ou de l'exercice d'un droit de communication, à demander au responsable du traitement de leur communiquer des données à caractère personnel, ne constituent pas des destinataires.

La loi informatique, fichiers et libertés, en son chapitre XII, précise également les conditions de transfert des données à caractère personnel vers des pays non membres de l'Union Européenne, notamment la nécessité que le pays en question offre un degré de protection équivalent.

• Vers une sectorisation des standards biométriques ?

Une solution envisageable consisterait à sectoriser les normes selon leur finalité. Ainsi, on pourrait imaginer une biométrie à deux vitesses, non interopérable, entre le secteur privé et le secteur public, les techniques libres d'utilisation et les techniques protégées par le secret défense.

Il s'agit précisément de la dichotomie retenue pour la cryptologie, dissociée entre les applications militaires et les applications « grand public ».

L'absence de débat en la matière a particulièrement nuit à une application intelligente de la biométrie. Le processus aujourd'hui semble irréversible, alors même que d'autres technologies en développement comportent à la fois la sécurité et l'interopérabilité recherchées et une très forte protection de la vie privée. Nous aborderons cette possibilité au dernier chapitre.

SOUS-SECTION 2. Une infrastructure de surveillance

§ 1. Traçage biométrique et liberté de circulation

• *Un outil de surveillance des déplacements*

Une entrave à la liberté de circulation ? - La biométrie soulève également des questions en matière de libre circulation des personnes. C'est ce que relève la CNIL dans plusieurs décisions et notamment l'autorisation unique n°AU-007[56] sur la 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.

L'article 5 de l'autorisation unique, « liberté de circulation des employés protégés », dispose que *« 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 ».*

En effet, l'identification biométrique tient aujourd'hui une place de choix au sein de l'arsenal de surveillance à la disposition des autorités du secteur privé et du secteur public. La mise en relation des différents lieux et moments où l'on a procédé à une identification, les journaux d'enregistrement et l'archivage des accès permettent de suivre « à la trace » les déplacements d'une personne, notamment dans le cadre de la gestion des accès, des horaires et des flux.

En localisant un point de départ, un point d'arrivée, des points de passages, la biométrie permet de reconstituer *a posteriori* le parcours d'une personne, d'analyser la fréquence, la durée du parcours et d'estimer *a priori* les parcours à venir. Il s'agit donc aussi d'un outil de surveillance des déplacements. La convergence technologique de la biométrie avec la vidéo surveillance en est d'ailleurs le paroxysme.

• *Aller et venir : une liberté relative*

Pouvoir se déplacer librement et sans contrainte constitue encore aujourd'hui l'apanage des sociétés démocratiques. Le mur de Berlin en reste un symbole, tout comme de nos jours, le *jidar al-fasl al-'unsuri*[57], la barrière de séparation israélienne. En quoi la biométrie peut-elle constituer une

[56] Délibération n°2006-101 du 27 avril 2006

[57] « Mur de séparation raciale », également surnommée « mur de la honte ». Cette succession de murs, de tranchées et de portiques électroniques de près de 700 km est un édifice construit par Israël en Cisjordanie sous le nom de « clôture de sécurité » (security fence), dans le but officiel d'empêcher physiquement toute intrusion d'activistes palestiniens en Israël et de lutter contre le terrorisme.

entrave à la liberté de circulation ?

Large reconnaissance de la liberté de circulation. - De nombreux textes nationaux ou européens reconnaissent la liberté d'aller et venir et la liberté de circulation. Le Conseil constitutionnel a érigé la liberté d'aller et venir en principe à valeur constitutionnelle[58] et la rattache à l'article 66 de la Constitution pour la qualifier de liberté fondamentale[59]. Au plan européen, L'article 18 du Traité de Rome dispose que le marché intérieur comporte un espace sans frontières intérieures dans lequel la libre circulation des personnes et des services est assurée. Les articles 39 et 43 énoncent que la libre circulation des travailleurs est assurée à l'intérieur de la communauté. L'article 2 du protocole n°4 à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales indique que « *quiconque se trouve légalement sur le territoire d'un État a le droit d'y circuler librement* ». Enfin, la Charte des droits fondamentaux de l'Union Européenne reconnaît à tout citoyen de l'Union Européenne ainsi qu'aux ressortissants des États tiers résidant légalement sur le territoire européen, le droit d'y circuler et d'y séjourner librement.

Suppression des contrôles dans l'espace Schengen. - Le passage au marché unique s'est accompagné d'une suppression plus ample des frontières en Union Européenne et l'affirmation du droit des citoyens communautaires « *à vivre dans un espace de liberté, de sécurité et de justice* », l'activité économique n'étant plus un pré-requis. Les accords de Schengen du 14 juin 1985 ont posé le principe de la suppression du contrôle des frontières à l'intérieur de la Communauté, mis en œuvre par la Convention d'application du 19 juin 1990.

Caractère relatif de la liberté de circulation. La liberté de circulation n'a jamais eu vocation à se poser comme une liberté absolue. Historiquement, avant la reconnaissance de cette liberté, les restrictions étaient matérialisées par des droits de péages (abolis sous la Révolution), des passeports intérieurs (mis en place sus Louis XI), un carnet de circulation pour les sans domiciles fixes et un livret ouvrier qui servait de fiche policière d'immatriculation au 19ème siècle[60].

La reconnaissance de cette liberté au plan européen, dont la finalité était essentiellement économique, passait déjà par un encadrement. Le respect de la souveraineté des États aux fins de préservation de leur ordre public ou de leur sécurité intérieure justifie encore des dérogations fondées sur les exigences de police administrative, sanitaire, de propriété industrielle et commerciale, de clauses de sauvegardes, d'exigences impératives d'intérêt général. Aujourd'hui, on peut citer les limites relatives à la circulation et au stationnement des véhicules, aux mesures de sûreté et à des sanctions pénales, ou encore à la qualité de certaines personnes, à savoir les itinérants et les ressortissants des États tiers à l'Union Européenne, dont l'admission sur le territoire reste à la discrétion de l'État membre.

Ainsi, le traité d'Amsterdam prévoit en son article 61 « *qu'afin de mettre en place un espace de liberté de sécurité et de justice, le Conseil arrête des mesures visant à assurer la liberté de circulation des personnes, conformément à l'article 14, en liaison avec des mesures d'accompagnement directement liées à cette libre circulation et concernant les contrôles aux frontières extérieurs, l'asile et l'immigration* ».

De même, il est affirmé que la liberté de circulation des capitaux (transferts de devises, opérations financières) n'est possible qu'en contrepartie de mesures d'accompagnements visant à assurer une circulation dans un espace de sécurité. Cette libéralisation s'est accompagnée de nouvelles obligations. Par exemple, dans le cadre de la lutte anti-blanchiment et de la protection des

[58] Cons. Const. déc. n°79-107 DC du 12 juillet 1979

[59] Cons. Const. déc. n°92-307 DC du 25 février 1992

[60] Un bref historique de la carte d'identité, récemment publié par Libération en complément d'un article sur la carte d'identité biométrique, peut être trouvé en annexe de ce mémoire.

consommateurs, les prestataires de services financiers, aux termes de la directive 91/308 du 10 juin 1991, ont de nouvelles obligations : obligation d'identification des clients et de leurs relations d'affaires, obligation de conservation des documents d'identification, obligation de coopération avec les autorités judiciaires, obligation de vigilance, obligations de dénonciation.

Des contrôles sont également mis en œuvre en matière de produits, soumis à des contrôles sanitaires, des spécificités techniques, des critères de conformité, qui autorisent leur mise sur le marché.

La liberté de circulation des personnes n'a donc jamais été conçue comme une liberté absolue, comme beaucoup d'autres. Reste à savoir si les mesures de restrictions y afférentes sont justifiées.

• La traçabilité, une contrepartie à la liberté de circulation

Notion de traçabilité. La traçabilité se définit comme un outil de sécurité *a posteriori*, comprenant des usages et des mesures concrètes, utilisé aux fins d'expertises, de localisation, de conservation, d'arrestation, de remise de confrontation, de destruction, de prévention des risques.

La « traçabilité » est un vocable ordinairement utilisé pour le contrôle de la circulation des marchandises ou des capitaux. Mais il peut être aujourd'hui appliqué aux personnes, en raison du recours aux mêmes usages et quasiment aux mêmes mesures techniques, bien que nous n'en soyons pas encore à la boucle d'identification des bovins[61] pour les citoyens. Dans le monde numérique, on parle encore de « traçage électronique » sur Internet.

Un schéma d'organisation sociale ? - On peut certes estimer que les mesures de traçabilité, au premier rang desquelles la biométrie, constitue une entrave à la liberté d'aller et venir.

On peut aussi considérer que la traçabilité fonde un schéma d'organisation sociale. Elle dépasse les réponses sécuritaires traditionnelles fondées sur des contrôles entravants (édification de barrières, mesures d'isolement). La traçabilité instaure à l'inverse des contrôles *a posteriori*, permettant la constitution d'éléments de preuve et la mise en oeuvre de la responsabilité. Les contrôles opérés dans le cadre des différents systèmes d'information et de filtrage par listes noires, mis en oeuvre au niveau européen et décrit dans les pages précédentes, s'inscrivent dans la recherche de cet équilibre.

La création d'un espace de sécurité - une utopie ? - pourrait permettre d'imaginer un territoire où la liberté de circulation s'exercerait sans contrôles, mais il n'en est rien aujourd'hui. Partant de l'assertion que la liberté de circulation n'a de sens que dans un espace sécurisé, la traçabilité est donc une tentative de conciliation des deux impératifs. À ce titre, elle constitue une contrepartie à la liberté de circulation[62].

La question de la surveillance dans les entreprises privées et les administrations, et de l'installation de « pointeurs biométriques » en dehors d'impératifs de sécurité, pose en revanche davantage de questions, qui dépassent le cadre juridique.

---

[61] Depuis 1er septembre 2004, les animaux de compagnie doivent être présentés avec un passeport, une directive européenne prévoyant à terme d'implanter une puce électronique sous la peau de l'animal. Cela s'inscrit dans une tendance générale à la traçabilité dans l'espace Schengen, puisque les bovins sont « encartés » depuis les années 70. Les sanctions au défaut de conformité sont cependant plus radicales que pour les hommes, puisque les postes d'inspection frontaliers vétérinaires sont en droit de procéder à l'abattage de l'animal.

[62] Florence STIRLING-BELIN, *Traçabilité, liberté de circulation et Union Européenne,* Revue de droit prospectif R.R.J., 2005-1, n°107

Quelle nouvelle liberté est accordée aux salariés en contrepartie de la mise en place d'un dispositif de traçage biométrique ? Jusqu'à quel point peut-on utiliser la technologie pour observer les moindres faits et gestes des personnes sur le lieu de travail et les mettre ainsi sous pression psychologique ? Ces considérations sociologiques sont tristement illustrées par l'actualité.

§ 2. Un embryon de « biopouvoir » ?

• *Biométrie à l'école*

Un phénomène nouveau. - La généralisation de la biométrie touche aujourd'hui les écoles, collèges et lycées. Alors que ce domaine d'application en est encore à ses balbutiements en France, il est largement répandu dans d'autres pays, notamment au Royaume-Uni et aux États-Unis. Nul doute que ce phénomène touchera aussi la France, si l'on s'en réfère à la décision prise par la CNIL de prendre une autorisation unique relative à l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire[63]. Ce n'est pas extrapoler de dire que cette décision anticipe la multiplication des demandes d'autorisation par les établissements d'enseignement.

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.

Cette application ne devrait pas poser en soi de problème particulier par rapport aux autres traitements. Les risques et les garde-fous sont sensiblement les mêmes, et l'on se référera à la doctrine de la CNIL étudiée dans les pages suivantes.

Jeunesse et "*citoyenneté de l'Informatique et des Libertés*". - Il existe cependant une difficulté spécifique du fait notamment de l'âge des personnes concernées par le traitement. Constatant un certain relâchement de l'opinion publique face aux risques relatifs à la protection des données, le président de la CNIL, Alex TÜRK s'était prononcé en faveur d'un renforcement des moyens de communication à l'égard de la jeunesse, lors de la Conférence Internationale des Commissaires à la protection des données[64], les 2 et 3 décembre 2006 à Londres.

« *Il faut s'adresser aux jeunes générations qui, bien souvent, font preuve d'une grande indifférence vis-à-vis de ces questions, tant ils sont habitués à manipuler ces nouvelles technologies au fur et à mesure qu'elles font l'objet d'usages publics.*

Chacun comprend que l'usage précoce de cette technologie dépourvue de référence aux principes de la protection des données personnelles, ne favorise pas l'accès des jeunes à une citoyenneté de l'informatique et des libertés.

Il faut donc agir dans le secteur éducatif le plus tôt possible. Si l'on osait risquer cette image : il faut faire en sorte que dès l'instant où un enfant pose le doigt, pour la première fois, sur

[63] Autorisation unique n°AU-009 - Délibération n°2006- 103 du 27 avril 2006

[64] Conférence Internationale des Commissaires à la protection des données, Londres, 2 et 3 novembre 2006, Réflexions proposées par Alex Türk, président de la CNIL. http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/Pdt-initiativeConfLondres06112006.pdf

un clavier d'ordinateur, il intègre à son apprentissage l'impératif de la protection des données ».

Fascination. - Le chemin est encore long. Une étude[65] menée par l'Institut National des Télécommunication sur l'introduction de la biométrie à l'école, donne un éclairage sur ce que peut être la réaction de collégiens face à l'introduction de la biométrie pour l'accès à la cantine.

Cette réaction se situe entre la fascination, le scepticisme au regard de la fiabilité technique du dispositif et l'acceptation de ce qui apparaît comme une extension de l'autorité parentale. De manière générale, si l'idée de transgression subsiste, la légitimité du procédé n'est jamais remise en question par les élèves.

Par ailleurs, une partie croissante du grand public semble s'attacher à l'aspect ludique de cette technologie, à la fois dénoncée et relayée par l'imaginaire des oeuvres de science-fiction. Le succès considérable de l'exposition « Biométrie, le Corps identité[66] » à la Cité des Sciences de la Villette confirme cette tendance. Il suffit de constater que les installations réservées aux enjeux éthiques étaient désertées et qu'on se disputait les places devant les capteurs biométriques installés tout au long du parcours en libre utilisation. Personne n'hésitait d'ailleurs à s'enrôler à l'entrée de l'exposition pour pouvoir être reconnu par les machines exposées.

Un panoptique des élèves. - L'ambition du principal du Collège Joliot-Curie de Carqueiranne est claire : le recours au procédé biométrique, associé à d'autres dispositifs comme le système d'alerte des absences et retards par SMS aux parents et le contrôle sécurisé en ligne des notes, doit permettre d'assurer une « *transparence absolue* ».

Selon les auteurs, de manière paradoxale, l'objectif est à la fois répressif et humaniste. Il s'agit de savoir en permanence et en temps réel ce que fait et ce que ne fait pas un élève.

Les auteurs du rapport n'hésitent pas y voir des éléments de comparaison avec le panoptique du philosophe Jeremy BENTHAM, l'idée d'une prison soumise à l'omniscience invisible de l'autorité, ou du biopouvoir de Michel FOUCAULT, c'est-à-dire très schématiquement, l'investissement du corps par le pouvoir au moyen des techniques disciplinaires de dressage.

Il se dégage de cette étude qu'indirectement, les directeurs d'établissement participent au développement d'une culture de l'acceptation chez les enfants, dès le plus jeune âge, au renoncement à toute forme d'esprit critique face aux technologies menaçant les libertés. D'une certaine manière, ils font échos aux méthodes décrites par les industriels dans le tristement célèbre Livre Bleu[67] du GIXEL visant conditionner les populations à accepter les technologies de contrôle.

« La sécurité est très souvent vécue dans nos sociétés démocratiques comme une atteinte aux libertés individuelles. Il faut donc faire accepter par la population les technologies utilisées et parmi celles-ci la biométrie, la vidéosurveillance et les contrôles. Plusieurs méthodes devront être développées par les pouvoirs publics et les industriels pour faire accepter la biométrie. Elles devront être accompagnées d'un effort de convivialité par une reconnaissance de la personne et par l'apport de fonctionnalités attrayantes : éducation dès l'école maternelle, les enfants utilisent cette technologie pour rentrer dans l'école, en sortir, déjeuner à la cantine, et les parents ou leurs

---

[65] Sylvie CRAIPEAU, Gérard DUBEY, Xavier GUCHET, *La biométrie, usage et représentations*, février 2004, Projet Incitatif Get2003, Institut national des Télécommunications.
http://perso.orange.fr/perso.web/hebergement/biometrie/doc/INT_GET2003.pdf

[66] http://www.cite-sciences.fr/francais/ala_cite/expositions/biometrie/index2.php

[67] Livre Bleu du GIXEL, Groupement des industries de l'interconnexion des composants et des sous-ensembles électroniques, *Grand programmes structurants, Propositions des Industrie électroniques et numériques*, juillet 2004.
http://perso.orange.fr/perso.web/hebergement/biometrie/doc/Livre_bleu_GIXEL.pdf

représentants s'identifieront pour aller chercher les enfants.

(extrait de la version non-censurée)

Soubresauts de résistance. - Certains faits divers tenant de la désobéissance civile - ou d'une forme de résistance - permettent néanmoins d'avoir une vision moins pessimiste du tableau. Bien que poussée à l'extrême, c'est bien par conscience des aspects liberticides de la biométrie que des élèves du lycée de Gif-sur-Yvette ont détruit des bornes biométriques installées dans leur établissement pour contrôler l'accès aux cantines.

Le moyen de défense a évidemment été rejeté par le Tribunal d'Evry dans une décision du 17 février 2005, mais les « sauvageons » en question étaient soutenus par l'ensemble des figures intellectuelles anti-biométrie. Si l'acte est condamnable, il reflète néanmoins que la « *citoyenneté de l'informatique et des libertés* » meurt mais ne se rend pas, comme en témoigne également le développement de réseaux militants en ligne.

• Vidéosurveillance et biométrie

Une technologie en phase de développement. - La reconnaissance faciale et par l'iris des personnes par vidéo surveillance est une technologique encore en phase de développement mais promise à un avenir certain. Elle permet la captation des données biométriques à distance, à la volée, de manière invisible et sans consentement préalable. Ces données peuvent ensuite être utilisées pour vérifier qu'une personne ne figure pas dans une liste noire. L'identification de terroriste dans les aéroports est évidemment une des premières applications envisagées.

Ainsi, un programme de recherche "Techno Vision" et IV2, autorisé par la CNIL dans une délibération 2007-006 du 18 janvier 2007 a été mis en œuvre par l'université d'Evry Val d'Essonne. Soutenu par les ministères de la Recherche et de la Défense, le projet est destiné à évaluer les algorithmes de reconnaissance du visage et de l'iris par la vidéo, mis au point dans des laboratoires de recherche. Une base de données multimodale des quelques 1000 participants a été constituée et peut être communiquée à des laboratoires étrangers, dans le cadre de conventions de recherche, comportant des clauses de protection des données.

Avis du Conseil de l'Europe. - Le Conseil de l'Europe s'est prononcé sur les implications de la biométrie associée à la vidéosurveillance. Pour le Conseil, il n'est pas exclu que la technique permette par exemple de comparer secrètement le visage des individus dans les zones publiques à une base biométrique de personnes recherchées. L'enrôlement pourrait consister à prendre des photos d'un criminel après son arrestation. Il s'agirait alors d'un traitement déloyal. À ce titre, il ne devrait être permis qu'en adoption d'une loi décrivant précisément les exceptions admises au traitement loyal, en application des critères de l'article 9 de la Convention.

Pour le Conseil, « *une surveillance secrète générale du public, même prévue par la loi, ne serait ni conforme aux dispositions de la Convention européenne des droits de l'homme, ni à celles de la Convention 108.* »

Consensus. - De fait, la vidéosurveillance biométrique, en ce qu'elle ne nécessite même plus la coopération des personnes concernées pour la captation des données biométriques, stigmatise des dangers particuliers, certainement plus importants encore que la biométrie traditionnelle.

Les récents attentats déjoués au Royaume-Uni grâce système de vidéosurveillance semblent, à tort ou à raison, avoir convaincu l'opinion de la nécessité de mettre en place tous les outils efficaces au regard de la lutte contre le terrorisme. La question des libertés individuelles est le plus souvent éludée par la peur que génèrent les risques d'attaques, et semble faire de moins en moins d'écho au sein de la population., au point qu'Alex TÜRK puisse parler d'« *endormissement* » des

citoyens.

SECTION 2. Portée des risques au regard des autres droits de l'homme

SOUS-SECTION 1. La protection de la personne humaine

La plupart des études relatives à la biométrie affirment que cette technologie comporte des risques au regard de la dignité de la personne, de l'intégrité du corps humain, voire de l'identité humaine. Il convient cependant d'examiner ce que signifient juridiquement ces notions et en quoi les dispositifs biométrique sont susceptibles de constituer une atteinte à ses principes.

§ 1. L'intégrité du corps humain

• *Une « mise en cause » relative du corps humain*

Les données biométriques sont collectées à partir du corps humain. Or, le corps humain fait l'objet d'une protection juridique. Les techniques biométriques tombent-elles nécessairement sous le coup de cette protection ?

Une "mise en cause" de principe selon la jurisprudence. - Le TGI de Paris[68] semble répondre par l'affirmative : « *Son utilisation met en cause le corps humain et porte ainsi atteinte aux libertés individuelles* ».

Ainsi, dans une formule générale, le tribunal semble volontairement ignorer le principe de neutralité des technologies, affirmant que l'utilisation de la biométrie porte atteinte aux libertés individuelles, dès lors qu'elle met en cause le corps humain. Certains auteurs ont vu dans cette formulation une application par le juge judiciaire du principe de précaution. Le paradoxe de la décision veut que les juges constatent la légalité du recours à la biométrie - les formalités préalables auprès de la CNIL et du comité d'entreprise avaient été respectées - tout en avançant l'idée d'une illégalité de principe de la biométrie au regard des libertés.

Pourtant, la simple « mise en cause » du corps humain n'est pas sanctionnée par la loi. Le chapitre 2 du Code civil est ainsi consacré à la protection du corps humain, ses dispositions (articles 16 à 16-9) étant d'ordre public. Aux termes du Code civil, chacun a droit au « *respect de son corps* », le corps humain étant « *inviolable* » (article 16-1). Le juge peut prescrire toutes mesures propres à empêcher ou faire cesser « *une atteinte illicite au corps humain*" ou « *des agissements illicites portant sur des éléments ou des produits de celui-ci* » (article 16-2). Il ne peut être porté « *atteinte à l'intégrité du corps humain* » qu'en cas de nécessité médicale pour la personne ou à titre exceptionnel dans l'intérêt thérapeutique d'autrui (article 16-3). De même, à titre d'illustration, la loi pénale se réfère aux « *atteintes à l'intégrité physique ou psychique de la personne* » que constituent les tortures et actes de barbarie, les violences, les menaces, les agressions sexuelles.

On peut dès lors se demander ce qui a motivé les juges à adopter une formulation qui n'est pas visée par les textes.

Absence d'atteinte à l'intégrité du corps humain. - L'atteinte à l'intégrité du corps humain est en général réalisée par la violation d'une frontière au-delà de laquelle on considère le corps atteint. Généralement, cette frontière est plus au moins assimilée à la surface de la peau. La transgression de la surface de la peau sans consentement permet de qualifier l'atteinte à l'intégrité

[68] TGI Paris, 19 avril 2005 , Comité d'entreprise d'Effia Services c. Fédération des syndicats Sud Rail, n° 05/00382 http://perso.orange.fr/perso.web/hebergement/biometrie/doc/TGIPARiS_250405.pdf

du corps humain.

En pratique, les capteurs utilisés pour acquérir de l'information biométrique ne touchent que la surface du corps. Certains dispositifs peuvent même opérer à distance, comme le fait la reconnaissance du visage par biométrie vidéo. L'analyse de l'ADN ne nécessite pas forcément une prise de sang, puisqu'elle peut être réalisée à partir d'un cheveu, d'un échantillon de salive, de cellule de la peau.

On réservera l'hypothèse de la biométrie en tant que facteur de risque, celui d'inciter les criminels à croire que la mutilation d'un doigt d'une personne habilitée pourrait lui permettre d'accéder à des zones qui lui sont interdites. La majorité des systèmes actuels, et la totalité des systèmes futurs, intègrent ou intégreront des dispositifs "anti-doigt mort", permettant au système de détecter l'afflux sanguin, la température du corps... Il s'agit là d'un cas d'école, qui espérons-le sera amené à disparaître.

En dehors de cette hypothèse, l'intégrité physique du corps paraît peu atteinte. En réalité, comparées à des technologies plus anciennes qui extraient de l'information à partir du corps, les méthodes informatiques produisant des données corporelles sont peu intrusives, pour la majorité d'entre elles. Dans le domaine médical, la précision et le niveau de détail d'une radiographie remplacent avantageusement l'autopsie ou une intervention chirurgicale. On admet cependant ces méthodes invasives lorsqu'elles sont nécessaires à la défense des intérêts vitaux de la personne.

L'usage de la biométrie n'a pas besoin de ce type de justification, mais on s'aperçoit au final que la numérisation du corps ne porte pas plus atteinte au corps qu'une photographie. Il suffit de réserver les cas de dysfonctionnement des dispositifs biométriques (électrocution, brûlure, lésions) qui pourraient éventuellement survenir. Dans ce cas, c'est la responsabilité présumée du fait des produits défectueux (articles 1386-1 à 1388-18 du Code civil) ou du fait des choses que l'on a sous sa garde (article 1384 du Code civil) qui aura à s'appliquer pour indemniser les victimes.

Difficultés de qualification. - Les juges de cette affaire ont cependant que la biométrie pouvait difficilement rentrer dans les tiroirs juridiques du droit positif. Ainsi, ils n'ont pas cherché à soutenir l'idée que la biométrie portait intrinsèquement atteinte à l'intégrité du corps humain. Ils ont au contraire soigneusement évité de le faire. Pour ne pas employer le terme d'atteinte, inapplicable en l'espèce, ils s'en sont référés à la notion ambiguë de « mise en cause », expression dont le champ est tellement large, qu'en fait, elle ne correspond à rien de précis. À s'en tenir à cette définition, de nombreux objets et gestes de la vie quotidienne « mettent en cause le corps humain », sans qu'on puisse en déduire une atteinte de principe à l'intégrité du corps humain. Le fait de conduire une voiture ou d'utiliser un couteau « met en cause » le corps humain, sans que l'on considère que cela constitue une atteinte aux libertés individuelles.

La formulation des juges reflète donc cette ambiguïté. La biométrie n'est pas anodine au regard du corps humain, mais ne constitue pas à proprement parler une atteinte à l'intégrité du corps humain. Comment dès lors interpréter cette « mise en cause » ?

Éléments d'interprétation. - Une décision de la Cour EDH peut donner un premier élément d'interprétation. Dans un arrêt *Salvetti c/ Italie* du 9 juillet 2002, la Cour Européenne a considéré qu'une vaccination non volontaire constituait une ingérence dans le droit au respect de la vie privée, dont la sphère recouvre l'intégrité physique et morale d'une personne. Un autre élément d'interprétation peut être pris en compte du fait de la protection du corps pris en image, ou le droit à l'image représentant le corps, sanctionné par plusieurs arrêts, à propos de la publication de clichés

du corps d'une personne assassinée[69] et de photographies d'un mannequin dénudé[70].

La confrontation de ces différents arrêts montre qu'il existe une zone grise, au carrefour de l'intégrité physique des personnes, du droit au respect de la vie privée, voire du droit à l'image, dans laquelle flotte la biométrie. En l'absence d'autres arrêts relatifs à la biométrie, on se gardera donc de donner à cette décision une portée trop générale.

Certains auteurs en appellent à une redéfinition de certaines notions, redéfinition qui pourrait permettre de donner corps à l'intuition des juges sur la mise en cause du corps humain par la biométrie.

• L'intégrité du corps informatisé

Réification du corps. - Le Conseil de l'Europe estime que la biométrie peut susciter des réactions différentes, relevant que certains pourront éprouver une « *résistance psychologique à l'idée que le corps humain soit utilisé comme une source d'information (...) ou analysé par une machine* », cette résistance pouvant dépendre de facteurs sociaux, culturels, religieux propres à la personne.

Le Conseil poursuit en notant que certains peuvent exprimer une inquiétude face à la « *banalisation sans considération du corps humain* » et que « *l'attitude à l'égard de l'utilisation du corps humain par la biométrie pourrait également évoluer avec le temps* ». Ce que le Conseil semble mettre en avant, c'est l'idée du corps humain, comme quelque chose de sacré. Or, il est aujourd'hui courant de parler de réification, ou d'informatisation du corps humain, tendance que la biométrie ne fait qu'accélérer.

Certains auteurs[71] ont mené une réflexion sur les conséquences de l'utilisation de l'informatique sur la définition d'un corps « *lisible par la machine* ».

Comme il a été décrit, l'inviolabilité du corps dépend des frontières que l'on entend protéger, au-delà desquelles on considère le corps comme atteint dans son intégrité. Il s'agit généralement de la surface de la peau. Cependant, la délimitation de cette frontière est plus délicate qu'il n'y parait. Il existe là aussi des « zones grises », comme les orifices, les secrétions, le sang, les gamètes… Ainsi, les éléments du corps font l'objet d'une protection particulière. Au final, l'exacte nature des frontières du corps humain est en fait essentiellement une question de culture et de conventions.

Reconstitution numérique du corps physique. - Une nouvelle zone grise peut apparaître lorsqu'on prend en considération les transcriptions des caractéristiques corporelles en information exploitable électroniquement. La mise en relation ou le rassemblement des données du corps, à savoir des données alphanumériques médicales, des radiographies, des échantillons, éventuellement en trois dimensions, d'empreintes digitales, de la morphologie de la main, du réseau veineux, de l'iris, du visage, de l'ADN, des échantillons physiques de sang ou de gamètes, peuvent servir de base à une reconstitution numérique du corps physique.

On peut considérer que cette mise en relation d'informations corporelles multiformes donne au corps une existence virtuelle, ce dernier devenant explorable à distance, transférable, dissocié de l'espace et du temps du corps physique.

---

[69] Civ.1ère, 20 décembre 2000

[70] Cour d'Appel de Paris, 10 février 1999, 14e ch. *A, Lacambre c/ E. Hallyday.*

[71] Irma VAN DER PLOEG, Biometric Identification technology : Ethical Implications of the Informatisation of the Body, draft march 05, BITE policy Paper 1.
http://perso.orange.fr/perso.web/hebergement/biometrie/doc/IRMA_VANDERPLOEG_Informatisation.pdf

Exploration virtuelle du corps. - Ainsi, le « rendu digital » du corps sous la forme de fichiers d'ordinateurs, de codes, de modèles enregistrés, d'images dynamiques, et de paquets d'informations permet des formes de traitement, d'explorations, d'analyse de l'intimité qui ressemblent à une véritable recherche corporelle. Si le corps acquiert une existence virtuelle, et qu'il est susceptible d'être ainsi atteint dans son intégrité, le principe d'inviolabilité du corps par référence à la surface de la peau ne suffit pas à protéger ce corps, redéfinit par les usages qui en sont fait. La protection de l'intégrité de ce corps informatisé relèvera uniquement d'une protection technique, de politique d'accès et des matrices d'habilitation, en dehors de tout contrôle par le principal intéressé.

§ 2. La dignité de la personne humaine

• *Qualification juridique de l'atteinte à la dignité*

Bien que les risques de la biométrie au regard de la dignité de la personne humaine sont quasi-systématiquement évoqués par les documents d'analyse, il n'existe à l'heure actuelle que très peu d'études sur les conséquences réelles de la biométrie sur la dignité de la personne humaine, d'un point de vue juridique. Ainsi, la dignité de la personne figure parmi les enjeux relevés par les Commissaires à la protection des données au regard de la biométrie et par le Conseil de l'Europe, dans son rapport sur l'applicabilité de la Convention 108 aux données biométriques.

Un « sentiment » d'atteinte à la dignité. - Le Conseil relève que « *la collecte de ces données pourrait être ressentie comme une atteinte à la dignité humaine* ». Cependant, le sentiment que peut éprouver une personne sur un procédé biométrique n'a pas d'incidence sur la qualification d'un fait juridique. Il n'est d'ailleurs par rare que certaines personnes aient un sentiment « *positif* » sur des pratiques qui portent atteinte à leur dignité mais pour lesquelles elles ont donné leur consentement[72]. Le fait de caractériser une atteinte à la dignité humaine par la biométrie ne dépend donc pas de l'idée que l'on se ferait de la biométrie.

Le Conseil de l'Europe a cependant une approche nuancée s'écartant d'une stigmatisation *a priori* de la biométrie. Le Conseil affirme que l'utilisation d'un procédé biométrique doit effectivement s'apprécier au regard de la protection du corps humain et de la dignité humaine, des finalités du système, de la proportionnalité aux intérêts en jeu et renvoie au responsable du traitement le soin de prendre en compte ces considérations lors du choix de la solution technique.

Portée de la protection en droit civil et en droit pénal. - Le droit civil interdit toute atteinte à la dignité, au titre du respect de la primauté de la personne (article 16 du Code civil). Il découle de cet article la protection du droit à la vie en application de la Convention EDH (article 2), l'interdiction des peines ou traitements dégradants ou inhumains (article 3), l'interdiction des pratiques d'esclavage et de servitude (article 4). Les juridictions françaises y intègrent également le droit au logement[73], le droit à l'image[74], l'interdiction des humiliations[75] et des discriminations[76].

Le Code pénal sanctionne dans un Titre II sur les atteintes à la personne humaine : atteintes la vie (chapitre I), à l'intégrité physique ou psychique (chapitre II), aux libertés (chapitre IV), à la dignité (chapitre V), à la personnalité (chapitre VI) aux mineurs et à la famille (VI).

---

[72] CE, Assemblée, 27 octobre 1995, Commune de Morsang-sur-Orge, affaire du « lancer de nain »
[73] Cons. const. 19 janvier 1995
[74] Civ. 1ère, 20 décembre 2000
[75] Crim. 10 janvier 1995
[76] CE, 9 octobre 1996

En ce qui concerne la dignité de la personne, le Code pénal sanctionne les discriminations, la traite des êtres humains, le proxénétisme, le recours à la prostitution de mineurs, l'exploitation de la mendicité, les agressions ou atteintes sexuelles, les conditions de travail ou d'hébergement contraires à la dignité, le bizutage, les atteintes au respect dû aux morts.

Ainsi, à moins de considérer l'usage de procédés biométriques en entreprise comme des conditions de travail contraires à la dignité des salariés, il paraît peu pertinent de placer l'identification biométrique aux côtés des situations décrites précédemment.

• La protection contre les discriminations

Cependant, le Code pénal sanctionne également au titre des atteintes à la dignité de la personne, les actes de discrimination opérés entre les personnes physiques. Il s'agit de discriminations opérées sur des personnes *« à raison de leur origine, de leur sexe, de leur situation de famille, de leur grossesse, de leur apparence physique, de leur patronyme, de leur état de santé, de leur handicap, de leurs caractéristiques génétiques, de leurs moeurs, de leur orientation sexuelle, de leur âge, de leurs opinions politiques, de leurs activités syndicales, de leur appartenance ou de leur non-appartenance, vraie ou supposée, à une ethnie, une nation, une race ou une religion déterminée* ».

Ce texte fait d'ailleurs écho à l'article 8 de la loi de 1978, qui interdit – avec certaines exceptions - les traitements de données à caractère personnel faisant apparaître « *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 sexuelle de celles-ci* ».

• La décision biométrique : un acte discriminatoire ? - Le Code pénal interdit donc les actes discriminatoires. Or, l'identification biométrique est précisément un processus décisionnel fondé sur la discrimination, puisqu'elle vise à « *différencier, en vue d'un traitement séparé, un élément des autres ou en l'identifiant comme distinct* ».

Par ailleurs, ce processus décisionnel peut être fondé sur des caractéristiques génétiques, expressément visées par le texte, ou sur des caractéristiques révélant indirectement la race (reconnaissance faciale, empreintes digitales) ou le handicap (reconnaissance de l'iris, de l'empreinte digitale, de la morphologie de la main).

Ainsi, parmi les actes discriminatoires visés par le Code pénal figure le refus de fournir un bien ou un service à une personne « de race arabe »[77] ou à des personnes handicapées[78]. Par analogie, on peut imaginer une borne biométrique, située à l'entrée d'une boîte de nuit, analysant les caractéristiques des personnes et interdisant systématiquement l'accès à des personnes d'origine étrangère.

Risque d'anthropomorphisme. - Est-ce à dire que la biométrie constitue automatiquement une atteinte à la dignité de la personne, en tant que pratique discriminatoire ? Certes, les actes visés par la jurisprudence ne sont pas éloignés des décisions « prises » par les systèmes biométriques.

Mais celles-ci n'émanent évidemment pas de la machine elle-même. La décision prise par un dispositif biométrique ne fait que sous-tendre une « politique » mise en place par l'administrateur du système. À moins de procéder à un anthropomorphisme inopportun, la décision biométrique est purement technique et elle ne fait que mettre en œuvre un cadre décisionnel défini par du

[77] TGI Strasbourg, 21 novembre 1974
[78] TGI Nantes, 1er mars 1990

responsable. La réponse déterministe de la machine ne sera que la conséquence d'une « logique » voulue par l'administrateur. Or la décision doit « *émaner d'une personne physique ou morale* » selon le Code pénal.

Il résulte de ce qui précède, que les responsables d'un traitement de données biométriques ont entre les mains un instrument dédié à la discrimination, qui peut se fonder sur des données sensibles, susceptible d'entraîner des effets de droits, et dont la logique mise en place par eux peut constituer un acte de discrimination.

Cependant, si la biométrie peut être une technologie facilitant les atteintes à la dignité humaine, rendant cette politique discriminatoire totalement invisible aux intéressés, le Code pénal sanctionne les actes eux-mêmes et non les moyens utilisés pour perpétrer ces discriminations. La biométrie peut donc faciliter le travail d'une personne mal intentionnée, mais il paraît difficile de dire qu'elle porte intrinsèquement atteinte à la dignité humaine.

Il résulte de ce qui précède, que l'évocation systématique des risques de la biométrie au regard de la dignité humaine, en termes abstraits et sans qualification juridique, mériterait d'être davantage étayée. En pratique, on voit mal en quoi la biométrie est susceptible de porter atteinte à la dignité des personnes, au même titre que l'esclavage ou les traitements inhumains. Sur le plan de l'analyse, il s'agit d'une impasse, ou d'une hypothèse qui reste éminemment théorique, à moins d'étendre indéfiniment la notion de dignité à des situations relativement dérisoires en comparaison de celles visées par le Code pénal.

Il découle de ce raisonnement une très classique application du principe de neutralité des technologies et la nécessité d'encadrer les usages et prévenir les abus. Mais il serait illusoire de vouloir condamner la biométrie, comme technologie portant intrinsèquement atteinte à la dignité humaine … à moins d'ériger le « sentiment » d'une atteinte, en atteinte qualifiée.

Enfin, il existe d'autres notions qui sont susceptibles de fonder l'analyse des procédés biométriques. Ainsi, des dispositions particulières figurent au Code pénal du fait des « *résultant de l'examen de ses caractéristiques génétiques ou de l'identification par ses empreintes génétiques* »[79], suivant ainsi les atteintes aux droits de la personne « *résultants des fichiers ou des traitements informatiques* »[80] en application de la loi informatique, fichiers et libertés. Ces dispositions figurent au chapitre IV sur les « *atteintes à la personne* » et non au chapitre V sur les « *atteintes à la dignité* ».

§ 3. La protection de l'identité humaine

• *Un besoin d'identité renouvelé*

Mondialisation. - Le développement de la biométrie en tant qu'outil d'identification rationalisée peut s'expliquer par plusieurs facteurs. La mondialisation s'est accompagnée d'une multiplication des déplacements des personnes, et des biens, particulièrement en Europe avec la suppression des frontières, nécessitant en contrepartie l'identification des personnes dans le cadre de la lutte contre le terrorisme et la criminalité. La lutte contre la fraude aux titres d'identités est également à placer dans ce contexte. Par ailleurs, le contrôle de l'immigration nécessite aujourd'hui l'identification des demandeurs d'asile et de visa, pour connaître l'État compétent d'une demande.

L'anonymat sur Internet. - La démocratisation d'Internet constitue le paroxysme

[79] Articles 226-25 à 226-30 du Code pénal.
[80] Articles 226-16 à 226-24 du Code pénal.

(provisoire ?) de cette évolution. Le principe veut que son utilisation puisse se faire de manière anonyme. Il existe de fait, sur Internet, une liberté d'aller et venir anonymement, au point que certains considèrent qu'il est le lieu d'exercice idéal du « droit à l'identité multiple ». Internet est en effet le royaume du pseudonyme, de l'avatar et du nom d'utilisateur. Il est possible de mener sur le réseau plusieurs vies virtuelles et d'avoir plusieurs identités, comme en témoigne le succès du jeu « massivement multi-joueurs » *Second Life*[81], avec pour seul élément tangible, l'identité de l'ordinateur, c'est-à-dire une adresse IP.

On se gardera cependant d'avoir une vision naïve ou utopique d'un Internet anonyme, en précisant qu'en pratique, la surveillance est omniprésente sur le réseau, mais ces considérations pourraient à elles seules faire l'objet de plusieurs ouvrages.

Reste que le lien final entre une personne physique déterminée et un internaute naviguant d'un site à l'autre, se livrant à des transactions bancaires ou financières, à des recherches scientifiques, à des actes répréhensibles, au téléchargement illégal d'oeuvres multimédia, à la participation à des forums, est en théorie impossible à établir de manière fiable. Comment affirmer que la personne avec qui je dialogue sur le logiciel MSN n'est pas en réalité un petit malin qui se fait passer pour quelqu'un d'autre ?

Cet état de fait a incité le secteur public et le secteur privé à trouver des solutions d'identification plus fiables, notamment pour sécuriser les transactions financières ou les téléservices. Le recours à la signature électronique, techniquement fiable mais mal perçue, s'inscrit dans cette démarche. Il ne s'agit pourtant que d'une étape vers une généralisation de l'identification sur le réseau.

Il existe en effet une volonté forte de refonder l'identité sur ce qui est intangible, en réaction à une configuration sociale totalement bouleversée par les réseaux. Parce que les éléments corporels ne peuvent être transférés ou subtilisés, sauf chirurgie ou atteinte à l'intégrité du corps, on considère par comparaison aux autres techniques qu'elle offre dans l'absolu un haut degré de sécurité.

La fin de l'anonymat sur Internet. - Ainsi, il n'est pas impossible qu'à terme, l'idée d'anonymat sur Internet fasse long feu. L'idée d'une carte d'identité électronique, comportant des éléments de signature électronique et d'identification biométrique, destinées notamment aux téléservices de l'administration, permet d'envisager une régulation des activités numériques par le biais de l'identité. Le fait de pouvoir lire sa messagerie pourrait un jour requérir qu'on fournisse son état civil, certifié par une donnée biométrique. Le procédé a déjà été mis en place par certaines sociétés de services financiers à distance, notamment la société Bloomberg.

En effet, ce qui a justifié dans le monde physique le recours à la biométrie peut être grossièrement résumé par la lutte contre le terrorisme. Or, on se réfère aujourd'hui de plus en plus au cyberterrorisme, comme on se réfère depuis plusieurs années à la cybercriminalité. Pourquoi les autorités ne se serviraient pas de la même justification - la lutte contre le cyberterrorisme - pour imposer dans le monde virtuel les mesures de sécurité qui ont cours dans le monde réel ?

• L'objectivation de l'identité

Protection de l'identité « *humaine* ». - Les conséquences de l'automatisation de la preuve de l'identité, non plus simplement cantonnée à l'enquête judiciaire, sont difficiles à évaluer. Est-ce un hasard si la loi informatique, fichiers et libertés en son article 1er, précise que l'informatique « *ne doit pas porter atteinte à l'identité humaine* » ?

[81] Seconde Vie.

Cette disposition ne dissipe pas l'extrême ambivalence de l'expression « *identité humaine* ». Paul RICOEUR opère une distinction entre deux types d'identité : une identité objective (« idem ») qui correspond à ce qui est permanent et intangible chez un individu, comme le groupe sanguin, la filiation, par opposition à une identité subjective (« ipse »), fluctuante, en perpétuelle construction.

Quelle conception de l'identité ? - Or, on ne sait pas quelle conception de l'identité la Loi Informatique et Libertés entend défendre. On sait en revanche que la loi défend l'identité en ce qu'elle est « *humaine* ». L'humanité de notre identité découle-t-elle des caractéristiques tangibles et objectives de notre corps ? Dans ce cas, cette identité matérialiste ne nous distingue finalement pas des autres organismes vivants aux propriétés chimiques et physiques définies.

À l'inverse, notre identité humaine découle-t-elle d'une conception existentialiste - donc humaniste[82] - récusant toute forme de prédétermination, et réaffirmant au contraire le postulat que nous sommes ce que nous souhaitons être ?

Si l'on considère que ce qui fait l'humanité de notre identité est une conception de l'homme libre, et donc non prisonnier de ses caractéristiques corporelles, génétiques, est-ce cette identité que la loi informatique, fichiers et libertés entend protéger ?

Déséquilibre. - En partant du principe que la loi défend l'humanité de notre identité, face à une tendance endémique à l'objectivation, alors la biométrie remet en cause cette conception humaniste de l'identité. La biométrie renouvelle, généralise, et légitime l'idée d'une identité objective, intangible, irrévocable, et à l'intérieur de laquelle l'homme se trouve piégé, piégé dans son propre corps par ceux qui en ont fait un outil au service de leur pouvoir. Comment ne pas penser à l'histoire de Jean VALJEAN[83], identifié et fiché à vie comme un criminel, alors que ce dernier, forcément sous un faux nom, aura passé le reste de sa vie à faire le bien autour de lui.

La biométrie fait nettement peser la balance de ce côté, phénomène dont il est difficile de mesurer les effets à long terme. Cependant, cette tâche n'est plus du ressort exclusif du juriste. Les récents débats politiques sur le caractère déterministe de la génétique pour la prévention des infractions sexuelles, tout comme les théories déjà anciennes fondées sur la distinction de l'espèce humaine en races, donnent aussi une idée de ce qu'on peut attendre de l'évolution de l'identité humaine, en tant que source d'information objective.

SOUS-SECTION 2. Le droit à un procès équitable

Envisager l'identification biométrique sous l'angle du droit au procès équitable peut apparaître surprenant. Cependant, le droit au procès équitable, garanti aux termes de l'article 6§1 de la Convention Européenne des Droits de l'Homme, constitue une grille d'analyse intéressante au regard de la biométrie pour plusieurs raisons.

Loyauté de la collecte de la preuve. - Le droit au procès équitable (6 § 1) comporte d'abord un principe de loyauté dans la collecte de la preuve susceptible d'intéresser le domaine de la biométrie. L'archivage des données d'identification peut constituer un élément de preuve, au même titre qu'un écrit électronique, une séquence de vidéosurveillance, des écoutes téléphoniques. Ainsi,

[82] *L'existentialisme est un humanisme*, Jean-Paul SARTRE, 1946.

[83] Dans le roman de Victor Hugo, un homme arrive à Montreuil-sur-Mer et sauve deux enfants d'un incendie. Il est alors très respecté et, de ce fait, on ne pense pas à lui demander ses papiers d'identité. Cet homme, qui dit s'appeler « le père Madeleine », deviendra par la suite d'abord un industriel, puis maire de la ville, où il fait construire deux écoles. Il sera un jour rattrapé par son identité objective d'ancien bagnard et d'évadé de prison.

la CEDH a pu se prononcer sur le caractère loyal de la collecte d'un enregistrement téléphonique[84] : « *La Cour attache aussi du poids à la circonstance que l'enregistrement téléphonique n'a pas constitué le seul moyen de preuve retenu pour motiver la condamnation.* ».

Principe d'égalité des armes. - Le droit au procès équitable implique ensuite un principe d'égalité des armes. Or, les données de traçabilité biométrique ne sont à l'origine accessibles qu'à l'administrateur, au propriétaire, ou au responsable du système biométriques. Ainsi, à propos d'une procédure d'expropriation, la Cour de Cassation a estimé que l'accès privilégié aux informations contenues au fichier immobilier dont bénéficiait le Commissaire du gouvernement constituait un « *déséquilibre incompatible avec le principe de l'égalité des armes* »[85].

Sous l'appellation de « droit au procès équitable », cette section a donc pour objet de situer la biométrie au regard du droit et de la pratique probatoire, étant admis que les règles procédurales ont vocation à protéger le justiciable. Il sera donc question des systèmes de présomption de fiabilité de la preuve électronique, de liberté d'appréciation du juge face à la preuve scientifique, ou encore des décisions automatiques visées par la loi informatique, fichiers et libertés.

§ 1 Présomptions de fiabilité et automatisme probatoire

• *Perfectionnisme de l'identification biométrique*

La rationalisation de la preuve de l'identité s'est manifestée très tôt avec la technique d' « encartement ». Elle est devenue scientifique dans le cadre des enquêtes judiciaires, s'est démocratisée avec la diffusion des cartes de crédit pour la vérification de l'identité bancaire. Elle s'est encore renouvelée avec l'apparition des réseaux numériques et la signature électronique. Au fil du développement des technologies, la place de l'intervention humaine est apparue de moins en moins indispensable. Il ne s'agit plus de protocoles formalisés entre État, partenaires économiques et sujets de droits mais d'analyses de probabilité, de comparaisons numériques, de programmes informatiques.

Une présomption technique. - Cette évolution, de nature perfectionniste, part de la présomption que la machine est suffisamment infaillible pour qu'on puisse la substituer à l'appréciation humaine. Si elle n'est pas dénuée de sens, cette fiabilité présumée tend à déresponsabiliser ses utilisateurs, et à les déposséder de toute liberté d'appréciation, à ne se fier qu'au déterminisme informatique, à faire « *de l'ordinateur un ordonnateur (...) renforçant les mécanismes de rigidité, d'autorité, et de domination* » selon la formule de Simon Nora et Alain Minc dans leur rapport sur « *l'informatisation de la société* » en 1978.

Or, il a déjà été démontré que les systèmes biométriques ne sont pas parfaits, reposant fondamentalement sur des calculs de probabilités et sur un équilibre entre deux taux d'erreurs contradictoires : le taux de faux rejets et le taux de fausse acceptation. Tout système biométrique est susceptible selon la configuration, de ne pas reconnaître des personnes habilitées ou de reconnaître des personnes non habilitées. Comme le rappelle le Conseil de l'Europe dans son Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques[86], « *toute présomption d'infaillibilité est erronée* ».

Il est certain que le perfectionnisme de l'identification biométrique ne doit donc pas être assimilé à une quelconque perfection des dispositifs techniques. Les responsables de traitements

---

[84] CEDH., *Schenk c. Suisse*, 12 juillet 1988, série A n° 140

[85] Civ. 3ème, 2 juillet 2003

[86] http://www.coe.int/t/f/affaires_juridiques/coop%E9ration_juridique/protection_des_donn%E9es/documents/rapports_et_%E9tudes_des_comit%E9s_de_protection_des_donn%E9es/O-Biometrie_2005.asp

biométriques doivent tenir compte des limites inhérentes à leur dispositif, ne pas vouer une confiance aveugle au processus de décision automatique, ni nourrir l'illusion que l'identification ou l'authentification/vérification de la personne concernée est toujours correcte.

Difficultés d'apporter la preuve contraire - Cette présomption technique n'a *a priori* rien de juridique. Il reste que le système produit une décision, erronée ou non. Si une personne est « reconnue » à tort comme figurant sur une liste de criminels ou de délinquants recherchés, la conséquence pratique pourrait être qu'elle ait à démontrer son innocence, ou plutôt qu'il y a eu erreur. Inversement, une personne présente au sein d'une liste noire peut ne pas être reconnue, le système biométrique donnant alors une fausse impression de sécurité.

Dans ce cas, il peut être difficile, voire impossible pour la personne concernée de contester la décision. On bascule alors d'une présomption technique selon laquelle le système n'a pas commis d'erreur, à une présomption juridique, contre laquelle la personne concernée doit apporter une preuve contraire.

Une procédure de secours doit donc être prévue et permettre de compenser les erreurs éventuelles. Le candidat à l'identification doit être en mesure de contester le résultat de l'identification, de ne pas pénaliser les personnes qui ne sont pas en mesure de se soumettre à l'identification biométrique (handicapés, personnes blessées ...). Des réactions de panique peuvent naître lorsqu'une personne se trouve seule face à une machine qui lui refuse un accès ou un droit. La définition de droits spécifiques s'analyserait alors comme une compensation justifiée par le recours à de tels procédés.

• Preuve scientifique et liberté d'appréciation

On le voit, la fiabilité présumée des procédés biométriques pourrait contaminer le droit. C'est déjà le cas en matière de preuve biologique. Les conclusions des experts scientifiques ont intégré depuis longtemps le débat judiciaire et de l'administration de la preuve, souvent de manière décisive. Au point qu'on peut considérer le droit aujourd'hui, selon l'expression Jean CARBONNIER comme « *de la science enserrée dans une forme de droit* ».

Valeur de la preuve biométrique. - Ainsi, la fréquence du recours aux identifications génétiques ou biométriques semble attester d'une confiance quasi-aveugle en la « preuve corporelle », que les scientifiques eux-mêmes considèrent incertaine.

Par exemple, en matière de filiation, la preuve scientifique fonde à la fois la prétention des parties, la preuve, et le verdict final. Le réalisme biologique prend le pas sur la présomption légale de paternité et les valeurs protégées par le droit de la famille, qui prend compte des relations affectives et sociales durables entre l'enfant avec le père légitime. Pour Alice MILANOVA[87], le juge ne pouvant délivrer qu'une décision conforme à l'avis de l'expert, cette preuve scientifique « *abolit la liberté d'appréciation du juge, au mépris de l'équilibre des intérêts des parties* ».

En matière pénale, la portée de cette preuve corporelle est plus réduite. Elle n'est qu'un instrument pouvant ou non renforcer une « intime conviction » fondée sur l'ensemble de faits : témoignages, aveux selon les versions des faits exposés par les témoins. Dans un arrêt du 3 juin 1998, la Cour de cassation a ainsi conclu : « *la preuve biologique scientifique est une caractéristique imparfaite de la personne humaine et de ses relations sociales et affectives, que seule la vérité juridique, libérée du poids du réalisme biologique est en mesure d'exprimer.* »

[87] Alice MILANOVA, *Preuve corporelle, vérité scientifique et personne humaine*, Revue de Droit Prospectif, R.J.J., 2003-3 n°99.

Si l'on applique ce raisonnement à la biométrie, le fait d'avoir apposé sa main ou son doigt sur un capteur biométrique peut attester des horaires ou de la présence d'un salarié sur son lieu de travail, ou de transactions économiques en ligne par un investisseur. Les techniques biométriques d'identification peuvent alors fournir des indices susceptibles d'être pris en compte dans le cadre du règlement d'un litige portant sur un fait matériel, voire sur un acte juridique.

Au final, comme le souligne le rapport de Christian CABALE[88], « *il appartiendra au juge de décider du crédit qui pourra être accordé à cet indice de nature technique* ». Il y a cependant fort à parier que la tendance à l'admission de la preuve biologique et scientifique en général, en tant qu'élément déterminant, se confirme en matière de preuve biométrique.

Vers une présomption de fiabilité ? - L'identification biométrique est promise à un bel avenir dans le domaine des communications électroniques, notamment au vu du manque d'intérêt dont souffre la signature électronique. L'identification sur Internet restant une nécessité à bien des égards, notamment pour la sécurité des transactions, la cryptologie pourrait demeurer afin d'assurer la confidentialité des transmissions. Parallèlement, des dispositifs plus efficaces, plus sûrs et accessoirement plus « ludiques », pourraient remplacer la fonction d'identification de la signature électronique.

Application potentielle du régime de la signature électronique. - Aux termes de l'article 1316-1 du Code civil, l'écrit électronique est admis à titre de preuve à la double condition que « *la personne dont il émane puisse être identifiée* » et que « *l'établissement et la conservation dudit écrit soient de nature à en garantir l'intégrité* ». Le caractère général des termes employés permet fort simplement d'anticiper son application à la preuve biométrique. Par exemple, la passation d'un ordre d'achat en bourse, ayant nécessité une identification en ligne de l'investisseur par biométrie pourra être admise à titre de preuve. À charge pour la partie qui s'en prévaut d'en démontrer la fiabilité.

Par ailleurs, de même que le progrès scientifique conduit le législateur à définir des présomptions, compte tenu du degré de fiabilité des techniques mises en œuvre, le développement des techniques biométriques renforcera vraisemblablement cette tendance. Ainsi, une présomption de fiabilité existe aux termes de l'article 1316-4 du Code civil pour la signature électronique.

La signature électronique est ainsi définie comme « *procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* » et "*sa fiabilité est présumée, jusqu'à preuve contraire, lorsqu'elle est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'État* ». En substance, les conditions en question consistent à recourir à un prestataire de services de certification électronique (PSCE) agréé par la DCSSI. Nul doute qu'à terme se développe une activité de certification biométrique, permettant d'entrevoir sans difficulté, l'idée d'une présomption juridique de fiabilité de l'identification biométrique.

Dans cette perspective, il est probable que le régime de la signature électronique puisse accueillir, à quelques modifications près, les usages de la biométrie. Ces derniers pourraient à terme bénéficier sous les mêmes conditions, de la présomption de fiabilité dont bénéficie la signature électronique.

§ 2. Portée et limites des garde-fous existants

[88] Christian CABAL, 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*, Rapport n° 938 déposé le 16 juin 2003 et Compte rendu de l'audition publique du 4 mai 2006 sur la biométrie.

• Le nécessaire maintien d'une présence humaine

Cette automatisation ne doit nullement impliquer une déshumanisation totale du processus. Au contraire, il conviendrait de définir des procédures, des obligations et un régime de responsabilité, relatifs à l'enrôlement et l'appariement, encadrée par des agents spécifiquement formés.

Responsabilité de l'agent chargé de l'enrôlement. - Une présence humaine subsidiaire au moment de l'enrôlement est d'abord nécessaire. Cette phase détermine en réalité pour une grande part la fiabilité du processus puisque l'on fixe une identité de référence. En raison de la présomption de fiabilité qui pèsera de fait sur l'identité biométrique, il serait utile de déterminer précisément quelles sont les obligations et responsabilité de « l'enrôleur ».

Ainsi, un agent devrait toujours accompagner le futur candidat à l'identification, s'assurer que les données biométriques enregistrées sont les bonnes, être capable de détecter et de dissuader les tentatives de contournement du système. Cela suppose en conséquence de sa part à la fois une connaissance de la technologie, des manœuvres susceptibles de révéler un comportement frauduleux, des obligations relatives à la vérification de l'état civil s'il est requis, des règles de droit relatives à la collecte des données. L'agent devrait en outre, être en mesure de traiter les cas de personnes non-éligibles à l'enrôlement : personnes blessées, handicapées, malades.

Cette tâche place quasiment l'agent en charge de l'enrôlement, dans la position d'un « certificateur », au sens des prestataires des services de certification électronique. En cas de préjudice subi par la personne enrôlée, l'agent concerné pourrait engager sa responsabilité pour faute, ou en tant que tiers au contrat liant l'agent à un employeur, pour non-respect d'une obligation de sécurité. À terme, l'agent pourrait être concerné par le régime spécial de responsabilité qui s'applique aux prestataires de services de certification électronique.

Responsabilité de l'agent chargé de l'appariement. - Une présence humaine est également requise lors de la phase d'appariement, essentiellement en cas d'erreur et dans le cas ou la décision du système biométrique emporte des effets de droit pour les personnes. L'agent a alors la responsabilité d'offrir et d'appliquer une procédure de secours en faveur du candidat à l'identification. L'agent, placé en qualité d' « arbitre », décidera s'il y a lieu à une nouvelle identification, au passage à un autre procédé biométrique d'identification, à une identification manuelle, à se fier au témoignages, à apprécier la situation de la personne (urgence, vulnérabilité).

Les responsabilités de l'agent, en tant que « certificateur » ou en tant qu'« arbitre », doivent donc pouvoir être définies, et ce dernier doit pouvoir bénéficier d'une formation spécifique.

• Régime juridique des « décisions automatiques »

Évaluation du profil de l'intéressé. - L'article 10 de la loi française transposant l'article 15 de la directive 95/46 précise qu'« *aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de sa personnalité* ».

De même « *aucune autre décision produisant des effets juridiques à l'égard d'une personne ne peut être prise sur le seul fondement d'un traitement automatisé de données destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité* ».

L'utilisation de la biométrie est une façon de rationaliser et de sécuriser une politique de droits d'accès et d'habilitation et de conserver une trace de ces accès. En ce sens, c'est une

automatisation du processus de décision, préalablement défini par le responsable. L'identification biométrique produit des décisions qui reflètent cette politique et donc des effets juridiques. Cependant, un dispositif n'a en principe pas pour fonction d'évaluer des aspects de la personnalité ou de définir un profil de l'intéressé.

L'hypothèse reste cependant envisageable. Ainsi, le contrôle des horaires par biométrie en entreprise peut parfaitement révéler l'absentéisme, ou les retards à répétition d'un salarié, justifiant par exemple un licenciement. L'article 10 de la loi Informatique et Libertés pourrait alors être applicable, nonobstant les règles de droit du travail.

Droit d'accès limité à la logique de la décision. - La loi définit un droit d'accès par la personne aux informations lui permettant de « *connaître et de contester la logique qui sous-tend le traitement automatisé* » sauf atteinte au droit d'auteur au sens des dispositions du code de la propriété intellectuelle. Ainsi, l'article 39 de la loi dispose que le responsable du fichier doit mettre à la disposition de la personne concernée « *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.* »

TITRE SECOND

RÉGIME JURIDIQUE DES DISPOSITIFS ET DES DONNÉS BIOMÉTRIQUES : EFFICACITÉ ET LIMITES

Chapitre 1.
LE DROIT POSITIF DES DISPOSITIFS ET DES DONNEES BIOMETRIQUES

SECTION 1. Conditions de licéité du traitement et protection des données

SOUS-SECTION 1. Conditions de licéité du traitement

§ 1. Formalités préalables

Quatre régimes distincts. - Il existe aujourd'hui en France quatre régimes de formalités préalables, qui témoignent notamment d'une survivance de la distinction privée - public.

En effet, la réforme de la loi informatique, fichier et liberté du 6 août 2004 avait estompé cette frontière traditionnelle, en soumettant à un régime similaire la majorité des traitements, qu'ils soient opérés pour le compte de l'État ou pour le secteur privé.

Cette dichotomie a été conservée pour la biométrie, qui faisait en même temps son entrée dans le droit commun de la protection des données.

Par ailleurs, les traitements de données biométriques opérés pour le compte de l'État obéissent à deux types de procédure selon leur finalité. Enfin, parallèlement, la CNIL a créé un régime de déclaration simplifié pour certains traitements biométriques, en prenant trois autorisations uniques le 24 avril 2006.

• Le régime commun d'autorisation

La France est un des rares pays européens à faire explicitement référence à la biométrie au sein de la loi consacrée à la protection des données à caractère personnel. En effet, la directive européenne CE/95/46, transposée en France par la loi du 6 août 2004 modifiant la loi informatique, fichiers, et libertés, ne mentionne à aucun moment les traitements de données biométriques.

Un régime de contrôle *a priori*, à contre-courant. - Le considérant 52 de la directive indique que « *le contrôle a posteriori par les autorités compétentes doit être en général considéré comme une mesure suffisante* ».

De manière générale, la notification à l'autorité de contrôle a pour objet « *d'organiser la publicité des finalités du traitement en vue de son contrôle* » (considérant 48), et de simplifier les procédures « *afin d'éviter des formalités administratives inadéquates pour les traitements qui ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées* » (considérant 49).

A contrario, la directive précise que pour certains traitements, les États « *doivent prévoir un examen préalable à leur mise en oeuvre, effectué par l'autorité de contrôle (qui peut) émettre un*

avis ou autoriser le traitement des données, (y compris) au cours de l'élaboration d'une mesure législative » (considérant 52).

Le contrôle *a priori* est donc maintenu, à titre subsidiaire et exceptionnel[89], pour les traitements « *susceptibles de présenter des risques particuliers au regard des droits et des libertés des personnes concernées, du fait de leur nature, de leur portée ou de leurs finalités telles que celle d'exclure des personnes du bénéfice d'un droit, d'une prestation ou d'un contrat, ou du fait de l'usage particulier d'une technologie nouvelle* ».

C'est donc bien en raison des risques particuliers pressentis par le législateur à propos des traitements de données biométriques, que la loi les soumet au régime contraignant du contrôle *a priori*, en dépit d'une évolution générale du droit de la protection des données, tendant à faire du contrôle *a posteriori* le régime de droit commun (déclaration simplifiées, pouvoirs d'enquêtes, sanctions pénales ...). Il revient donc à la CNIL d'examiner les demandes d'autorisations et les projets législatifs ou réglementaires sur tout traitement répondant à la définition donnée par la loi.

Définition des traitements concernés. - En vertu de l'article 25-I alinéa 8, sont donc concernés par ce régime d'autorisation les « *traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes* ». La formule étant un peu lourde, on continuera à se référer aux dispositifs ou systèmes d'identification biométrique, comme le fait maintenant la CNIL.

Cette définition constitue un des rares points d'appui purement législatifs au soutien d'un mémoire consacré à la biométrie. Il est donc tentant de se livrer à une petite exégèse. On ne sait d'abord si l'expression « *nécessaires au contrôle de l'identité des personnes* » se réfère aux données elles-mêmes ou aux traitements, ou encore aux deux. Par ailleurs, cette définition souffre du paradoxe d'être à la fois trop générale, et trop restrictive.

Une définition trop générale des données biométriques ? - Trop générale, car la donnée biométrique elle-même n'est pas réellement définie. Une photographie faciale est-elle une donnée biométrique ? La réponse n'est pas évidente. Si la réponse était positive, cela aurait pour effet de soumettre un grand nombre de traitements, comportant par exemple une photo d'identité, au régime des d'autorisation. Une donnée génétique est-elle une donnée biométrique ? La loi semble bien les différencier en leur consacrant des dispositions propres - mais qui se rejoignent - alors que parallèlement, la CNIL compte au rang des données biométriques, les données de l'ADN.

Une définition trop restrictive des traitements ? - Tous les systèmes biométriques n'ont pas nécessairement pour finalité le contrôle de l'identité d'une personne. Par exemple, on peut s'assurer de l'authenticité d'un titre et de son lien avec le porteur, en vérifiant que les données intégrées au titre et les empreintes du porteur sont les mêmes. On peut alors parler de contrôle anonyme d'authenticité. La finalité du traitement peut encore être le contrôle d'accès à un restaurant d'entreprise. Dans ce cas, il s'agit moins d'un contrôle d'identité que d'un contrôle anonyme d'habilitation. Enfin, le traitement peut avoir pour objet le contrôle des horaires et l'enregistrement des heures d'entrée et de sortie du lieu de travail. L'identité n'est alors qu'un support à la traçabilité.

Est-ce à dire que les exemples cités - c'est-à-dire une grande partie des traitements mis en

---

[89] Herbert MAISL, *Changer la CNIL ? Pourquoi faire ?*, Expertise des systèmes d'informations N° 200-Décembre 1996 http://www.celog.fr/expertises/sommaires/96/articles200/MAISL.HTM. *« On peut penser que la Cnil devrait réorienter son activité davantage vers des contrôles a posteriori. On observera, d'ailleurs, que la directive va dans ce sens. La déclaration de traitement y est la règle mais des exonérations et des simplifications sont envisagées, l'examen préalable du projet de traitement ne devant intervenir que dans des cas "très restreints" si apparaissent "des risques particuliers.* »

oeuvre dans le secteur privé - sont exclus du régime de déclaration préalable ? Il semble que non, la CNIL ayant eu à examiner tout type de traitement comportant des données biométriques. Mais quelle est l'utilité de restreindre ainsi le champ d'application du régime d'autorisation aux traitements de données biométriques « *nécessaires au contrôle de l'identité des personnes* » ?

Est-ce pour ouvrir une brèche et dispenser de formalités les responsables de traitements biométriques dont la finalité serait autre que le contrôle de l'identité ? En cas de contentieux, le responsable ayant omis sciemment ou non, de soumettre un de ces traitements à l'examen de la CNIL, pourrait utiliser cette brèche comme moyen de défense : « *mon traitement n'a pas pour finalité le contrôle de l'identité des personnes, il n'est pas soumis à autorisation préalable* ».

Or, il nous semble que la volonté du législateur d'accorder un statut particulier à la biométrie est incompatible avec ce moyen légal mis à la disposition des responsables de traitements pour contourner leurs obligations.

Une définition contradictoire ? - Aux termes de l'article 2 de la loi informatique, fichiers et libertés, constitue une donnée à caractère personnel « *toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres* ». La loi ajoute que pour déterminer si une personne est identifiable, il convient de considérer « *l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* ».

Contrairement à la définition de l'article 25, celle de l'article 2 a pour effet de rendre la loi applicable à tout les traitements biométriques, dès lors que la personne concernée puisse être identifiée, indirectement ou indirectement, au vu des moyens dont dispose le responsable. Aux termes de cet article, ce n'est plus le contrôle de l'identité des personnes, nécessaire finalité du traitement, qui conditionne l'applicabilité de la loi, mais le caractère identifiable des personnes, en tant que modalité accessoire du traitement. Cela a pour effet d'inclure les exemples d'application précités de la biométrie, dont la finalité n'est pas l'identification, mais qui peuvent permettre d'identifier les personnes.

• Les traitements opérés pour le compte de l'État

Survivance de la distinction privé - public. - Le cadre juridique témoigne d'une survivance de la distinction entre traitements pour le privé et ceux opérés pour le compte de l'État, après la modification de la Loi Informatique et libertés en 2004.

Procédure solennelle. - Ainsi, l'article 27-I alinéa 2 soumet à autorisation par décret en Conseil d'État, pris après avis de la CNIL « *les traitements de données à caractère personnel mis en oeuvre pour le compte de l'État qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes* ».

Il s'agit là de la procédure la plus stricte et la plus solennelle prescrite par la loi, prévue pour deux cas spécifiques : les données biométriques, et le numéro NIR. Cela qui n'a évidemment rien d'une coïncidence, le lien de parenté existant entre ces deux types d'identifiants universels potentiels ayant déjà été souligné.

Procédure simplifiée. - Cependant, certains traitements administratifs comportant des données biométriques peuvent être autorisés par arrêté ou par décision de l'organe délibérant, en cas de traitement opéré pour le compte d'un établissement public ou d'une personne morale de droit privé gérant un service public, après avis de la CNIL. Il s'agit de traitements dont les risques sont

moindres ou qui sont réalisés dans l'intérêt des administrés.

Cette procédure est d'abord mise en oeuvre pour les traitements de données biométrique qui ne comportent pas de données sensibles au sens de l'article 8-I (origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, données de santé, données relatives à la vie sexuelle) et au sens de l'article 9 (données relatives aux infractions, condamnations et mesures de sûreté.)

Elle concerne également les traitements comportant des données biométriques ne donnant pas lieu à une interconnexion entre des traitements ou fichiers correspondant à des intérêts publics différents.

La procédure est enfin applicable aux traitements comportant des données biométriques mis en oeuvre par des services ayant pour mission, soit de déterminer les conditions d'ouverture ou l'étendue d'un droit des administrés, soit d'établir l'assiette, de contrôler ou de recouvrer des impositions ou taxes de toute nature, soit d'établir des statistiques.

On constate donc que les traitements biométriques, opérés pour le compte de l'État, et donnant lieu à des interconnexions de fichiers correspondant à des intérêts publics différents, ou comportant des données sensibles, restent en principe soumis à l'appréciation du Conseil d'État. En effet, il s'agit de traitements qui ont déjà identifiés comme présentant les risques les plus importants et il parait légitime de confier cette responsabilité à la plus haute juridiction administrative.

• Régime simplifié de déclaration

Aux termes de l'article 25 II la loi informatique, fichiers et libertés, les traitements qui répondent à une même finalité, qui 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 CNIL. Le responsable du traitement adresse alors à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

La CNIL a usé de cette prérogative en matière de biométrie en prenant le 27 avril 2006 trois autorisations uniques[90], simplifiant les formalités préalables pour certains traitements. La CNIL prescrit ainsi en détail les modalités de mise en oeuvre des dispositifs biométriques, auxquelles les responsables déclarent se conformer.

Ces autorisations uniques ont permis à la CNIL d'enregistrer 299 déclarations de conformité sur les 7 derniers mois de l'année 2006.

• Sanctions pénales

Non respect du formalisme. - Il est relativement rare que le non respect du formalisme soit sanctionné pénalement et aussi lourdement. Ainsi, l'article 226-16 du Code pénal dispose que le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à

[90] Délibération n°2006-103 n°AU-009, 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. Délibération n°2006-102 n°AU-008, 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. Délibération n°2006-101 (n°AU-007) 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.

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 € d'amende. Les responsables de traitements de données comportant des données biométriques ont donc fortement intérêt à respecter les formalités prescrites.

Utilisation illégale de données identifiantes. - Cette sanction devrait paraître suffisamment dissuasive. Il est pourtant intéressant de noter que l'utilisation du NIR, en dehors des cas prescrits par la loi, est punie de cinq ans d'emprisonnement et de 300 000 € d'amende[91].

Cette disposition appelle à plusieurs remarques. Dans un premier temps, on peut comprendre qu'en raison du statut particulier du NIR, son utilisation illicite fasse l'objet d'une sanction spécifique. Cependant, l'utilisation illicite du NIR suppose un manquement aux formalités préalables, à moins d'être passé entre les filets de la CNIL, ce qu'on ne saurait imaginer.

Problème du concours d'infractions. - Or, ce manquement aux formalités constitue déjà une infraction. Il nous apparaît alors que l'utilisation du NIR met quasi-nécessairement le juge pénal en présence d'un « concours d'infraction » au sens de l'article 132-2 du Code pénal. Qu'il s'agisse alors d'un concours réel (constitué par plusieurs faits distincts constituant des infractions distinctes) ou d'un concours idéal (un fait unique, indivisible, susceptible de recevoir plusieurs qualifications pénales), il s'agira de savoir si les peines en question sont cumulables.

Cette hypothèse est relativement rare, en vertu du principe de *non bis in idem*, les mêmes faits ne pouvant être sanctionnés plusieurs fois. Par ailleurs, si l'on acceptait le principe du cumul, il apparaît qu'un seul traitement pourrait parfaitement revêtir les caractères des quelques quinze infractions sanctionnées par le Code pénal, ce qui aurait pour effet de porter à 75 ans d'emprisonnement et 4.500.000 € d'amende les peines encourues. Il nous apparaît donc que les peines en question sont difficilement cumulables.

L'existence d'une sanction spécifique à l'utilisation du NIR nous paraît ainsi inutile, étant déjà sanctionnée par le non respect du formalisme. Il est probable qu'une confusion s'opérerait de plein droit entre les peines de même nature, à hauteur du maximum le plus élevé encouru pour l'une des infractions.

Ces réflexions permettent de juger de l'opportunité de créer une infraction particulière, incriminant l'usage illégal de données biométriques.

Il a été dit que le NIR et les données biométriques comportaient sensiblement les mêmes risques au plan de la vie privée, ce qui justifiait un régime identique de contrôle *a priori*. Pourquoi dès lors ne pas avoir aligné leurs régimes respectifs de contrôle *a posteriori* ? On aurait parfaitement pu imaginer, sous l'article 226-16-1 du Code pénal relatif au NIR, un article 226-16-2 relatif à la biométrie.

Les considérations précédentes nous incitent à croire que, de même que pour le NIR, l'usage illégal de la biométrie est déjà sanctionné par les peines applicables au non-respect du formalisme, et que l'existence d'une peine spécifique ne permettrait pas de les accumuler.

Valeur économique des données. - Enfin, il sera sage de mesurer exactement la valeur économique de ces données et de la mesurer à l'aspect véritablement dissuasif de la sanction par rapport aux gains potentiel issus de leur commercialisation. Un rapport positif entre la valeur d'un fichier biométrique et le montant des peines pécuniaires applicables pourrait inciter les responsables

[91] Article 226-16-1 du Code pénal.

à considérer la sanction comme un risque acceptable.

§ 2. Contrôle de proportionnalité par la CNIL

Nous fournissons en annexe une liste des décisions de la CNIL, qui a rendu en la matière plus d'une centaine de décisions. On se bornera donc à relever quelques cas d'espèce.

Une appréciation *in concreto*. - Depuis que la CNIL a eu à se prononcer sur des systèmes biométriques, il n'a jamais été question pour elle d'émettre un jugement d'ordre général sur la biométrie. Il n'y a pas une biométrie mais des dispositifs biométriques, dont les modalités de mise en oeuvre peuvent être considérablement différentes d'un système à l'autre et surtout, plus ou moins problématique au regard de la vie privée.

Ainsi, il y a autant de types de dispositifs biométriques que de marqueurs biométriques. Citons pour l'essentiel les empreintes digitales, la morphologie de la main, la reconnaissance faciale, et la reconnaissance de l'iris, auxquelles on a le plus souvent recours. Par ailleurs, il y a une distinction à faire selon que le système stocke les gabarits servant de référence dans une base de donnée enregistrée sur un serveur, directement dans la borne biométrique servant à l'identification, ou encore dans un support externe détenu par l'utilisateur (clé USB, carte à puce, badge).

Le contrôle de proportionnalité par la CNIL s'effectue donc *in concreto*, en fonction des modalités de fonctionnement retenues par le responsable du traitement.

• Utilisation des empreintes digitales sur base de données

Impératif de sécurité. - Le fait pour le responsable d'avoir accès aux gabarits biométriques, ou le fait qu'il soit stockés sur un serveur, potentiellement vulnérable aux attaques informatiques, amplifie le risque de détournement d'usage des empreintes. Par ailleurs, les empreintes digitales sont considérées comme sensibles, du fait de leur utilisation par les services de police (FNAED).

Le responsable du traitement devra donc apporter la preuve de l'existence d'un fort impératif de sécurité. Le critère d'impératif de sécurité est apprécié par la CNIL de façon subjective, apprécié en fonction du cas d'espèce.

Obligation légale de sécurité. - Certains impératifs découlent directement d'une obligation légale ou réglementaire. Par exemple, l'impératif de sécurité des locaux d'impression des matrices de l'Euro est lié aux exigences de la Banque Centrale Européenne et imposé par la réglementation relative aux installations classées Point Sensible de niveau 2, instaurée par les Ministères de l'Intérieur, de la Défense et de l'Economie de l'Industrie et des Finances Délibération[92].

De même, les prestataires de services de certification électronique sont soumis à une obligation de sécurité, aux termes de l'article 6 du décret n° 2001-272 du 30 mars 2001, qui justifie la sécurisation des salles abritant les serveurs informatiques contenant les certificats électroniques[93].

C'est encore le cas lorsque la société est soumise au régime des Installations Classées pour la Protection de l'Environnement[94], ou aux exigences de sécurité imposées, par l'habilitation spécifique « confidentiel défense » et « secret défense », octroyée par la direction centrale de la

[92] Délibération n° 2007-050 du 21 mars 2007.
[93] Délibération n° 2007-082 du 25 avril 2007.
[94] Délibération n° 2007-089 du 25 avril 2007.

sécurité du Commissariat à l'Energie Atomique[95].

Existence de zones sensibles. - Plus généralement et en dehors des obligations légales ou réglementaires, le responsable du traitement pourra apporter la preuve de l'existence de « zones sensibles » impliquant une sécurité accrue, à laquelle est susceptible de répondre la biométrie. Il en est ainsi, par exemple, lorsque le dispositif doit répondre à la nécessité :

• de garantir l'intégrité des blocs opératoires d'un hôpital dans le cadre d'une procédure d'accréditation (délibération n° 2007-080 du 25 avril 2007) ;

• de contrôler l'utilisation chariots de manutentions particulièrement dangereux (délibération n° 2007-081 du 25 avril 2007) ou cages d'ascenseurs (Délibération n° 2007-025 du 8 février 2007) ;

• d'empêcher l'accès non-autorisé à un centre de contrôle des moyens de surveillance, comprenant les moyens d'éditions des badges d'accès, le système de vidéosurveillance, la gestion des alarmes, le système de géolocalisation des véhicules (délibération n°2007-086 du 25 avril 2007) ;

• d'empêcher l'accès non-autorisé à des pièces abritant des serveurs contenant des informations classées « confidentiel défense », « secret défense » aux termes de l'Instruction Générale Interministérielle sur la protection du secret et des informations concernant la défense nationale et la sécurité de l'État (délibération 2007-054 du 21 mars 2007) ; zones classées secret défense (délibération n° 2006-070 du 16 mars 2006) ;

• de protéger des documents sur des sites nucléaires (délibération n° 2006-068 du 16 mars 2006) ;

• d'empêcher l'accès non-autorisé aux salles où sont gardés les sujets nationaux d'examens et de concours (délibération n° 2007-052 du 21 mars 2007) ;

• de contrôler l'accès à un appontement pétrolier et gazier, classés "SEVESO II" dans lequel sont stockés simultanément des produits dangereux (délibération n° 2007-056 du 21 mars 2007) ;

• locaux sensibles de l'usine chimique classée "SEVESO II" seuil haut dans la mesure où y sont traités des produits potentiellement dangereux (tétrachlorure de titane, Oléum, Chlore, soude, potasse, ammoniac, acide chlorhydrique).les serveurs pilotant le fonctionnement et les automates des chaînes de fabrication (délibération n° 2007-051 du 21 mars 2007) ;

• de fournir la liste exacte des personnes présentes sur le site en cas d'accident sur un site classé de type "SEVESO» ; salles informatiques qui contiennent des systèmes sensibles et vitaux pour le fonctionnement de la CSI, établissement ouvert au public dans lequel les couloirs d'accès traversent les zones privées (cité des sciences) (délibération n° 2005-281 du 22 novembre 2005) ;

• de contrôler l'accès à des zones du site où sont produits les documents d'identité, telles que les passeports, les cartes grises et les cartes d'identité. (délibération n° 2005-113 du 07 juin 2005) ;

• Modalités alternatives de traitement

Absence d'impératif de sécurité. - À défaut pour le responsable du traitement d'apporter la preuve de l'existence d'un impératif de sécurité, la CNIL refusera d'autoriser les traitements basés sur l'empreinte digitale et leur stockage sur base de donnée, même si « *l'objectif est légitime* »[96].

Les responsables peuvent alors opter soit pour un autre mode de stockage des données, soit pour un autre type de marqueur biométrique. Ainsi, le responsable du traitement pourra alternativement choisir un dispositif reposant sur l'utilisation des empreintes digitales stockées sur support externe individuel, ou un dispositif basé sur le contours de la main, le recours à une base de donnée n'étant pas proscrit.

[95] Délibération n° 2007-057 du 21 mars 2007.

[96] Délibérations n°2006-153 à 2006-157 du 30 mai 2006 (contrôle d'accès aux salles informatiques).

Utilisation d'empreintes digitales sans base de données. - L'utilisation des empreintes digitales n'est pas proscrite en l'absence d'impératif de sécurité. Le responsable devra en revanche opter pour le stockage des données de référence sur une carte individuelle, une clé USB.

Par exemple, la signature d'un « protocole sur la promotion du jeu responsable[97] » signé par le Syndicat des Casinos de France et le Ministère de l'Intérieur, fait obligation aux casinos contrôler l'accès à leurs établissements. Il s'agissait notamment de vérifier que les personnes entrantes ne figurent pas au fichier des interdits de jeu. Il n'y avait pas en l'espèce d'impératif de sécurité à proprement parler. La CNIL a autorisé 18 traitements dans ce domaine[98] dont les modalités étaient toutes parfaitement identiques. Ils reposaient notamment sur le stockage des données biométriques chiffrées dans une carte « sans contact ».

De même, dans une délibération 2007-025, du 08 février 2007, la CNIL a autorisé l'Établissement Public du Musée du Louvre à mettre en oeuvre un traitement biométrique reposant sur les empreintes digitales, afin d'empêcher l'accès non-autorisé aux armoires où sont conservées les clés d'accès à certaines zones sensibles du musée, comme les réserves d'oeuvres d'art. Les gabarits étaient chiffrés et stockés sur une carte à puce dotée d'une piste magnétique.

La CNIL a même simplifié les formalités préalables pour l'utilisation d'empreintes pour les traitements aux fins de contrôle de l'accès aux locaux sur les lieux de travail. Aux termes de l'autorisation unique n°AU-008[99], les responsables du traitement doivent alors se conformer aux modalités techniques définies par la CNIL, dont entre autres, le stockage des données exclusivement sur un support individuel détenu par la personne concernée.

• Utilisation de la morphologie de la main

Si le responsable souhaite néanmoins recourir à une base de données, le responsable n'aura d'autre choix que de recourir à une technologie autre que les empreintes digitales, ou toute autre technologies laissant des traces. La morphologie de la main (encore appelée « contours de la main », « géométrie de la main » ou « forme de la main ») est aujourd'hui la technologie quasiment incontournable. Il est très rare que la CNIL se prononce défavorablement à l'égard d'un traitement utilisant cette technologie, quelle qu'en soit la finalité.

Ainsi, l'utilisation de la morphologie de la main est régulièrement autorisée pour le contrôle des horaires et de l'accès aux restaurants sur les lieux de travail[100]. C'est également le cas pour les accès aux restaurants scolaires, la gestion de la demi-pension des collèges et lycées[101].

• Vers un contrôle a posteriori ?

---

[97] Ce protocole signé le le 5 janvier 2006 a notamment pour objet de supprimer le droit de timbre à l'entrée des salles des jeux de table et ainsi de réunir au sein d'un même espace les machines à sous, jusqu'à présent en accès libre, et les jeux de table dont l'accès doit être contrôlé. Il prévoit également, à compter du 1er novembre 2006, la mise en oeuvre d'un contrôle généralisé des personnes désirant accéder aux salles de jeux, et donc au casino dans son ensemble, afin de s'assurer qu'elles ne sont pas mineures ou qu'elles ne figurent pas dans le fichier national des interdits de jeux. Ce fichier comprend les données relatives aux personnes ayant volontairement fait une demande auprès du Ministère de l'intérieur pour être exclues des salles de jeux ainsi que celles ayant fait l'objet d'une exclusion administrative.Le respect de cette obligation implique, pour chaque personne souhaitant entrer dans un casino, un contrôle de la pièce d'identité suivi d'une vérification dans le fichier national des interdits de jeux.

[98] Délibérations 2006-265 à 2006-278 du 5 décembre 2006.

[99] Délibération n°2006-102 du 27 avril 2006.

[100] Autorisation unique n°AU-007, délibération n°2006-101 du 27 avril 2006 ; délibération 2006-099 et 2006-097 du 6 avril 2006 ; délibération n°2006-58 et 2006-59 du 2 mars 2006.

[101] Délibération 2006-031 du 2 février 2006 (Collège Rolland-Garros) ; délibération 2006-006 et 2006-0078 du 12 janvier 2006 (lycée de la Vallée de Chevreuse, lycée Thierry Maulnier) ; délibération n°02-070 du 15 octobre 2005 (collège Joliot Curie de Carqueiranne).

On constate cependant que de nombreuses redondances ont lieu. Des traitements de type similaire sont régulièrement examinés par la CNIL. Or ces dernières font jurisprudence, de sorte qu'on peut se demander si certaines décisions ne sont pas qu'une répétition artificielle de ce qui a été décidé, uniquement pour assurer le respect du formalisme en vigueur.

Engorgement de la CNIL. - L'engorgement de la CNIL dans ce domaine était prévisible au regard de l'intérêt porté par l'ensemble des acteurs et des perspectives d'évolution du marché. Un renforcement des moyens de la CNIL n'aurait été qu'une manière de pérenniser artificiellement le principe de l'autorisation. La CNIL relève ainsi dans son dernier rapport d'activité[102] que le nombre de demandes a été multiplié par 10 entre 2005 et 2006. Au 25 avril 2007, on décompte près de 150 décisions relatives à la biométrie.

La CNIL a ainsi usé de la prérogative que lui octroie de l'article 25 II la loi informatique, fichiers et libertés pour autoriser par décision unique « *les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires* ». Dans ce cas, le responsable de chaque traitement adresse à la Commission un engagement de conformité à la description figurant dans l'autorisation.

Autorisations uniques. - La CNIL a ainsi pris trois autorisations uniques le 27 avril 2006[103] en matière de biométrie.

On remarque que la spécificité des traitements de données biométriques, auxquels la loi avait entendu conférer un statut particulier par une procédure de contrôle *a priori*, trouve ainsi sa portée réduite, puisque la CNIL commence à substituer au régime d'autorisation préalable un régime de déclaration de conformité.

Le renversement était inévitable, mais il traduit le fait que l'idée d'un contrôle *a priori* des traitements de données biométrique ne suffit plus, ou est inapproprié, pour conférer à ces traitement un statut particulier, comme le souhaitait le législateur. Serait-il judicieux de compenser ce glissement par l'existence d'une infraction spécifique pour l'usage non autorisé des données biométriques, à l'image du NIR ? Comme il a déjà été démontré, nous pensons que cela serait d'un intérêt et d'une efficacité limitées.

SOUS-SECTION 2 : Protection des données biométriques

§ 1. Qualification des données biométriques

• Des données « potentiellement » à caractère personnelles

Les données biométriques sont-elles nécessairement des données à caractère personnel ? « *Rien n'est plus personnel que le corps, affirment certains* »[104]. Les données issues du corps que traite la biométrie, seraient donc par essence des données à caractère personnel.

La réponse ne peut cependant pas être apportée de manière aussi catégorique.

Nature des données brutes. - Les données biométriques peuvent d'abord être des données

[102] Commission nationale de l'informatique et des libertés - 27e rapport d'activité 2006.

[103] Délibération n°2006-103 (n°AU-009) ; délibération n°2006-102 (n°AU-008) ; délibération n°2006-101 n°AU-007).

[104] 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.

brutes, c'est-à-dire des images numérisées des marqueurs biométriques. Pour cette catégorie, un élément de réponse est apporté par le 14ème considérant de la directive CE/95/46.

« *Compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer des données constituées par des sons et des images, relatives aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données* ».

L'image numérisée d'un doigt, ou de l'iris, peut donc être concernée par les règles de protection des données.

Nature des gabarits. - Les gabarits sont le résultat d'un algorithme permettant d'en relever les points-clés, une sorte de canevas ou de colonne vertébrale de la donnée brute. Il ne s'agit donc pas d'une image pixellisée, ni d'une suite alphanumérique, ni d'un son, mais davantage d'une figure géométrique ou vectorielle complexe, ce qui pose des difficultés à lui donner le statut de donnée à caractère personnel. C'est la difficulté que relève le rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques.

Débat doctrinal. - « *Différents points de vue existent quant à savoir si les données biométriques constituent toujours des données à caractère personnel. Certains arguent du fait qu'il pourrait s'avérer impossible d'identifier quelqu'un sur la base par exemple d'une empreinte digitale incomplète. En outre, l'on pourrait soutenir que les données biométriques en elles-mêmes ne fournissent aucune information sur l'individu. D'autres au contraire défendent l'idée que les données biométriques permettent par leur nature même l'identification d'un individu, puisque ces données peuvent être rattachées de manière unique et permanente à une personne* ».

L'analyse des définitions ne nous semble pas permettre d'inclure par principe les données biométriques dans le champ d'application matériel des règles de protection des données. C'est en effet moins la nature elle-même des données que la possibilité de faire un lien avec une personne qui est en cause, en fonction des modalités du traitement.

Le critère du lien avec une personne identifiable. - Conformément à l'article 2, point a), de la directive 95/46/CE, il faut entendre par données à caractère personnel « *toute information concernant une personne physique identifiée ou identifiable ; 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* ».

Par ailleurs, au considérant 26, il est précisé que « *pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne* ». La loi informatique, fichiers, et libertés n'a pas repris la même formulation. Pour déterminer si une personne est identifiable, il convient de considérer « *l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne* ».

Appréciation *in concreto*. - Aux termes de ces définitions, la possibilité d'établir un lien avec une personne identifiée n'est pas appréciée *in abstracto* (« *les données biométriques sont des données personnelles parce qu'elles permettent, en général, d'identifier les personnes* ») mais *in concreto* (« *les données biométrique ne sont des données personnelles que lorsque des moyens susceptibles d'être raisonnablement mis en oeuvre sont à la disposition du responsable du traitement pour identifier la personne* »).

Cette analyse confirme l'idée qu'une collection d'empreintes digitales non identifiables au vu des moyens dont on dispose, ne constitue pas un traitement de donnée à caractère personnel.

Il nous apparaît même que les données biométriques, prises isolément, sont des données anonymes, de la même manière que l'information « personne mariée » ne devient une donnée personnelle que lorsqu'elle peut être rapprochée d'une personne déterminée.

C'est donc uniquement dans leur dimension relative que les données biométriques sont des données à caractère personnel. Elles n'entrent pas par principe dans le domaine d'application de la loi, la condition nécessaire et suffisante étant la possibilité d'établir un lien avec une personne déterminée, c'est-à-dire la même condition que pour toute donnée à caractère personnel.

En pratique, des données nécessairement personnelles ? - Dès lors que l'identification des personnes est la finalité du traitement, il apparaît que les données biométriques utilisées sont nécessairement des données à caractère personnel. Cependant, il n'est pas exclu qu'un système d'identification ou de vérification fasse l'objet d'un procédé d'anonymisation. La délivrance de badges d'accès personnel ne nécessite nullement d'associer l'identité d'une personne aux données collectées. Il suffit que le système puisse être en mesure de comparer un gabarit de référence anonyme et un gabarit de test non conservé, pour que le procédé soit indépendant de l'identité de la personne.

On voit au final qu'il est inutile de vouloir décider si une donnée biométrique est par essence une donnée à caractère personnel et donc si le texte est applicable.

D'abord parce qu'établir une liste des données concernées par les textes serait inévitablement amenée à être incomplète ou obsolète en fonction des évolutions technologiques.

Ensuite parce qu'en droit français, il existe une forte présomption de l'applicabilité de la loi aux données biométriques, du fait de la soumission des « *traitements comportant des données biométriques nécessaire à l'identification des personnes* » à des formalités spécifiques. Il peut cependant exister certaines brèches, qui rendent la loi inapplicable à ces traitements.

Conséquences de l'applicabilité de la loi aux données biométriques. - Les dispositions de la loi informatique, fichiers et libertés partent donc du principe que les traitements de données biométriques, lorsqu'ils répondent aux critères d'applicabilité, doivent être mis en oeuvre conformément aux règles qu'elle pose. Par ailleurs, le recours à ces dispositifs est soumis à un formalisme plus strict, qui correspond à une volonté de réguler leur utilisation, en considération de leur nature particulière.

L'applicabilité de la loi aux données biométriques rend ces dernières potentiellement concernées par les exceptions visées par les textes. Ainsi, l'article 3 de la directive 95/46/CE exclu de son champ d'application les traitements ayant pour objet la sécurité publique, la défense et la sûreté de l'État, ainsi que les traitement de vidéo surveillance (à terme ayant vocation à fusionner avec la biométrie) mis en œuvre « *à des fins de sécurité publique, de défense, de sûreté de l'État ou de droit pénal* ». Les conditions juridiques d'utilisation des dispositifs biométriques nationaux utilisés à ces fins, relèvent donc de la compétence de chaque État.

Sont également exclus les traitements mis en oeuvre pour l'exercice d'activités exclusivement personnelles, les copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises (article 4).

Enfin, le champ d'application territorial a également pour objet de définir les traitements concernés ou non par la loi. Aux termes de l'article 5 de la loi informatique, fichiers et libertés, sont soumis à la loi les traitements de données à caractère personnel dont le responsable est établi sur le territoire français[105], ou dont le responsable, sans être établi sur le territoire français ou sur celui d'un autre État membre de la Communauté européenne, recourt à des moyens de traitement situés sur le territoire français[106].

• Des données indirectement sensibles

En principe, une donnée biométrique est neutre, sauf lorsque son interprétation permet de déduire certaines caractéristiques sur la personne. Dans ce cas, la donnée biométrique est soumise au régime des données sensibles. Les données brutes peuvent comporter des informations dont l'interprétation peut révéler l'origine raciale ou ethnique - comme les données issues de la reconnaissance faciale - ou encore des données relatives à la santé, comme un handicap ou une maladie (reconnaissance de l'iris, de l'ADN, des empreintes digitales).

Or, l'article 8 pose un principe d'interdiction de collecte ou de traitement des données 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 sexuelle de celles-ci* ». Les traitements de données biométriques qui tomberaient sous le coup de l'article 8 pourraient donc être frappé d'interdiction.

Toutefois, ces traitements demeurent possibles, la loi informatique, fichier, et libertés définissant plusieurs exceptions générales au principe d'interdiction :

• lorsque le consentement exprès de la personne a été recueilli, ou lorsque cette dernière a rendu publiques les données en question ;
• lorsque le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
• dans le cas de la recherche médicale ou de la médecine préventive ;
• au bénéfice des associations religieuses, politiques, philosophiques ou syndicales ;
• lorsque le traitement a une finalité statistique réalisée par l'INSEE ;
• lorsque le traitement a fait l'objet d'une d'anonymisation reconnue par la CNIL ;
• lorsque le traitement fait l'objet de formalités de contrôle (article 25-I et 26-II) ;

On remarque ainsi que le traitement de données sensibles est possible lorsqu'il est expressément soumis au formalisme des articles 25-I et 26-II. Les traitements de donnée biométrique étant soumis à ces procédures spécifiques, on peut en déduire que le législateur a implicitement entendu traiter les données biométriques comme des données sensibles, ce qui conforterait d'ailleurs l'opinion de la CNIL.

• Des données publiques ?

Il est une notion présente dans la loi informatique, fichiers et libertés, rarement mentionnée et qui appelle à commentaire. Il vient d'être dit que la collecte de données sensibles était autorisée

[105] Le responsable d'un traitement qui exerce une activité sur le territoire français dans le cadre d'une installation, quelle que soit sa forme juridique, y est considéré comme établi.
[106] À l'exclusion des traitements qui ne sont utilisés qu'à des fins de transit sur ce territoire ou sur celui d'un autre État membre de la Communauté européenne.

lorsque la personne concernée avait « rendu publiques » les données en question[107].

Or, certains spécialistes de la sécurité informatique affirment que les données biométrique sont des données publiques. Elles seraient de fait rendues publiques, à l'insu des personnes concernées, les marqueurs biométriques laissant des traces plus ou moins exploitables où que nous nous trouvions, quoi que nous fassions.

Impossibilité de rendre secrètes les données biométriques. - Ainsi, pour Philippe WOLF[108], toute personne peut s'approprier les données biométriques d'une autre à tout moment : données génétiques à partir d'un cheveux, d'un ongle, d'un échantillon de salive, ou d'une cellule de la peau ; empreintes digitales laissées sur un verre ou toute surface lisse - y compris les capteurs biométrique ! ; photographie haute définition du visage, de l'iris, susceptibles d'être prises sans le consentement de la personne.

Or, l'identification et l'authentification en matière de sécurité informatique repose par principe sur un secret, un mot de passe par exemple, dont la divulgation doit être limitée au maximum. Cette protection est impossible à assurer en pratique pour nos marqueurs biométriques, à moins de porter des gants, un masque, de passer l'aspirateur partout où l'on passe ou de brûler tout ce qu'on touche. L'idée selon laquelle une donnée biométrique peut être protégée plus facilement qu'un mot de passe n'est donc pas évidente. Contrairement à un mot de passe, une donnée biométrique ne peut être dissimulée dans la seule mémoire d'une personne.

De sorte que les données biométriques, si elles ne sont pas tout à fait des données « rendues publiques » au sens juridique, ne peuvent pas être des données totalement privées. Pour Philippe WOLF, il s'agit techniquement de données publiques, ce qui suffit à déconseiller leur usage au titre d'identification.

Caractère irrévocable des données biométriques. - Ce risque est d'autant plus grand que les données biométriques ne sont pas révocables. Une fois rendues publiques, ces données éventuellement appropriées et stockées par un usurpateur, compromettent l'élément corporel de l'utilisateur légitime et l'en dépossède. Les facilités de communication et de diffusion par Internet rendent ce risque encore plus important. D'autant qu'il s'agit alors de données brutes, dont il n'est pas exclu qu'elles puissent servir à la constitution d'un gabarit. Les méthodes artisanales permettant cette opération ont déjà été décrites dans les pages précédentes.

Ces données compromises, support potentiel de toute forme d'usurpation d'identité - accès non autorisé à des zones sensibles, contrefaçon de titres officiels - auraient alors intérêt à être définitivement révoquées de tout système d'identification. Dans le cadre d'un méta-système d'identification fondé sur la biométrie, cela reviendrait d'une certaine manière, à l'effacer la personne même.

En revanche, et pour poursuivre l'analogie avec le couple identifiant / mot de passe, les données biométriques pourraient servir sans risque de login. L'identifiant étant public, comme un nom d'utilisateur, une adresse email, un identifiant sur un forum, le secret serait maintenu par l'exigence d'un mot de passe, révocable en cas de perte, de divulgation ou de toute autre forme de compromission.

---

[107] On distinguera cette notion des données produites par les services de l'État, dont le régime juridique est notamment fixé par Loi n° 78-753 du 17 juillet 1978, relative à la liberté d'accès aux documents administratifs et à la réutilisation des informations publiques.

[108] Philipe WOLF, *De l'authentification biométrique*, Sécurité informatique, n°46, CNRS, octobre 2003, http://perso.orange.fr/perso.web/hebergement/biometrie/doc/WOLF_SSI_46.pdf

Dans un système idéal, un utilisateur présenterait une carte à puce contenant un gabarit de référence chiffré et sa propre donnée biométrique. La comparaison validée donnerait lieu à la reconnaissance d'un login. L'accès serait ensuite protégé par un mot de passe personnel.

Ces considérations nous permettent une nouvelle fois d'avancer l'idée qu'un système biométrique n'équivaut pas à un autre. C'est pourquoi la CNIL, à l'occasion de l'examen des nombreuses demandes d'autorisation qu'elle a eu à traiter, a pu définir des recommandations sur les modalités techniques de mise en oeuvre des dispositifs. Au point que beaucoup s'en réfèrent à une doctrine en matière de biométrie.

§ 2. La protection des données biométriques selon la CNIL

• *Modalités de conservation des données références*

Stockage externe. - La CNIL privilégie le stockage des données biométrique de référence (les gabarits) sur un support externe et mobile (clé USB, carte à puce, magnétique ou à lecture optique), par opposition à leur stockage sur une base de donnée. Il existe un mode de stockage hybride, dans la mémoire interne d'une borne biométrique permettant l'identification, qui est généralement assimilé à la constitution d'une base de donnée.

Protection contre les détournements. - Comme cela a déjà été évoqué, le fait de remettre à la personne concernée la donnée référence pour s'identifier lui permet d'en contrôler l'usage et d'en empêcher une utilisation détournée, ou une interconnexion abusive avec un autre fichier, y compris par le responsable du traitement. Le risque par exemple d'un croisement avec des fichiers de police est rendu impossible, du fait que personne n'a accès aux gabarits biométriques en dehors de l'utilisateur lui-même.

Il s'agit aussi d'une mesure préventive, dans l'hypothèse où plusieurs traitements aux finalités différentes seraient interopérables. On l'a dit, il n'y a pas - pas encore - d'interopérabilité générale des gabarits biométriques. Le responsable du traitement peut donc aussi apporter la preuve de l'existence d'une autre mesure préventive empêchant les interconnexions. Ainsi, le fait de recourir à un dispositif reposant sur une technologie autre que celle qui est utilisée par exemple pour les fichiers de police, peut également permettre à la CNIL de considérer que le traitement ne comporte pas de risque d'interconnexion illicite.

Le fait de ne pas recourir à une base de donnée permet plus généralement de contourner les dangers liés à la vulnérabilité des systèmes informatiques et à la possibilité de pirater les serveurs. Par ailleurs, la perte ou la compromission du support externe ne met pas en danger les données des autres personnes concernées par le traitement.

Responsabilisation des utilisateurs. - En contrepartie, les personnes sont davantage responsabilisées. Une protection négligente du support des données biométriques, qui serait à l'origine d'une appropriation par un tiers, d'une utilisation frauduleuse, d'un accès non autorisé à une zone sécurisée et au final, d'un préjudice causé au responsable du traitement, serait de nature à engager la responsabilité civile des utilisateurs. À noter qu'au Québec, cette obligation de sécurité de l'utilisateur est explicitement reconnue par la loi qui a intégré des dispositions spécifiques relatives à la biométrie.

Cette approche du stockage des données biométriques est celle retenue par toutes des autorités nationale et supranationale de protection. Recourir à une telle modalité donne de fortes chances d'aboutir aux demandes d'autorisation soumises à la CNIL.

Destruction des données brutes. - Les données brutes servent à la constitution des gabarits. Une fois ceux-ci créés, les données brutes ne sont d'aucune utilité pour l'identification. Le principe devrait donc être celui de la destruction des données brutes, utilisées une première fois lors de la phase d'enregistrement (enrôlement) et de manière ponctuelle, lors de l'identification (appariement).

Cette modalité du traitement est prise en compte par la CNIL pour apprécier le niveau de protection des données. Cette recommandation est conforme au principe selon lequel il ne faut pas collecter plus de données que ce qui est nécessaire à la finalité du traitement.

• Préférence pour les technologies « sans traces »

La CNIL est particulièrement stricte quant au recours aux empreintes digitales. La dactyloscopie, traditionnellement utilisée pour l'identification des criminels et des délinquants, a en effet la particularité de mettre en oeuvre un des marqueurs biométriques les plus interopérables et les plus vulnérables à une collecte déloyale. C'est également le cas de l'ADN, mais dont les applications restent plus limitées, et en l'occurrence, bel et bien cantonnées à l'identification judiciaire. Quant à la reconnaissance faciale, elle est explicitement citée par l'OACI comme la technologie biométrique de référence au niveau mondial.

À l'opposé, la reconnaissance de la géométrie de la main ou de l'iris ne comporte pas à l'heure actuelle les mêmes risques. Il est extrêmement difficile de recueillir ces données à l'insu de la personne concernée. Il s'agit de technologies qui ne laissent pas de « traces ».

Une petite visite de l'exposition de la Cité des sciences suffit à se faire une idée de l'impossibilité d'obtenir une image exploitable de l'iris sans la coopération de la personne concernée. Plusieurs tentatives sont nécessaires, à quelques centimètres du capteur. Le moindre plissement de paupière, le moindre mouvement de l'oeil, la moindre dilatation intempestive de la pupille, le moindre défaut de positionnement du visage sur le capteur empêche tout enrôlement et *a fortiori* tout identification ultérieure. Il en est de même pour la reconnaissance de la géométrie de la main, qui nécessite un positionnement des doigts en fonction d'une douzaine de repères en relief, qui ne souffre aucune imprécision. Ainsi, le fait de laisser une trace de la main sur une surface lisse ne permettra pas à un pirate de leurrer le système.

Pour la CNIL et la majorité des autorités de protection des données, l'utilisation de la géométrie de la main et de l'iris « ne pose pas de difficultés au regard de la protection des données personnelles », ces données se protégeant elles-mêmes, du fait de leurs caractéristiques et de la manière dont elles sont utilisées par les systèmes biométriques.

• Utilisation de gabarit non interopérables

Élément d'appréciation supplémentaire. - Il ne s'agit pas encore d'une recommandation de portée générale, pourtant elle nous semble suffisamment importante pour que l'on cite une décision de la CNIL qui a pris en compte ce critère.

Dans une délibération 2005-206 du 22 septembre 2005, la CNIL a autorisé la société Bloomberg L.P à mettre en œuvre un dispositif biométrique reposant sur l'empreinte digitale ayant pour finalité de contrôler l'accès logique à un service d'informations financières.

Elle s'est notamment fondée sur le fait que les gabarits n'étaient pas interopérables avec les systèmes basés sur les minuties. « *La Commission considère que dans la mesure où (...) le gabarit enregistré est généré à partir d'une analyse des caractéristiques générales du tracé des crêtes du doigt des utilisateurs et n'est pas interopérable avec les systèmes basés sur les minuties, le dispositif*

soumis par la société Bloomberg L.P. ne comporte pas de risques particuliers pour la protection des libertés et des droits fondamentaux de la personne. »

En effet, on distingue deux grandes catégories d'approches, l'une basée sur la recherche des minuties, points caractéristiques remarquables situés sur les traits formant l'empreinte, approche traditionnelle utilisée pour les fichiers de police et l'autre, plus récente, consistant à faire une analyse purement statistique de la répartition des points formant le tracé des empreintes. Dans ce dernier cas, les minuties n'y jouent aucun rôle particulier.

On peut déduire de cette décision que l'utilisation de gabarits non interopérables d'empreintes digitales, stockés et chiffrés sur une carte à puce, est également susceptible d'être pris en compte par la CNIL.

Un critère non exclusif. - La finalité du traitement, notamment dans le cadre de la coopération internationale, peut cependant justifier le recours à une technologie interopérable.

Ainsi, dans un avis du 22 novembre 2005[109] sur le projet de décret instituant le passeport électronique, la CNIL observe que cette modification du contenu du passeport résulte du règlement européen du 13 décembre 2004 et a pour but de « *mieux sécuriser le passeport, par l'établissement d'un lien plus fiable entre ce titre et son titulaire grâce à l'introduction d'éléments de sécurité communs et à l'intégration d'identificateurs biométriques interopérables* ». En effet, le projet de décret prévoit en son article 25 l'interconnexion du fichier national des passeports, non seulement avec le fichier des personnes recherchées comme c'est le cas depuis 1999, mais également avec le Système d'information Schengen et le système d'information d'Interpol.

On peut donc donner à ce critère une portée non-négligeable, essentiellement en matière de traitements opérés pour le compte de personnes privées. Au regard des risques qui ont déjà été présentés concernant l'interopérabilité, et plus généralement, de la doctrine de la CNIL concernant la sectorisation des identifiants (identifiants de santé, identifiants fiscaux ...), on pourrait voir dans cette décision l'embryon d'un principe de sectorisation des gabarits, voire des technologies biométriques.

• Chiffrement des données biométriques

Il s'agit là encore d'un élément d'appréciation qui n'a pas de valeur obligatoire, mais qui donne à la CNIL un élément d'appréciation sur les mesures de protection des données que le responsable entend mettre en oeuvre pour un traitement. Le chiffrement des données biométriques est ainsi régulièrement relevé par la CNIL.

Un élément d'appréciation supplémentaire. - Ainsi, dans ses 17 décisions du 12 mai 2006 sur l'accès aux casinos[110], la CNIL a autorisé la mise en place de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale ayant pour finalité le contrôle de l'accès à certains casinos. Il n'y avait en l'espèce pas d'impératif de sécurité mais l'obligation de contrôler l'entrée des personnes interdite de jeu à l'entrée des établissements en question. La CNIL relève notamment que les gabarits biométriques sont stockés sur une carte individuelle - qui fait au final, office de licence -, ces gabarits faisant l'objet d'un chiffrement.

La CNIL a relevé également l'existence d'un chiffrement également dans une délibération 2005-001 du 13 janvier 2005 : « *La Commission relève en outre qu'en complément de l'algorithme*

[109] Délibération n°2005-279
[110] Délibérations 2005-262 à 2005-278

de chiffrement utilisé pour les badges dits "sans contact", les données biométriques font l'objet d'un chiffrement supplémentaire et que les données contenues dans le badge ne peuvent être activées que dans la limite d'une distance de trois centimètres du lecteur ».

De même, dans son avis[111] sur le projet de visas biométriques, la CNIL a considéré que le recours aux empreintes digitales du détenteur du visa était adéquat, pertinent et non excessif au vu des modalités envisagées. Pour la CNIL, les conditions de sécurité étaient satisfaisantes « *dès lors que des précautions particulières étaient adoptées lors de l'enrôlement des données biométriques, et que des mesures de sécurité spécifiques étaient prises pour garantir la confidentialité des données, tout particulièrement contre les risques de captation irrégulière, notamment grâce à des méthodes sûres de chiffrement et de signature électronique* ».

Le groupe de l'article 29 s'est prononcé dans le même sens dans un avis[112] sur l'insertion d'éléments biométriques dans les visas. « *Le groupe souhaite disposer, au moment opportun avant décision d'adoption, d'un document démontrant que les spécifications envisagées pour l'insertion des données dans les puces et leur accès assurent que les données ne pourront être accessibles ni à l'insu des personnes concernées, ni par des personnes publiques autres que celles qui en ont légalement le pouvoir, ni par des personnes privées. Il serait approprié, à cet égard, de prévoir que les données doivent faire l'objet d'un chiffrement pour en assurer la confidentialité* ».

Une obligation légale implicite ? - Plus généralement, le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Le recours à des procédés de cryptographie, parallèlement à des mesures physiques de sécurité, paraît être à l'heure actuelle incontournable, bien que la loi ne le précise pas, préfigurant peut-être l'avènement de technologies encore plus fiables.

Eût égard cependant à la nature particulière des données biométriques et du silence de la loi, le chiffrement des données biométriques devrait être une obligation expresse. Elle n'est que très implicitement visée par la loi informatique, fichiers et libertés, là où elle est reconnue en droit civil au titre de la signature électronique et du droit public, par exemple dans le Code des marchés publics.

Depuis quelques années, il est revenu au droit de définir certaines modalités techniques permettant de s'assurer de l'effectivité des règles de droit. Au demeurant, des décrets devaient fixer les prescriptions techniques auxquelles doivent se conformer certains traitements mais ils sont inexistants aujourd'hui. Or, le chiffrement est indéniablement une sécurité supplémentaire importante, dont le contournement requiert la mobilisation de ressources humaines, intellectuelles et matérielles considérables.

Faire du chiffrement une simple option à la disposition du responsable du traitement nous paraît être préjduciable. Il s'agit d'une véritable garantie, qui ne fait pas obstacle par ailleurs à une l'utilisation légitime des données biométriques par l'autorité judiciaire, l'article 230-1 du Code de procédure pénal[113] prévoyant la possibilité pour le procureur de la République, le juge d'instruction, ou la juridiction de jugement, d'ordonner le déchiffrement des données saisies lors d'une enquête.

---

[111] Délibération n°04-075 du 05 octobre 2004

[112] Groupe de travail sur la protection des données (Article 29), Avis n° 7/2004 du 11 août 2004, sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visas (VIS).

[113] Loi nº 2001-1062 du 15 novembre 2001, loi relative à la sécurité quotidienne

Ainsi, les magistrats peuvent « *désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire* ».

SECTION 2. Droits des personnes concernées et obligations des responsables

L'applicabilité de la loi aux données biométriques donne des droits aux personnes concernées par les traitements et des obligations aux responsables du traitement. Ces droits et obligations sont ceux du régime de droit commun de protection des données, applicables à tout type de données.

Étant admis qu'il serait inutile de paraphraser la loi informatique, fichiers et libertés, on se bornera simplement à soulever les problèmes d'applications que le traitement et la collecte de données biométriques sont susceptibles de soulever, au regard des droits et des obligations consacrés par elle.

SOUS-SECTION 1. Droits des personnes concernées

§1. Droits relatifs à la collecte et au traitement

• ***Consentement***

La loi informatique, fichiers et libertés pose le principe du consentement préalable. Aux termes de l'article 7 qui dispose « *un traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée* » avec plusieurs exceptions.

Le consentement n'est pas qualifié. Inversement, la loi précise les cas dans lesquels un traitement requiert un consentement *exprès* de la personne concernée. On pourrait en déduire *a contrario* qu'un consentement tacite suffit à pouvoir mettre en oeuvre les traitements de droit commun, ce consentement devant en revanche être exprès pour la collecte de données sensibles.

En l'absence de qualification des données biométriques, on ignore si la loi implique de recueillir un consentement exprès de la personne concernée. Tout au plus, peut-on s'inspirer des règles particulières relatives aux traitements mis en oeuvre aux fins de recherche dans le domaine médical : « *dans le cas où la recherche nécessite le recueil de prélèvements biologiques identifiants, le consentement éclairé et exprès des personnes concernées doit être obtenu préalablement à la mise en oeuvre du traitement de données* ».

On ne voit pas pourquoi cette règle devrait être cantonné à la recherche médicale, l'ensemble des autorités de protection des données considérant le consentement préalable de la personne comme indispensable.

Le fait que l'on puisse recueillir des données biométriques à l'insu de la personne devrait être pris en compte, pour poser un principe de consentement exprès, mais également de collecte directe auprès de la personne concernée, comme cela a été fait dans certains pays comme le Canada.

• ***Droit d'information***

Catégories d'information. - Aux termes de l'article 39 de la loi informatique, fichiers et libertés, toute personne physique justifiant de son identité peut obtenir du responsable du traitement des informations sur le traitement, dont notamment :

• la confirmation que des données la concernant font ou ne font pas l'objet de ce traitement ;

• les finalités du traitement et les catégories de données traitées ;
• les destinataires ou catégories de destinataires auxquels les données sont communiquées ;
• les informations relatives aux éventuels transferts de données vers un État tiers à l'Union.

Aux termes de l'article 32, la personne auprès de laquelle sont recueillies des données la concernant est notamment informée par le responsable du traitement :

• de l'identité du responsable du traitement et, le cas échéant, de celle de son représentant ;
• de la finalité poursuivie par le traitement auquel les données sont destinées ;
• des destinataires ou catégories de destinataires des données ;
• des droits qu'elle tient des dispositions de la section 2 du présent chapitre ;
• des transferts de données envisagés à destination d'un État tiers à l'Union.

Droit du travail. - Le recours à un dispositif biométrique suppose également de respecter les règles de droit du travail en vigueur, notamment celles relative à l'information et la consultation du comité d'entreprise.

Ainsi, le TGI de Paris[114] a posé parmi les *« conditions préalables de mise en œuvre du système biométrique* » l'information des salariés au titre de l'article L 121-8 du Code du travail. Cet article dispose qu'« *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* ».

En l'espèce, un courrier individuel avait été adressé aux salariés présentant le nouveau mode de gestion et contrôle des temps de présence par pointage biométrique, afin de permettre d'éviter toutes les difficultés liées à la gestion du temps, ce qui a permis aux juges de considérer que le traitement avait satisfait aux exigences d'information des salariés.

§2. Droits sur les données biométriques

• *Particularité et portée limitée du droit d'accès*

Aux termes de l'article 39 de la loi informatique, fichiers et libertés, toute personne physique justifiant de son identité peut obtenir du responsable du traitement la communication, « *sous une forme accessible* », des données à caractère personnel qui la concernent.

L'interprétation et la vérification des données pourrait nécessiter la présence d'un expert. Le responsable de traitement ne devrait pas pouvoir refuser de telles demandes au seul motif qu'une machine ou un expert ne sont pas disponibles.

Accès aux gabarits. - Les gabarits sont des données d'un type particulier, puisqu'ils ne sont pas traitées sous forme alphanumérique. Il s'agit de fichiers structurés, exploitables uniquement par le système qui les a créés. Il peut même s'agir d'un format ou d'un langage de programmation propriétaire. De sorte que la lecture du gabarit peut éventuellement se faire à partir d'une application texte mais le fichier apparaîtra sous une forme inintelligible et sera de toute façon trop volumineux. Ainsi, il conviendrait de mettre à disposition de la personne concernée des moyens matériels ou logiciels pour consulter effectivement le gabarit (lecteur, application …). Cependant, la lecture du gabarit correspond au traitement de la donnée brute au moment de l'enrôlement, et on peut s'interroger sur l'intérêt de se voir communiquer un fichier de ce type. L'étendue ou la pertinence de ce droit ici conféré, semble bien dérisoire.

[114] TGI de Paris, 1ère chambre, section sociale, jugement du 19 avril 2005.
http://perso.orange.fr/perso.web/hebergement/biometrie/doc/TGIPARiS_250405.pdf

Accès aux données brutes. - Quant aux données brutes éventuellement conservées, il s'agit la plupart du temps d'images numérisées qui doivent être accessibles. Leur lisibilité n'est *a priori* pas une limite, puisqu'il existe en matière d'images numériques une large interopérabilité.

Limites au droit d'accès. - Dans plusieurs hypothèses, le droit d'accès pourrait ne pas s'appliquer ou ne s'appliquer qu'indirectement. Lorsqu'un traitement a été autorisé par la CNIL, comme c'est le cas pour des traitements de données biométriques, on peut considérer qu'elle les autorise parce que les modalités de mise en œuvre ne portent pas atteinte à la vie privée (stockage externe, données sans traces …).

Or le législateur a réservé la possibilité de déroger aux dispositions régissant le droit d'accès « *lorsque les données sont conservées sous une forme excluant manifestement tout risque d'atteinte à la vie privée des personnes concernées* ». On peut se demander si la CNIL, en prescrivant une forme particulière de stockage excluant tout risque d'atteinte à la vie privée, ne prive pas *de facto* les personnes concernées de droit d'accès.

Il convient enfin de réserver l'hypothèse des fichiers de police, de gendarmerie, (article 41) d'imposition et d'infraction (article 42), qui ne font l'objet que d'un droit d'accès indirect : la demande est adressée à la CNIL qui désigne l'un de ses membres pour mener les investigations utiles et faire procéder aux modifications nécessaires. Lorsque la CNIL constate, que la communication des données ne met pas en cause la sûreté de l'État, la défense ou la sécurité publique, ces données peuvent être communiquées au requérant.

• ***Modification.***

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.

Quelle est la capacité d'une personne à évaluer l'exactitude d'une donnée biométrique ?

Les gabarits ne sont pas des données aussi objectives que la nationalité, le sexe, ou l'âge. En pratique, un gabarit n'est intelligible que par la machine. Si la personne concernée peut accéder à la machine, elle soumet nécessairement l'appréciation de l'exactitude des données à l'outil informatique. Si on procède manuellement, il faut rappeler que la comparaison d'empreinte digitale est une compétence et un métier à part entière. Qu'elle est donc la portée de ce droit de modification en matière de données biométrique ? Là encore, la question reste en suspens.

SOUS-SECTION 2. Obligations des responsables du traitement

§1. Devoir de loyauté

Ce concept juridique, issu du droit des obligations, est à la responsabilité délictuelle ce que la bonne foi est aux obligations contractuelles. On pourrait même aller plus loin, en reprenant totalement la terminologie du droit des obligations en considérant que le responsable du traitement doit agir « en bon père de famille ». Il n'est pas fait référence à un devoir de loyauté dans la loi informatique, fichiers et liberté, mais seulement à l'obligation d'une collecte et d'un traitement loyal et licite (article 6). On peut cependant regrouper sous cette appellation l'obligation d'information existant à la charge du responsable du traitement et le respect des principes de proportionnalité et de finalité du traitement.

• ***Obligation d'information***

Le droit de la personne concernée d'être informée a pour corollaire une obligation d'information à la charge du responsable. Les informations à communiquer sont celles du droit commun. Il s'agit notamment de la finalité poursuivie, des destinataires ou catégories de destinataires des données, des droits des personnes concernées, le cas échéant, des transferts de données à caractère personnel, envisagés à destination d'un État non membre de la Communauté européenne. L'identité du responsable du traitement doit également être communiquée, ce dernier point appelant à un commentaire.

Détermination du responsable du traitement. - Le responsable de traitement est la personne qui détermine la finalité des données, les catégories de données collectées et les opérations qui leur seront appliquées. Aux termes de la loi, il s'agit plus précisément de la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement. Or, comme le souligne le Conseil de l'Europe, il n'est pas toujours facile d'identifier le responsable du traitement dans le cas des systèmes biométriques.

Par exemple, le traitement de données biométriques en relation avec la délivrance des passeports biométriques est en pratique mis en oeuvre par les autorités locales qui traitent les demandes, centralisent les données, font fabriquer les passeports par l'Imprimerie Nationale. Pourtant la finalité du traitement et les catégories de données collectées sont définies par le législateur. Il est également fréquent que les responsables de traitements de données biométriques aient recours à la sous-traitance.

De manière générale, cette situation ne doit pas empêcher les personnes concernées d'être en mesure d'établir clairement qui est le responsable et de savoir auprès de qui exercer un recours.

Principe d'information préalable et de consentement. – Le principe de loyauté implique que la collecte des données biométriques ne se fasse pas à l'insu des personnes. Ces procédés devraient même être proscrits selon le Conseil de l'Europe. Certains systèmes biométriques, comme la reconnaissance faciale à distance, la collecte d'empreintes digitales ou l'enregistrement de la voix, présentent davantage de risques à cet égard.

Aux termes de l'article 7 de la loi, le traitement doit avoir reçu le consentement de la personne concernée, ce qui implique une obligation de la part du responsable de recueillir le consentement de la personne. On sait cependant que certains moyens de pressions existent pour obtenir le consentement d'une personne dans le cas des traitements de données à caractère personnel : signature d'un contrat de travail, d'un contrat d'adhésion... En dehors des traitements opérés pour le compte de l'État, ou des traitements nécessités par des impératifs de sécurité, les traitements biométriques « de confort » devraient se faire sur la base du volontariat, avec la possibilité pour les personnes concernées de disposer d'un moyen d'identification moins invasif. C'est le principe retenu par exemple, en matière d'accès aux restaurants scolaires.

Il existe une disposition relative aux informations recueillies par les prestataires de services de certification électronique pour les besoins de la délivrance et de la conservation des certificats liés aux signatures électroniques. Ces données doivent être directement recueillies auprès de la personne concernée. Sur ce modèle, un principe de collecte directe des données biométriques auprès de la personne concernée, principe adopté par exemple au Québec, permettrait de donner davantage de poids au devoir de loyauté, qui reste assez abstrait.

• ***Respect du principe de finalité et de proportionnalité***

Finalité. - Aux termes de l'article 6 de la Loi Informatique, Fichiers et Libertés, les données doivent être collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités. L'alinéa 5 prévoit de plus qu'elles ne doivent pas être conservées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitées. Il en résulte une obligation générale du responsable de respecter le principe de finalité.

Ce principe interdit donc aux responsables d'appliquer aux données un traitement ultérieur incompatible avec la finalité initiale sauf dérogations. Il ne peut être donc être contrôlé *qu'a posteriori*.

Proportionnalité. - Le principe de proportionnalité découle notamment de l'article 6 qui dispose que les responsables du traitement ne doivent utiliser que des données adéquates, pertinentes et non excessives, ce qui implique une évaluation rigoureuse du type de technologie biométriques, et donc du type de données traitées, susceptible de répondre à la finalité en cause.

Le principe de proportionnalité doit inciter les responsables à réfléchir à la possibilité d'une méthode alternative moins intrusive. Ainsi, pour le groupe article 29, le principe de finalité appliqué à la biométrie « *doit obliger les responsables à prendre en compte des risques relatifs aux libertés et aux droits fondamentaux* ».

De même, la question de l'anonymisation doit être envisagée, un gabarit biométrique pouvant être associé à une habilitation par exemple, sans référence à l'identité civile de la personne.

De plus, selon le Conseil de l'Europe, il serait contraire au principe de proportionnalité d'exiger qu'un système employant des données biométriques soit plus précis que ne le requiert la finalité initiale de ce système, « *pour l'unique raison que dans des cas exceptionnels les données pourraient être requises pour une finalité secondaire, comme par exemple la répression d'infractions pénales* ». Ainsi, en fonction de la finalité, l'analyse d'une donnée biométrique peut aboutir à la constitution d'un gabarit à 12 points, la constitution d'un gabarit plus précis à 50 points pouvant être jugé disproportionné.

On constate que beaucoup de règles ne peuvent qu'être déduites du devoir de loyauté, qui constitue un concept abstrait. Cette abstraction est cependant nécessaire. Elle permet de responsabiliser encore davantage le responsable du traitement. C'est en ce sens que l'on peut se référer à l'appréciation objective de son comportement, selon le modèle du « bon père de famille », et donc ne pas limiter ses initiatives à une liste d'obligation définitives. Ce constat est également vrai au regard de l'obligation de sécurité.

§2. Obligation de sécurité

Sécurité et confidentialité. - Aux termes de l'article 34 de la loi informatique, fichiers et libertés, le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

Par ailleurs, l'article 17 de la directive 95/46/CE, dispose que le responsable du traitement doit « *prendre toutes les mesures de sécurité techniques et organisationnelles appropriées pour protéger les données à caractère personnel* ».

Aucun texte ne prévoit expressément les méthodes technologiques ou organisationnelles de protection des données. Il s'agit ici sans doute d'une volonté de ne pas limiter les initiatives en ce domaine, ou risquer de graver dans le marbre législatif une technologie particulière, amenée un jour ou l'autre à l'obsolescence.

Référence implicite à l'état de l'art. - Le Conseil de l'Europe donne cependant quelques indications supplémentaires, relatives à l'obligation de sécurité pour la protection des données biométriques. Il prévoit ainsi que les normes de qualité relatives aux programmes et au matériel informatique puissent être définies par le secteur industriel « *en particulier pour les applications à grande échelle et les systèmes qui exigent un niveau de sécurité élevé* ». Le Conseil ajoute que les autorités de protection des données devraient veiller à ce que les standards techniques intègrent aux technologies la protection des données et les obligations relatives à l'application de la Convention

Formation du personnel. - Pour le Conseil, la formation et la sensibilisation du personnel devraient aussi être prises en compte au titre de l'obligation de sécurité.

Cryptage des données. Cet aspect ayant déjà été étudié dans les pages précédentes, nous rappellerons simplement qu'il ne s'agit pas d'une obligation, quand bien même le cryptage des données offre une garantie importante en termes de sécurité, notamment contre les détournements de finalité par des tiers qui auraient accès aux données. Par ailleurs, le groupe article 29 précise que le chiffrement des données doit s'accompagner de la mise en place d'un système de contrôle d'accès aux clés de cryptage et de protection de celles-ci.

Mesures organisationnelles. - Des mesures de sécurité particulières sont requises à la phase d'enrôlement, car c'est à ce stade que l'on « fixe » une identité. Pour le groupe article 29, cette phase est cruciale dans le sens où un enrôlement défectueux *« pénaliserait manifestement toutes les applications futures basées sur les informations contenues dans ces bases de données et infligerait un préjudice irréversible aux personnes concernées* ».

Toutes les mesures physiques de sécurité doivent être prise en considération. Ainsi, la protection et le contrôle d'accès aux locaux abritant les serveurs informatiques sur lesquels sont stockées les données doit être assurée. Le paradoxe est que ces contrôles d'accès physiques ou logiques aux données biométriques pourraient inciter à recourir à un dispositif biométrique, afin d'identifier les administrateurs du système, dispositif biométrique qui lui-même devrait être sécurisé afin de prévenir l'usurpations du statut d'administrateur !

Une politique de sécurité devrait donc être mise en place pour déterminer les niveaux et les matrices d'habilitations, sécuriser des clés de chiffrement, contrôler les accès logiques et physiques aux serveurs.

Obligation de résultat. - Il n'appartient pas au législateur de définir trop précisément ces obligations, bien que la loi prévoie expressément que des décrets, pris après avis de la CNIL, puissent fixer des prescriptions techniques pour certains traitements. En effet, ce serait offrir aux responsables du traitement une possibilité d'exonération. Ces derniers pourraient ainsi apporter la preuve qu'ils n'ont pas commis de faute en ayant respecté des prescriptions techniques plus ou moins pertinentes.

Il semble à l'inverse plus conforme au droit de la responsabilité délictuelle de faire peser sur eux une responsabilité sans faute. En effet, en mettant en oeuvre un traitement dont ils tirent un profit, plus ou moins directement, les responsables créent un risque qui justifie une obligation de sécurité de résultat. En leur appliquant la théorie du risque, utilisée par exemple en matière de produits défectueux, on permet aux victimes de ne pas avoir à apporter la preuve d'une faute du

responsable, celle-ci étant présumée. La seule possibilité d'exonération pour le responsable sera à alors la preuve de l'existence d'une cause étrangère.

Chapitre 2.
ÉVOLUTION DU DROIT DES DISPOSITIFS ET DES DONNÉES BIOMÉTRIQUES

SECTION 1. Uniformisation, harmonisation ou consolidation ?

Les règles de protection des données biométriques sont encore diffuses et protéiformes. Chaque traitement a ses finalités propres, des modalités de mise en oeuvre différentes, des risques plus ou moins prononcés au regard de la vie privée. Cet éclatement du droit est en partie inévitable, à moins de considérer que la loi doit appréhender de manière exhaustive toutes les formes de traitement, et innerver d'en haut tout le droit Informatique et Libertés. Et il n'est pas sûr que l'inflation législative soit utile à la protection des données.

Ce constat n'empêche cependant pas de remarquer que beaucoup des règles en question se recoupent, se répète, se font écho. La question d'une consolidation ou d'une harmonisation du droit des données biométriques n'est peut-être pas à exclure.

Harmonisation du 3è pilier. - On peut regrouper les traitements de données biométriques en trois grandes catégories. Les traitements de la première catégorie font l'objet de textes spéciaux, dans le cadre de la coopération judiciaire et policière en Union Européenne. Il s'agit essentiellement des fichiers SIS II et VIS, de leur interopérabilité avec les titres d'identité, passeports, et visas. Si chaque fichier obéit aujourd'hui à des règles propres, un projet de directive-cadre[115] relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale est aujourd'hui à l'étude. Il existe donc pour le troisième pilier une possibilité d'harmonisation.

Au cours de la Conférence de Budapest des 24 et 25 avril 2006, les autorités européennes de protection de données ont ainsi déclaré : « *Aucune alternative n'existe à la création d'une norme de protection des données harmonisée et de haut niveau dans le troisième Pilier de l'UE. Celle-ci est une conséquence logique du programme de la Haye, selon lequel la sauvegarde de la liberté, la sécurité et la justice sont des éléments indivisibles tant des missions de l'UE dans son ensemble que des mesures récemment prises au niveau européen telles que le système d'information visa (VIS), le système d'information Schengen II (SIS II) ou l'interopérabilité des bases de données européennes dans le secteur de la justice et des affaires intérieures* ».

Les fichiers biométriques nationaux. - Une seconde catégorie de fichiers est constituée par les fichiers biométriques nationaux, souvent complémentaires aux dispositifs européens précités. Ces fichiers ont généralement été créés par décret ou par arrêté, fixant les règles applicables échappant en partie au droit commun. Par exemple, le régime du fichier FNAED a d'abord été définit par un décret n °87-249 du 8 avril 1987.

[115] http://www.libertysecurity.org/IMG/pdf/COM_2005_475_final.pdf

Traitement régit par le droit commun. - C'est cette catégorie qui nous intéresse particulièrement. Elle regroupe en substance les traitements opérés par les sociétés privées et certaines personnes de droit public. En effet, on peut aujourd'hui considérer qu'une harmonisation est souhaitable pour cette catégorie. La doctrine de la CNIL est aujourd'hui extrêmement stable, voire prévisible, au point que l'autorité française a pu prendre des autorisations uniques qui ressemblent fortement à des tentatives de consolidation.

Or, cette doctrine est parfaitement cohérente avec celles des autorités nationales européennes saisies des questions relatives à la biométrie, mais aussi des autorités supranationales. Il existe aujourd'hui une certaine convergence autour de l'évaluation des risques et des solutions préconisées. Cette approche comparatiste des recommandations existantes en la matière, donne ainsi d'importants éléments d'appréciation quant à la pertinence d'une harmonisation, ou d'une consolidation du droit des données biométriques.

SOUS-SECTION 1. La convergence des doctrines

§ 1. La convergence des doctrines nationales

• Le Luxembourg, en voie d'harmonisation parfaite avec le droit français

Une doctrine conforme à celle de la CNIL. - L'étude du droit luxembourgeois au regard de la biométrie révèle une approche très similaire de celle du droit français. Les documents d'analyse font d'ailleurs très souvent référence aux décisions de la CNIL. Ainsi, la Commission nationale de protection des données du Luxembourg a eu l'occasion de se prononcer plusieurs fois sur des traitements de données biométriques, bien que contrairement à la loi de 1978, la loi luxembourgeoise ne les mentionne pas. La loi du 2 août 2002 « *relative à la protection des données des personnes à l'égard du traitement des données à caractère personnel* » contient en revanche des restrictions spécifiques liées à l'usage des données génétiques.

C'est donc en interprétation de la loi du 2 août 2002 que la CNPD a récemment autorisé l'établissement public Domaine Thermal de Mondorf[116] à mettre en œuvre un dispositif biométrique pour ses abonnés.

Le contrôle de proportionnalité de la CNPD se fonde sur les mêmes critères que ceux utilisés par la CNIL. Notamment, l'autorité luxembourgeoise relève que les gabarits biométriques sont stockés sur support externe (en l'espèce des « bracelet-chips ») pour autoriser le traitement. La CNDP avait estimé dans une délibération précédente[117] que le recours par le même requérant à une base de données d'empreintes digitales n'était pas proportionné au but recherché.

Traitements de surveillance. - La CNDP va cependant plus loin que la CNIL, en considérant que les traitements biométriques sont pas nature des traitements « de surveillance ». En effet, l'article 2, lettre (q), de la loi luxembourgeois définit la surveillance comme « *toute activité faisant appel à des moyens techniques en vue de détecter, d'observer, de copier ou d'enregistrer des mouvements, images, paroles, écrits, ou l'état d'un objet ou d'une personne fixe ou mobile* » ce qui inclue la vidéosurveillance et toute forme de surveillance électronique[118], dont la biométrie,

---

[116] CNPD, délibération n°33/2006 du 12 avril 2006, http://www.cnpd.lu/objets/deliberation_33_2006.pdf

[117] CNPD, délibération n°89/2005 du 21 décembre 2005, http://www.cnpd.lu/objets/deliberation_89_2005.pdf

[118] « *Outre les caméras, tombent dans cette catégorie les détecteurs de mouvements, à condition toutefois qu'ils permettent d'identifier, directement ou non, une personne. Sont surtout visés ici les (…) portiques et points de passage qui identifient les personnes qui les franchissent (La Protection des données personnelles, Cyril PIERRE-BEAUSSE, éd. Promoculture, n°162). En l'espèce, le système utilise une borne d'accès qui détecte et enregistre les mouvements des abonnés du « Club » et constitue par conséquent un traitement de surveillance.* »

selon les rapports parlementaires (n°4735/0 p.36 et 4735/13 p.97.)

Projet de loi incluant les données biométriques. - Un projet de loi[119] n°5554 portant modification de la loi du 2 août 2002 a été dépose à la Chambre des Députés le 16 mars 2006. Ce projet permet au Luxembourg d'aligner sa position sur celle de la France, puisque l'article 14 soumet explicitement à autorisation les « *traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes* » sauf lorsqu'ils concernent la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'État. Par ailleurs, le projet de loi prévoit la suppression des formalités préalables pour certaines catégories de traitements afin de « *permettre à la Commission nationale de réorienter ses moyens d'action vers des activités jugées prioritaires à savoir l'examen des projets sensibles, notamment les données génétiques ou biométriques* ».

Au final, pour la CNPD, l'opportunité de l'utilisation de la biométrie dépend fortement de « *la finalité de son application et de la configuration du système biométrique* », ce qui a le mérite d'être parfaitement conforme à la doctrine dominante. Elle recommande de renoncer à traiter des données biométriques si l'identification des personnes peut être réalisé avec la même efficacité et sécurité avec des moyens moins intrusifs.

• Le contrôle de proportionnalité par la Garante italienne

L'autorité italienne de protection des données ne se distingue pas des lignes directrices énoncées. On peut ainsi relever deux décisions relatives à l'utilisation des empreintes digitales, dont les finalités et les modalités de mise en oeuvre étaient différentes.

Contrôle d'assiduité sur le lieu de travail. - Dans une décision[120] du 21 juillet 2005, l'autorité italienne de protection des données (*Garante Per La Protezione Dei Dati Personali*) n'a pas autorisé la société Landini S.p.A à mettre en oeuvre un traitement de données biométriques dont la finalité était le contrôle de l'assiduité sur le lieu de travail. Les conditions techniques du traitement, notamment le stockage centralisé des « *codes d'identification issu des données biométriques* » - les gabarits - sur le système d'information de la société, ont suffit à convaincre l'autorité de contrôle que le traitement était illicite.

Pour la *Garante*, un tel traitement pouvait en effet porter préjudice aux droits individuels, si les mesures de sécurité étaient contournées, si des personnes non autorisées avaient accès aux données, ou si les données stockées étaient utilisées à d'autres fins, y compris par des tiers. Elle précise qu'il est préférable de recourir à des méthodes moins invasives, comme le stockage du code d'identification sur un médium détenu exclusivement par la personne concernée. C'est donc aux termes des sections 3, 11, 17 et 154(1), d), du Code de protection des données que le traitement a été interdit.

Contrôle d'accès aux zones réservées. - En revanche dans une décision[121] du 23 novembre 2005, la Garante a autorisé la société Galileo Avionica S.p.A. à mettre en oeuvre un traitement de données biométriques dont la finalité était le contrôle d'accès à des zones réservées. Les activités en question nécessitaient des moyens d'identification en rapport avec les standards stricts et spécifiques de sécurité auxquels devait se conformer la société requérante, et avec les projets industriels classés « secret défense » dont elle avait la charge. Cette société avait également comme impératif de pouvoir *a posteriori*, déterminer avec certitude l'identité des personnes présentes sur le site.

---

119 http://www.cnpd.lu/fr/objets/actualites/doc_pdl_5554.pdf

120 http://www.garanteprivacy.it/garante/doc.jsp?ID=1166892

121 http://ec.europa.eu/justice_home/fsj/privacy/docs/policy_papers/italy/biometrics_prior_checking05.pdf

La *Garante* relève ainsi que les gabarits des empreintes digitales seront chiffrés et stockés sur un support détenu exclusivement par l'employé, et autorise finalement le traitement, considérant que les modalités techniques de mise en oeuvre sont proportionnées à la finalité envisagée.

• Le contrôle strict en République Hellénique

Les décisions de l'autorité grecque révèlent une approche sensiblement plus stricte et encore davantage centrée sur le type de technologie biométrique utilisée.

Géométrie de la main. - Ainsi, dans une décision n°09/2003[122], l'autorité grecque rappelle le principe énoncé dans une décision de référence[123] et applique le même critère pour autoriser un traitement de données biométriques. En l'espèce, le recours à la technologie de la géométrie de la main dans le but de contrôler l'accès des employés aux zones sensibles du ATTIKO METRO a été jugé proportionné au but poursuivi. Plus généralement, l'autorité précise que les traitements doivent être analysé au cas par cas, et en considération du type de données biométrique en jeu.

Empreintes digitales, domaine réservé de la lutte contre le crime. - Dans la décision antérieure citée par l'autorité, cette dernière avait estimé que la surveillance et le contrôle de présence des employés pouvaient être réalisés par des moyens plus modérés, l'identification des personnes au moyen des empreintes digitales ayant toujours été et étant encore utilisée dans le cadre de la lutte contre le crime. Ainsi, l'enregistrement de données biométriques pour le contrôle de présence « *ne contrebalance pas la nécessaire protection de la vie privée des personnes et ne justifie pas que l'on déroge au principe général selon lequel les autorités légalement habilitées sont seules à pouvoir recourir à de tels traitements* ».

Il est enfin précisé qu'une telle dérogation ne pourrait être admise que pour contrôler l'accès à des zones réservées, où sont par exemple gardées des informations confidentielles. En l'espèce, le traitement avait été interdit en vertu de l'article 21 de la loi 2472/97 et déclaré illégal, le refus de se soumettre au traitement par les employés ne pouvant constituer une faute contractuelle justifiant une quelconque sanction, de même que leur consentement ne peut légitimer la mise en oeuvre du traitement.

Iris et empreintes digitales dans les aéroports. - Un projet pilote européen auquel participait l'Association Internationale de transport aérien avait pour objet de définir un modèle d'identification biométrique reposant sur la reconnaissance de l'iris et des empreintes digitales des passagers enregistrés avant les vols. Il s'agissait de s'assurer que la personne qui s'enregistre est bien la même personne qui embarque, en plaçant des bornes à l'enregistrement et à l'embarquement. L'expérimentation visait les aéroports d'Athènes et de Milan.

L'autorité de contrôle a considéré[124] en l'espèce que le traitement envisagé était illicite et ne devait pas être autorisé. D'autres moyens moins contraignants, comme la présentation d'une carte d'identité, du billet d'avion et de la carte d'embarquement suffisait à atteindre le but poursuivi. Le traitement de données biométriques répondait moins à un impératif de sécurité qu'à une démarche organisationnelle.

---

[122] Hellenic Republic Data Protection Authority, décision n°09/2003 du 31 mars 2003 http://www.dpa.gr/Documents/Eng/09_2003.doc

[123] Hellenic Republic Data Protection Authority, décision du 20 mars 2000 http://www.dpa.gr/Documents/Eng/245_9_2000.doc

[124] Hellenic Republic Data Protection Authority, décision n° 52/2003 du 20 mars 2000 http://www.dpa.gr/Documents/Eng/Dec%2052%202003%20Biometrics_IAA.doc

§ 2. La convergence des recommandations des autorités supranationales

Ces exemples nous ont montré à quel point une doctrine internationale semble se dégager. On aurait encore pu citer l'exemple du Portugal, où l'autorité chargée de la protection des données a interdit à une université de centraliser des gabarits d'empreintes digitales du personnel non enseignant pour contrôler leur assiduité et leur ponctualité, ou encore celui de l'autorité allemande, qui a rendu une décision favorable concernant l'introduction de caractéristiques biométriques dans les documents d'identité, en l'absence de constitution d'une base de donnée.

L'étude des travaux publiés par les autorités supranationales de protection des données ne fait que confirmer cette tendance. On ne rentrera pas ici dans les détails des avis et recommandations de ces autorités. Il existe aujourd'hui un large consensus sur les risques de la biométrie, les interrogations qu'elle suscite, et les principes techniques et juridiques qui permettent en partie d'y répondre. On se bornera donc à mentionner les documents de références dans le domaine publiés par ces instances internationales ou européennes.

• *Groupe de travail sur la sécurité de l'information et la vie privée (OCDE)*

Outre les et les cadres réglementaires et moyens de sécurité – matériel anti-effraction, jeton de confiance, cryptage, l'OCDE considère nécessaire d'intégrer la biométrie dans une architecture globale de sécurité *et* de protection de la vie privée. Pour l'OCDE[125], un des éléments essentiels de cette architecture réside dans le choix de l'emplacement physique du gabarit biométrique.

« *Le stockage du gabarit biométrique sur une carte à puce au lieu d'une base de données centralisée pourrait résoudre en partie bon nombre de problèmes de protection de la vie privée associés aux systèmes biométriques, à condition que la carte à puce et le système biométrique soient protégés de façon appropriée, par exemple en limitant l'accès au moyen d'un lecteur autorisé et d'un code d'identification personnelle* ».

• *Conseil de l'Europe*

Le Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD) a publié un rapport[126] en 2005 sur l'application de la Convention 108 aux données biométriques.

Pour le Conseil, le responsable du traitement doit faire un choix raisonné entre les fonctions d'identification et de vérification en fonction de la finalité du système, et au regard des avantages et inconvénient de ce choix au regard de la vie privée. Si une solution de vérification suffit, le recours à l'identification doit être évité. Ainsi, « *les données biométriques qui sont uniquement utilisées à des fins de vérification devraient être stockées de préférence sur un support individuel sécurisé de stockage, par exemple une carte à puce, que détiendrait uniquement la personne concernée.* »

• *Groupe de l'article 29*

---

[125] Organisation de Coopération et de Développement Economiques, Direction de la science, de la technologie et de l'industrie, Comite de la politique de l'information, de l'informatique, et des communications, Groupe de travail sur la sécurité de l'information et la vie privée, *Technologies Fondées Sur La Biométrie*, 10 juin 2005
http://perso.orange.fr/perso.web/hebergement/biometrie/doc/OCDE_JUIN2005.pdf

[126] Conseil de l'Europe, Rapport d'étape sur l'application des principes de la Convention 108 au traitement des données biométriques, 2005.
http://perso.orange.fr/perso.web/hebergement/biometrie/doc/CONSEIL_CONV_108_BIOMETRIE.pdf

Le groupe de travail porte le nom de l'article 29 de la directive 95/46/CE qui l'a institué. Il s'agit de l'organe consultatif indépendant de l'Union Européenne sur la protection des données et de la vie privée. Le groupe a publié 1er août 2003 un document de travail sur la biométrie[127] et plusieurs avis sur les différents traitements européens abordés précédemment (visas[128], VIS[129], SIS[130], passeports biométriques[131]). L'étude de ces différents documents révèle une approche parfaitement cohérente avec ce qui a été décrit précédemment.

« *Le groupe de travail est d'avis que l'utilisation de systèmes biométriques se référant à des caractéristiques physiques qui ne laissent pas de traces ou de systèmes biométriques se référant à des caractéristiques physiques qui laissent des traces, mais dont les données ne sont pas mises en dans une base de données centrale, crée moins de risques pour la protection des libertés et des droits fondamentaux de la personne* ».

« *Toutefois, si ce type de système est mis en oeuvre, par exemple dans le cas d'installations de haute sécurité, il peut être considéré comme un traitement de données qui présente des risques au sens de l'article 20 de la directive 95/46/CE, et donc être soumis au contrôle préalable des autorités chargées de la protection des données conformément à la législation nationale* »

SOUS-SECTION 2. Tentatives de consolidation

§ 1. Guides et codes de bonne conduite

• *Irlande : un guide sur l'introduction de la biométrie dans l'éducation*[132]

Très pragmatique, ce guide est proche de l'esprit qui émane des autorisations uniques de la CNIL mais ses effets juridiques sont moindres.

Ainsi, ayant rappelé les règles de protection des données qui ont vocation à s'appliquer dans ce type de traitement, l'autorité pose un certain nombre de principes comme la nécessité de recueillir le consentement préalable des élèves mais aussi des parents pour les mineurs, ou celle de garantir la possibilité de se désister.

Étude d'impact préalable. - Approche assez originale, l'autorité demande aux établissements de mener une « étude préalable d'impact sur la vie privée » avant toute mise en œuvre d'un système, rappelant les sanctions pénales qu'ils encourent en cas de traitements non conformes aux règles générales relatives à la protection des données à caractère personnel.

Ainsi, cette étude doit permettre aux responsables de répondre à une liste très complète de questions pratiques. Cette approche montre que des questions extrêmement pratiques peuvent être appréhendées différemment selon que l'on prend ou non en compte la nécessaire protection des

---

127 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_fr.pdf

128 Avis n° 3/2007 sur la proposition de règlement modifiant les instructions consulaires en liaison avec l'introduction d'éléments d'identification biométriques et les dispositions relatives aux demandes de visa, 1er mars 2007. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp134_fr.pdf

129 Avis n° 7/2004 sur l'insertion d'éléments biométriques dans les visas en tenant compte de la création du système VIS, 11 août 2004. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_fr.pdf

130 Avis n° 6/2005 sur les propositions de règlement sur l'établissement, le fonctionnement et l'utilisation du SIS II, 25 novembre 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp116_fr.pdf

131 Avis n° 3/2005 sur l'application du règlement (CE) n° 2252/2004 du 13 décembre 2004 établissant des normes pour les éléments biométriques intégrés dans les passeports délivrés par les États membres, 30 septembre 2005. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_fr.pdf

132 http://www.dataprotection.ie/docs/Biometrics_in_Schools,_Colleges_and_other_Educational_Instit/409.htm

données personnelles. Voici une proposition de traduction des questions auxquelles les responsables de traitement sont invités à répondre au cours de leur étude. Les responsables doivent s'interroger :

• sur la finalité, relative au contrôle d'accès ou au contrôle des présences ; sur la légitimité du recours au dispositif biométrique (sur la nécessité d'instaurer un haut niveau de sécurité au vu de la nature de l'établissement, de la présence ou non de zones sensibles ; sur la nécessité que ces zones soient plus sécurisées que des zones publiques ;

• sur la légitimité de l'objectif ; sur la possibilité de réaliser cet objectif par des moyens moins intrusifs ; sur l'utilisation complémentaire ou alternative d'un mot de passe ou d'un autre identifiant ;

• sur la présence ou non d'un système de contrôle existant ; sur les raisons éventuelles de l'échec de son dispositif, justifiant son remplacement ; sur les méthodes choisies pour évaluer ces dispositifs ; sur la capacité d'un système biométrique à résoudre ces difficultés ; sur les améliorations qu'on attend grâce à l'usage du système biométrique ;

• sur les modalités techniques envisagées ; sur la technologie biométrique adéquate ; sur la procédure envisagée, identification ou vérification ; sur la nécessité de constituer une base centralisée ; sur les raisons pour lesquelles un système décentralisé ne suffirait pas ;

• sur la sécurité de locaux et la protection des écrans d'ordinateur et des documents imprimés ; sur la désignation d'un responsable de la sécurité et d'audits au regard de la vie privée ; sur l'existence d'une serveur de secours ;

• sur le degré d'exactitude des données nécessaire et les procédures éventuelles mises à jour ; sur les modalités de sécurisation des données ;

• sur les modalité procédurales ; sur la légitimité des habilitations et de la procédure d'accès aux données ; sur la base légale qui permet de demander aux élèves de participer ; sur la méthode pour recueillir le consentement des élèves ; sur la procédure de sortie du système et d'information des élèves sur la possibilité de se désister ; sur les procédures alternatives pour les élèves non éligibles à l'identification ; sur la gestion des incidents)

• sur la mise en place d'un politique de protection des données ; sur la politique de conservation des données envisagée ;

• sur leur appréciation personnelle du recours à la biométrie dans un établissement scolaire en tant qu'ancien étudiant ; sur l'impact de la banalisation à l'école des technologies présentant des risques pour la vie privée ; sur l'existence d'une politique générale de protection des données au sein de l'établissement ; sur la formation du personnel.

• Code Australien de l'Institut de Biométrie

Le groupe de travail de l'article 29 dans son document de travail sur la biométrie avait insisté sur l'importance des codes de conduite qui devraient contribuer à la bonne application des principes de la protection des données. Des codes communautaires peuvent lui être pour déterminer leur conformité à la directive CE/95/46. Évidemment, l'Australie n'est pas directement concernée par ces recommandations, mais l'initiative prise s'inscrit dans cet ordre d'idée.

Un code homologué et contraignant pour ses adhérents. - L'Institut de Biométrie est une organisation indépendante à but non lucratif fondée en 2001 dont le but est d'encourager un usage

responsable de la biométrie au regard de la vie privée. Il est à l'origine de la rédaction d'un Code[133] homologué le 19 juillet 2006 par la présidente de l'autorité australienne de protection de la vie privée Karen CURTIS, en application de l'article 18BB(2) de la loi australienne sur la vie privée de 1988. Ce code est contraignant dès lors qu'une entité privée ou publique déclare y adhérer en signant un engagement de conformité.

Terminologie. - Le code commence par définir les termes techniques et juridiques habituellement employés dans le domaine de l'identification biométrique. Il rappelle ensuite les principes généraux de protection de la vie privée et des données personnelles au regard des traitements informatiques - principe de finalité, de proportionnalité, droits des personnes concernées - détaillant les diverses dérogations relatives à l'usage de données personnelles, ou à l'utilisation des données pour de nouvelles finalités.

Grands principes et préconisations techniques. - Une deuxième partie est consacrée plus particulièrement aux données biométriques, avec un certain nombre de recommandations, qui recoupent plus ou moins des lignes directrices du droit européen.

Le recours au chiffrement des données de leur collecte à leur archivage est préconisé, ainsi que la destruction des données brutes à l'enrôlement et à l'appariement. Le Code incite également à l'anonymisation des bases de données biométriques, à la séparation des données biométriques d'autres données telles que l'état civil, et à la conservation des données de manière à ce que leur rapprochement avec d'autres données ne soit pas possible.

Les signataires sont invités à définir une politique d'accès aux données biométriques, et donc une matrice d'habilitation justifiée par les fonctions et responsabilités des personnes au sein de l'entreprise, à tenir un journal des accès aux données biométriques.

Le texte pose encore le principe d'enrôlement volontaire sauf obligation légale, de consentement et d'information exprès en cas d'utilisation des données pour une nouvelle finalité.

Le code encourage les signataires à faire pratiquer des audits juridiques et techniques externes, analysant la conformité du dispositif aux règles du Code, notamment les politiques et procédures d'accès, d'enrôlement, de stockage, la formation et la sensibilisation du personnel, la sécurité des systèmes d'information, les procédures de recours et d'information. Enfin, les standards nationaux et internationaux relatifs à la sécurité des systèmes d'information et aux techniques biométriques sont énumérés, les signataires étant inviter à « les prendre en compte » lors de la mise en œuvre du dispositif.

§ 2. Exemples de consolidations législatives

• *Québec : consécration de grands principes au regard de la biométrie*

Le droit québécois est l'un des rares à avoir intégré des dispositions spécifiques à l'usage de la biométrie. C'est très tôt en 2001 que la province francophone, comprenant les enjeux liés à la biométrie, a entrepris de rappeler certains principes essentiels, auxquels l'usage de procédés biométriques ne doit pas porter atteinte, parallèlement à la seule protection des données et de la vie privée.

Légalité de l'identification biométrique. - Ainsi, la loi concernant le cadre juridique des

[133] http://www.biometricsinstitute.org/associations/4258/files/2006-07%20Biometrics%20Institute%20Privacy%20Code%20approval%20determination%20FINAL.doc

technologies de l'information consacre son chapitre III à l'*« établissement d'un lien avec un document technologique* » contenant des dispositions spécifiques à la biométrie et des dispositions générales relatives à l'identification des personnes.

Elle dispose que la vérification de l'identité ou de l'identification doit se faire dans le respect de la loi et peut être effectuée à partir de caractéristiques, connaissances ou objets qu'elle présente ou possède quel que soit le support au moyen duquel elle communique.

Principe du consentement préalable. - La loi pose en son article 44, le principe du consentement préalable, non pas seulement limité à la collecte, mais durant tout le processus d'identification . Elle précise ainsi 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.* ».

Principe de déclaration préalable. - Le principe d'une déclaration préalable auprès de la Commission d'accès à l'information est également posé lors de la création d'une « *banque de caractéristiques ou de mesures biométriques* ».

Responsabilisation des utilisateurs. - D'autres dispositions prescrivent des obligations à la charge des utilisateurs par exemple pour l'intégrité des documents, et surtout des protections contre :

• les atteintes à la liberté de circulation (article 43 alinéa 2 : « *nul ne peut exiger qu'une personne soit liée à un dispositif qui permet de savoir où elle se trouve* ») ;

• les atteintes à l'intégrité physique (article 43 alinéa 1 : « *nul ne peut exiger que l'identité d'une personne soit établie au moyen d'un procédé ou d'un dispositif qui porte atteinte à son intégrité physique* » ;

• les détournements d'utilisation (article 44 : « *tout autre renseignement concernant cette personne et qui pourrait être découvert à partir des caractéristiques saisies ne peut servir à fonder une décision à son égard ni être utilisé à quelque autre fin que ce soit* ») ;

La loi précise que les caractéristiques des personnes « *ainsi que toute note les concernant* » doivent être détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus.

- ***Loi portant réforme de l'aide sociale - Ontario (CANADA) : une loi modèle ?***

Dans la province canadienne de l'Ontario, de nouvelles mesures d'identification ont été prise dès 1997 pour lutter contre la fraude aux prestations sociales. La fraude reposait en grande partie sur des identités multiples déclarées par les bénéficiaires pour obtenir plusieurs fois la même prestation.

L'IPC[134] a alors travaillé avec le ministre des services sociaux pour définir un cadre juridique prévoyant les garde-fous techniques et procéduraux nécessaires. L'IPC avait explicitement recommandé que ces garde-fous soit consacrés par la loi, une manière de leur donner une force et

[134] Information Privacy Commissioner http://www.ipc.on.ca/

une légitimité incontestable.

• les données biométriques doivent être chiffrées (cryptées) dès leur conservation jusqu'à leur transmission ;

• le traitement doit être limité à la vérification de l'éligibilité de la personne à bénéficier des prestations et non à la surveillance ;

• l'empreinte digitale ne doit pas pouvoir être reconstruite à partir du gabarit stocké dans la base de donnée. Ainsi, une empreinte digitale relevée sur les lieux d'un crime ne doit pas être interopérable avec un gabarit stocké dans la base centralisée ;

• l'administrateur ou le directeur ne doivent pas mettre en oeuvre un traitement permettant de reconstruire la donnée brute à partir du gabarit ou permettant de la comparer à une donnée qui n'aurait pas été obtenue directement auprès de la personne concernée ;

• le gabarit chiffré ne doit pas servir d'identifiant unique facilitant les interconnexions avec d'autres bases de données ;

• la données brute (la numérisation de l'empreinte digitale) doit être détruite après la création et le chiffrement du gabarit ;

• des contrôles stricts d'accès aux données biométriques doivent être prévus ;

• l'accès par des tiers, comme des agences du gouvernement ou la police, n'est possible que sur ordre d'un magistrat ;

• toute autre donnée (notamment l'historique des paiements) doit être stockée séparément des identifiants comme le nom ou la date de naissance.

Au final, le gouvernement de l'Ontario a adopté une loi réformant le système aide sociale (consultable en annexe), qui reprend la grande majorité de ces recommandations, notamment la mesure-phare sur le chiffrement des données. Pour l'IPC, la loi offre des garanties sans précédent au regard de la biométrie, de sorte qu'elle pourrait servir de modèle aux administrations qui envisagent d'avoir recours à la biométrie pour lutter contre la fraude.

Par ailleurs, la loi définit explicitement la donnée biométrique : il s'agit de toute information issue des caractéristiques uniques d'un individu, à l'exclusion de la photographie ou de l'image de la signature[135].

L'uniformisation des données biométrique n'est donc pas impossible. Notamment en raison des flux transfrontières de données, de la multiplication des traitements transnationaux, le mouvement d'uniformisation du droit des données biométrique est en train de devenir une réalité, indirectement grâce au projet de directive-cadre relative à la protection des données au sein du troisième pilier. En dehors de ce cas particulier, il existe en Europe une harmonisation de fait, issue de l'alignement des autorités de protection des données sur la doctrine dominante, relayée par les autorités supranationales.

En définitive, se pose la question d'une possible consolidation législative de ce droit en France, qui reste selon l'expression consacrée plus ou moins à tort, d'origine « doctrinale » ». Certes, cette doctrine a aujourd'hui une véritable valeur contraignante. Mais les règles qui en découlent résultent encore largement de l'interprétation des décisions de la CNIL.

Le principe d'accessibilité et d'intelligibilité du droit voudrait que certaines d'entre elles soit légitimées par la loi, ne serait-ce que pour donner à la biométrie un statut à la hauteur des enjeux de société qu'elle soulève du fait de sa généralisation prochaine. C'est aussi dans cet esprit qu'on été

135 « *means information derived from an individual unique charactéristic but does not include a photographic or signature image* »

adoptés les textes relatifs à l'eugénisme et au clonage reproductif.

Il est trop tard aujourd'hui pour appliquer un principe de précaution à l'égard de la biométrie, mais il est encore temps que la loi s'y intéresse plus en détail, le travail ayant été en grande partie mâché par les autorités de protection des données. Il s'agirait aussi d'une manière de compenser le recours massif, en cours et à prévoir, parfois opaque, par les gouvernements à cette technologie, en garantissant aux citoyens le respect de règles qui ont déjà pu être dégagées à l'étranger et qui ont vocation à terme, à dépasser les frontières.

SECTION 2. La « signature biométrique », une technologie au renfort de la vie privée ?

SOUS-SECTION 1. Un protocole d'identification associant biométrie et cryptographie

§ 1. Principes techniques

• *Propos préliminaires*

Le sujet du chiffrement des données biométrique a déjà été abordé et cette section n'a pas pour objet d'y revenir. La cryptographie traditionnelle consiste pour l'administrateur d'un système à chiffrer en interne toute forme de données, dans le cadre d'une politique de sécurité des systèmes d'information et de ses obligations en tant que responsable de traitement de données à caractère personnel.

« **Privacy enhancing technologies** » **-** Il s'agit au contraire de présenter une technologie propre qui s'inscrit au carrefour de plusieurs domaines auparavant distincts, que l'on compte au rang de ce qu'on appelle « les technologies renforçant la vie privée » ou « privacy enhancing technology ». Pour ses défenseurs, il s'agit de renverser le schéma selon lequel toute technologie porte nécessairement atteinte à la vie privée. Elle consiste à faire fusionner au sein d'une même discipline la signature électronique et la biométrie.

La démonstration sera délicate, d'autant que la signature électronique elle-même ne fait pas l'unanimité. Mais il serait dommage, voire obscurantiste, de fermer *a priori* cette porte, car il s'agit d'un terrain d'investigation passionnant et qui renverse les conceptions traditionnelles. En évinçant d'emblée cette possibilité, les détracteurs de la biométrie risquent de se voir imposer une technologie déjà obsolète ou encore immature - avec tous les risques et inconvénients qu'elle suppose - et surtout, de passer à côté d'une biométrie qui précisément pourrait servir la cause qu'ils défendent.

Une signature biométrique. - De nombreuses dénominations sont utilisées pour désigner ces techniques. Le terme signature biométrique nous parait intéressante, sinon techniquement la plus pertinente, car elle permet au juriste du numérique de se situer dans un environnement connu.

Il n'existe pas à notre connaissance de travaux en France sur ce sujet. Cette étude aura donc pour seul fondement les travaux menés à l'étranger[136], notamment ceux d'Ann CAVOUKIAN[137], Commissaire à la protection des données de l'Ontario, Alex STOIANOV et Georges. J. TOMKO,

[136] Feng HAO, Ross ANDERSON, John DAUGMAN, *Combining cryptography with biometrics effectively*, Technical Report Number 640, Computer Laboratory, University of Cambridge, juillet 2005 http://www.cl.cam.ac.uk/~jgd1000/biocrypto.pdf

[137] Ann CAVOUKIAN et Alex STOIANOV, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*, Information and Privacy Commissioner/Ontario March 2007. http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

spécialistes des technologies de cryptographie biométrique, ainsi que les enseignements généraux sur la signature électronique dispensés par M. Philippe WOLF et Maître Thierry PIETTE-COUDOL, éminents spécialistes, dans le cadre du Master Droit de l'Internet Public.

• Bref rappel des principes de cryptographie

On se gardera de donner une portée scientifique aux considérations qui suivent. Il s'agit d'une tentative de vulgarisation menée du point de vue du juriste, mais qui est un préalable indispensable à la compréhension de l'intérêt que revêt la signature biométrique au regard de la vie privée.

Chiffrement. - Les systèmes de cryptographie reposent sur plusieurs principes assez simples, que l'on fait dialoguer de manière un peu plus complexe. Lorsque l'on cherche à rendre confidentiel un message, un texte, on peut utiliser une convention de cryptage, dont les plus anciennes remontent à l'apparition même de l'écriture. On peut par exemple remplacer toutes les lettres d'un message par leur numéro d'apparition dans l'alphabet (de 1 à 27). Droit s'écrira alors « 4-18-15-9-20 ». Cette méthode est évidemment trop facile à deviner et à renverser, c'est pourquoi on « chiffre » différemment à partir d'une fonction mathématique. Si le premier numéro à chiffrer est y, que son résultat chiffré est x , on lui appliquera la fonction « $x = y^2 + 12$ ». Dans l'exemple du mot précité le résultat chiffré de 4 sera 28. Ce genre d'équation à une inconnue est évidemment encore trop simple à deviner.

Fonctions mathématiques irréversibles. - C'est pourquoi on passe par une fonction mathématique irréversible (dite « asymétrique »), d'une complexité telle qu'on ne peut calculer, y compris avec la puissance cumulée de plusieurs milliers d'ordinateur travaillant automatiquement en ingénierie inversée, les éléments d'origine de l'équation à partir du résultat. Sans la convention de cryptage, sans indices sur l'équation mise en oeuvre pour le chiffrement, il est impossible de déchiffrer le message. Cela vient de la difficulté de « *factoriser les grands nombres entiers* ».

Un protocole d'identification. - Lors du chiffrement d'un message, un des élément de l'équation, un chiffre de 128 bits appelé clé A, sera généré de manière aléatoire, en même temps qu'une clé B différente mais complémentaire. Ces deux clés jumelles sont alors nécessaires pour résoudre l'équation et déchiffrer un message crypté. Le principe essentiel est qu'un message chiffré avec la clé A ne peut être déchiffré qu'avec sa fausse jumelle, la clé B. Au final, la présomption est la suivante : si j'ai pu déchiffrer un message avec la clé B, c'est que le message a été chiffré avec la clé A. Si on considère que la clé A est une clé privée, secrètement gardée par son détenteur, alors le message ne peut provenir que de ce dernier. Nous avons donc là à la fois techniquement et conventionnellement, un protocole d'identification et de vérification. Un document peut ainsi être signé électroniquement, la signature électronique étant vérifiée par le destinataire à partir de la clé publique.

• Intégration de la biométrie aux principes cryptographiques

Faiblesses de la signature électronique. - Il existe cependant plusieurs failles. En effet, les clés sont toujours générées à partir d'un mot de passe. Ce mot de passe peut être révélé, subtilisé, perdu, divulgué et permettre de régénérer la paire de clés. Celles-ci peuvent être stockées sur support externe, ce support pouvant lui-même être volé, reproduit à partir de l'original. Enfin, rien ne garantit jamais que la personne qui signe électroniquement un document devant son écran d'ordinateur, est bien la personne à qui est associée la signature. N'importe qu'elle personne ayant accès au poste de travail peut, en soi, utiliser la signature électronique d'une autre.

Intervention des principes de la biométrie. - On peut d'ores et déjà voir en quoi la biométrie est susceptible d'apporter une réponse. On pourrait déjà imaginer de sécuriser le poste de

travail, ou encore le support externe, par une identification biométrique. Plus subtilement, on peut faire en sorte de créer un lien entre une clé de 128 bits et une information biométrique, de telle manière que ni la donnée biométrique, ni la clé ne puisse être retrouvée. Ce lien consiste en un fichier qui permettra l'identification.

Création de la signature biométrique. - Dans un premier temps, on fixera une identité, comme à l'enrôlement. La procédure consiste d'abord à générer aléatoirement un mot de passe, de manière à ce que ni l'utilisateur, ni l'administrateur ne la connaisse. Le mot de passe est complètement indépendant de la donnée biométrique, et donc peut toujours être changé ou mis à jour. Le système créé alors automatiquement une clé publique et une clé privée. Dans un deuxième temps, on prélève un échantillon biométrique, par exemple à partir de l'empreinte digitale, convertie en gabarit. Puis l'algorithme de chiffrement va lier le mot de passe à la donnée biométrique pour créer un fichier protégé, à partir duquel il est impossible de retrouver ni la donnée biométrique ni le mot de passe. Sommairement résumé, le mot de passe est chiffré avec la donnée biométrique et inversement. À l'issue de l'enrôlement, le mot de passe, la donnée biométrique, et la clé privée sont effacés. Seul reste le fichier protégé et la clé publique. Le mot de passe n'est recréé que lorsque la donnée biométrique est présentée lors de la phase d'appariement. Le mot de passe permettra de régénérer la clé privée.

Vérification de l'identité. - A la vérification, l'utilisateur présente son doigt. Le programme de reconnaissance va alors comparer la donnée biométrique présentée avec le fichier protégé. Si les données correspondent, le programme va autoriser l'algorithme à récupérer le mot de passe, qui lui-même permettra de régénérer une clé privée. En d'autres termes, la donnée biométrique de l'utilisateur sert de clé de déchiffrement. À l'issue de la vérification, la donnée brute est effacée. La clé privée ainsi régénérée sera alors susceptible d'être reconnue par sa jumelle, la clé publique, protocole qui peut alors servir de base à toute application physique ou logique nécessitant une identification.

§2. Étude de cas

• Contrôle d'accès et vérification

Enrôlement. - La procédure d'enrôlement a lieu sous la surveillance d'une autorité de certification, à l'image des prestataires de services de certification électronique. Un mot de passe est créé aléatoirement et utilisé pour produire une paire de clés (une clé publique et une clef privée). Le programme de signature biométrique de l'autorité va alors créer un fichier confidentiel de référence, chiffré irréversiblement à partir d'une empreinte digitale et du mot de passe, après quoi ces données sont détruites, ainsi que la clé privée. Ni l'empreinte digitale, ni le mot de passe ne peuvent être retrouvés à partir du fichier de référence. Seul reste donc le fichier de référence chiffré et la clé publique. Si Alice satisfait aux conditions posées par l'autorité de certification, l'autorité certifie le lien créé entre Alice et la clé publique (il signe numériquement la paire). Alice peut alors publier sa clé privée, l'envoyer à des tiers qui auront besoin de l'identifier.

Appariement. Alice se présente pour la vérification de son identité. Elle présente un doigt sur le capteur d'une borne d'accès et une carte à puce contenant le fichier de référence. Le fichier de référence n'est déchiffré (et en fait déchiffrable) que si c'est la donnée biométrique qui est présentée et la même donnée biométrique qui a créé ce fichier. Ainsi, l'administrateur du système ne peut ni retrouver l'empreinte originelle, ni le mot de passe intégrés au fichier de référence. Si le fichier reconnaît l'empreinte qui l'a créé, Alice récupère son mot de passe et régénère ainsi sa clé privée automatiquement. Alice signe alors, avec sa clé privée, une demande d'accès. Cet accès ne sera alors autorisé que si cette signature par clé privée est reconnue par sa fausse jumelle, la clé publique certifiée, enregistrée dans la borne biométrique. Si elles se « reconnaissent », l'accès est autorisé.

Le système a ainsi pu vérifier le lien entre le corps d'Alice et la clé publique certifiée, garanti par le fait que la clé privée ne pouvait être obtenue que grâce à un mot de passe, et que ce mot de passe ne pouvait être obtenu que par identification biométrique.

• Identification et vérification : utilisation d'une base de donnée anonyme

On prendra l'exemple du contrôle aux frontières, qui requiert l'identification de la personne, la vérification au moyen du titre d'identité et éventuellement, le filtrage au travers d'une liste noire.

Comparaison en trois étapes. - Les recommandations de l'OACI comprennent une vérification d'identité en trois étapes : comparaison des données biométrique de la personne qui se présente, des données présentes dans le passeport électronique, et des données présentes dans une base de données centralisée. La technologie de signature biométrique permet de procéder à cette comparaison sans que soient stockées directement les données biométriques de la personne.

Seuls sont enregistrés dans la base de donnée et dans le passeport biométrique le fichier de référence, contenant le mot de passe chiffré avec une donnée biométrique, l'un et l'autre étant impossible à déchiffrer sans l'intervention de la personne concernée.

En pratique, une personne se présente pour l'identification devant une borne. Elle pose son doigt sur une borne biométrique, qui envoie alors une requête auprès de la base de donnée. Le fichier référence correspondant est alors transmis de la base de donnée à la borne, qui le garde temporairement en mémoire. La donnée biométrique de la personne est alors combinée au fichier pour récupérer le mot de passe et régénérer ainsi la clé cryptographique, ou plutôt une version hachée de la clé cryptographique. Une seconde clé cryptographique est extraite selon la même procédure à partir du passeport.

Les deux clés sont alors comparées, l'une extraite de la base centralisée, l'autre extraite du passeport, toutes deux ayant été créées pour ne pouvoir être régénérées que par la personne légitime, grâce aux données de son corps. Lorsqu'elles correspondent, la vérification est positive, la personne est identifiée, ou plus exactement son identité est vérifiée.

Inversement, si l'algorithme ne parvient pas à extraire le mot de passe, et donc à régénérer la clé, à partir des données présentées par la personne et du fichier référence, la vérification échoue. Le fichier référence est impossible à décrypter, il ne « reconnaît » pas la personne qui se présente.

SOUS-SECTION 2. Résolution de l'antinomie « *sécurité contre vie privée* »

§1. Évaluation technique

• Maintien des avantages de la biométrie

L'apparente complexité technique de ce protocole masque sa simplicité d'utilisation. Le candidat à l'identification n'a besoin de rien d'autre que de ses empreintes digitales pour accéder aux applications protégées. Le candidat à l'identification n'a pas à se souvenir d'un mot de passe, ni à le conserver où que ce soit, ni même à en avoir jamais eu connaissance. Le fait de sécuriser la régénérescence du mot de passe par la biométrie, permet d'écarter toutes les vulnérabilités auxquelles il est ordinairement soumis : le vol, l'oubli, la divulgation.

Ces vulnérabilités sont d'autant moins susceptibles d'affecter l'identification que personne, ni le candidat, ni l'administrateur n'ont d'accès visible au mot de passe en question. Ce dernier est

automatiquement récupéré lorsque le fichier de référence est déchiffré grâce au corps auquel il a été lié à sa création. Seul le logiciel l'utilise ponctuellement et temporairement pour appliquer des algorithmes de déchiffrement.

Il est par ailleurs possible de créer avec l'autorité de certification autant de certificats qu'on le souhaite pour diverses applications : compte bancaire, compte fiscal, accès au réseau d'entreprise, commerce électronique, accès physiques. On peut donc avoir en sa possession autant de certificats que nécessaire, sans avoir à posséder de support externe. Chaque système possédera le fichier référence permettant de régénérer une clé privée à partir des données biométrique et une clé publique qui lui correspond, sans que les fichiers stockés puissent être utilisés d'aucune autre manière et que personne d'autre ne puisse y accéder. En ce sens, on conserve les avantages de la biométrie en terme de sécurité.

• Contournement des inconvénients de la biométrie

Comme il a déjà été démontré, lorsqu'une donnée biométrique est divulguée, les risques d'usurpation d'identité sont tels que l'identité légitime doit être définitivement révoquée. On ne peut prendre le risque de conserver en mémoire et de maintenir les habilitations associées à une identité biométrique compromise, éventuellement usurpée par un tiers mal intentionné. De sorte que la personne légitime doit être rayée des cadres sans qu'il y ait d'alternative. Même dans le cas où les données auraient été chiffrées, il n'est pas impossible que le cybercriminel ait pu pirater le serveur abritant les clés ou même le support physique externe contenant la clé privée de l'administrateur sur laquelle repose toute la convention de cryptage.

Cette éventualité est largement écartée grâce à la signature biométrique. Sans l'intervention de la personne concernée, les gabarits ne peuvent être lisibles en clair. Le fichier référence lui-même peut être divulgué, publié même, il sera inexploitable pour toute autre personne que celle à laquelle il a été lié « par le corps ». Par mesure de sécurité, le certificat sera parfaitement révocable et réinitialisable auprès de l'autorité de certification.

De sorte que les risques d'usurpation d'identité à partir de gabarits biométriques sont quasiment inexistants. Il est même possible d'en déduire un principe de non interopérabilité des bases de données reposant sur des signatures biométriques différentes, crées pour la même personne, ce qui rend extrêmement hypothétique les risque de détournement.

De manière générale, il semblerait enfin qu'une très grande partie des risques techniques liés à la cybercriminalité et évoqués en première partie de ce mémoire, ne soient pas applicables à la signature biométrique. Les études en ce domaine manquent encore pour identifier de manière catégorique les abus qui peuvent ainsi être évités, mais il apparaît que l'architecture de la signature biométrique, fondée sur un fichier illisible en dehors de l'intéressé, soit une garantie particulièrement efficace.

§2. Appréciation juridique

• Au regard de la vie privée

Le corps, seul sésame de l'accès aux données biométrique. - En analysant les avantages en termes de sécurité, on s'aperçoit d'emblée des apports potentiels de la signature biométrique au regard de la vie privée. En faisant techniquement et corporellement de l'utilisateur la seule personne ayant accès logiquement à ses données biométriques, on prévient tout risque de détournement de finalité du traitement. D'une certaine manière, le corps redevient le seul sésame permettant de débloquer l'accès aux données biométriques. L'utilisateur redevient maître de la procédure et de ses

données. L'interconnexion devient de fait impossible, à moins de prévoir cette possibilité en amont et avec le consentement de la personne concernée, en optant par exemple pour un certificat commun entre deux applications.

Par ailleurs, les réticences qui se sont exprimées quant au recours aux bases de données biométrique ne sont donc plus justifiées, lorsque ces dernières ne sont constituées que par des fichiers de signature biométrique. Le caractère anonyme de la base de donnée est inhérent au concept lui-même, de même que la minimisation des informations collectées.

Il est encore possible, comme pour la signature électronique, de posséder autant d'identités que nécessaires, éventuellement rendues anonymes ou dissociées de l'état civil. Le prestataire de service de communication électronique doit en effet laisser à l'utilisateur la possibilité de n'associer qu'un pseudonyme au certificat.

La signature biométrique commence à être évoquée par les autorités de protection des données comme un outil intéressant, sans qu'elle ait encore fait l'objet d'évaluations. Ainsi, le groupe de l'article 29 aborde la question en quelques lignes dans son document de travail[138] sur la biométrie, l'OCDE, le Conseil de l'Europe, la CNIL, et le rapport Cabale s'étant exprimés dans le même sens, et avec le même laconisme :

"*Il y a lieu de tenir compte de certaines technologies nouvelles. La possibilité d'utiliser des données biométriques comme clés de cryptage constitue une évolution intéressante. Une telle solution engendrerait a priori moins de risques pour la personne concernée car le décodage ne pourrait se faire que sur la base d'une nouvelle collecte de données biométriques auprès de l'intéressé lui-même, ce qui éviterait la création de bases de données contenant des modèles de données biométriques susceptibles d'être réutilisés à des fins tout à fait différentes*."

On notera enfin qu'à notre connaissance, il existe d'ores et déjà un embryon d' application de la signature biométrique mise en oeuvre par le Cabinet LEXVIA, autorisé par la CNIL[139], et ayant pour finalité de sécuriser l'accès aux documents ainsi que leur envoi par courrier électronique. Ainsi, la CNIL relève que « *le gabarit de l'empreinte digitale enregistré au sein d'une carte servira à déverrouiller l'application d'envoi de messages et à générer une signature électronique. Ce service permettra d''adresser de façon confidentielle et sécurisée des courriers électroniques signés électroniquement à destination de tout correspondant disposant d'une adresse de courrier électronique et d'un dispositif de reconnaissance biométrique* ». Si les termes employés et le manque de détail ne nous permettent pas de savoir si ce traitement est exactement assimilable à la signature biométrique, il semble néanmoins que les modalités du traitement reflètent une approche très comparable.

À terme, la signature biométrique pourrait même devenir un outil de protection de la vie privée à part entière, pour toute forme de transaction et de communication électronique et toute forme de traitement de données à caractère personnel. Nul doute que des études plus poussées permettraient encore d'évaluer son potentiel.

• Au regard du régime juridique applicable

Les définitions de la directive 1999/93/CE du Parlement Européen et du Conseil du 13 décembre 1999 sur un « *cadre communautaire pour les signatures électroniques* » sont-elles

[138] Groupe de travail sur la protection des données (Article 29), Document de travail sur la biométrie, adopté le 1er août 2003, http://perso.orange.fr/perso.web/hebergement/biometrie/doc/ARTICLE29_2003_DOC.pdf
[139] Délibération n° 2005-249 du 03 novembre 2005.

suffisamment larges pour inclure la signature biométrique ?

Une définition ouverte. - Aux termes de la directive, la signature électronique est une méthode d'authentification qui repose sur la jonction ou la liaison logique de données électroniques avec d'autres données électroniques. Ces données sont définies comme « *des données uniques, telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique.* »

Plusieurs éléments appellent à commentaire. En premier lieu, il est indubitable que les données biométriques sont uniques. Elles le sont dès l'origine, au plan physique, et elles le sont par conséquent lors de leur conversion sous forme numérique. Par ailleurs, l'utilisation du terme « *telles que* » signifie que les rédacteurs du texte n'ont pas entendu limiter ce type de données aux codes et aux clés cryptographiques, et que d'autres données uniques sont susceptibles d'être utilisées. En l'espèce, la signature biométrique requiert codes (ou mot de passe), clé publique et privée, et donnée biométrique. D'autres données sont en cause, comme le fichier « référence » chiffré qui contient le gabarit et le mot de passe servant à reconnaître la personne et à recréer la clé privée.

La signature électronique avancée satisfait à des exigences particulières : « *être liée uniquement au signataire ; permettre d'identifier le signataire; être créée par des moyens que le signataire puisse garder sous son contrôle exclusif et être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable* ; » Il semble là encore que cette définition permette d'accueillir sans difficulté la signature biométrique. En effet, la signature biométrique est liée à la fois biologiquement, techniquement, et conventionnellement au signataire. Biologiquement puisqu'elle est créée à partir des données biométriques propres au corps de la personne, techniquement puisque le mot de passe ainsi récupéré permet de régénérer une clé privée strictement personnelle, conventionnellement puisque c'est une autorité tierce qui garantit ce lien.

Responsabilité des prestataires. - Au final, seuls sont susceptibles d'utiliser les données biométriques à mauvais escient les prestataires de certification. Or, on a vu qu'ils ne sont plus en possession des données brutes originales puisqu'elles sont détruites dès la fin de la procédure d'enrôlement et que seuls le corps originaire de ces données est susceptible d'ouvrir le fichier référence contenant le gabarit.

En tout état de cause, l'article 8 de la directive précise l'étendue de leur responsabilité en terme de protection des données, les prestataires devant *« satisfaire aux exigences prévues par la directive 95/46/CE* ». Ainsi, les États membres doivent veiller à ce qu'un prestataire de service de certification ne puisse recueillir des données personnelles que directement auprès de la personne concernée, ou avec le consentement explicite de celle-ci, et uniquement dans la mesure où cela est nécessaire à la délivrance et à la conservation du certificat, les données ne pouvant être recueillies ou traitées à d'autres fins sans le consentement explicite de la personne intéressée.

Rendre une conclusion définitive en matière de biométrie serait artificiel, à moins de paraphraser encore le principe de neutralité des technologies. Il est en revanche certain que le droit actuel n'est pas totalement prêt à limiter les effets potentiellement néfastes que recèle la biométrie en termes de libertés, alors qu'il a parfaitement assimilé les avantages qu'elle procure en termes de sécurité. Doit-on attendre des personnes qui détiennent le pouvoir d'imposer la biométrie, qu'elles restreignent leurs propres prérogatives ? La sempiternelle méthode du compromis est-elle satisfaisante ? Ces questions dépassent sensiblement le cadre de ce mémoire.

Cependant, cette première étude de la signature biométrique se veut être une réflexion prospective sur ce que « pourrait être » la biométrie : une résolution par le haut des antagonismes traditionnels. Ce chapitre n'ayant pas été placé par hasard à la fin de mémoire, libre à ses lecteurs d'en tirer les conclusions qui s'imposent.

- BIBLIOGRAPHIE –

Loi et Règlements

• Commission des Communautés Européennes, Proposition de décision-cadre du conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, Bruxelles, le 4.10.2005 COM(2005) 475 final 2005/0202 (CNS)
http://www.libertysecurity.org/IMG/pdf/COM_2005_475_final.pdf

• Conseil de l'Europe, *Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28 janvier 1981.
http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm

• Décret n°87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur, modifié par Décret n°2005-585 du 27 mai 2005
http://www.legifrance.gouv.fr/texteconsolide/PPHEP.htm

• 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
http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_fr.pdf

• Loi n°78-17 du 6 janvier 1978, *Loi relative à l'informatique, aux fichiers et aux libertés*, version consolidée au 24 janvier 2006, modifié par Loi n°2004-801 du 6 août 2004
http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm

• Règlement (CE) n° 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.
http://europa.eu.int/eur-lex/lex/LexUriServ/site/fr/oj/2004/l_385/l_38520041229fr00010006.pdf

Ouvrages généraux

• Rémy CABRILLAC, Marie Anne FRISON ROCHE, Thierry REVET (dir*), Libertés et Droits fondamentaux*, 10ème édition, Dalloz, 2004, Paris.

• Xavier CRETTIEZ, Pierre PIAZZA (dir), *Du papier à la biométrie*, identifier les individus, Presses de la fondation nationale des Sciences Politiques, Paris, 2006, 331 p.

• Catherine FERAL-SCHUHL, *Cyberdroit, le droit à l'épreuve de l'Internet*, 4ème édition Dalloz, 2006, Paris.

• Marie Laure LAFFAIRE, *Protection des données à caractère personnel*, Guide Pratique, Editions d'organisation, Paris, 2005.

• Jacqueline POUSSON-PETIT (dir.*), L'identité de la personne humaine. Étude de droit français et de droit comparé*, Bruxelles, Bruylant, 2002, 1001 p.

Rapports

• Christian CABAL, Office parlementaire d'évaluation des choix scientifiques et technologiques, *Méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, Rapport n° 938 déposé le 16 juin 2003 http://www.assemblee-nationale.fr/12/rap-off/i0938.asp et Compte rendu de l'audition publique du 4 mai 2006 sur la biométrie. http://www.assemblee-nationale.fr/12/pdf/rap-off/i3302.pdf

• Commission d'accès à l'information du Québec, *La biométrie au Québec : Les principes d'application pour un choix éclairé*, juillet 2002.
http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_appl.pdf

• Commission d'accès à l'information du Québec, *La biométrie au Québec : Les enjeux (document d'analyse)*, juillet 2002.
http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_enj.pdf

• CNIL, Document de travail sur la biométrie, 1er juin 2005 http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/LA_BIOMETRIEmai2005.pdf

• CNIL, 26 ème rapport d'activité 2006 « *La biométrie gagne du terrain* ».
http://perso.orange.fr/perso.web/hebergement/biometrie/doc/CNIL_27RAPPORTACTIVITE.pdf

• Conseil de l'Europe, Direction Générale des Affaires Juridiques, Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatise des données à caractère personnel, *Rapport d'étape sur l'application des principes de la convention 108 a la collecte et au traitement des données biométriques*, Strasbourg, février 2005.
http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/T-PD_2005_BIOM_F.pdf

• CLUSIF (Club de la sécurité des systèmes d'information français), Commission technique de sécurité physique, *Techniques de contrôle d'accès par biométrie*, juin 2003.
https://www.clusif.asso.fr/fr/production/ouvrages/pdf/ControlesAccesBiometrie.pdf

• Forum des Droit de l'Internet, *Projet de carte d'identité nationale électronique*, Rapport du 16 juin 2005. http://www.foruminternet.org/telechargement/documents/reco-cnie-20050616.pdf

• Jean-René LECERF, *Identité intelligente et respect des libertés*, Rapport d'information du Sénat n° 439 (2004-2005) déposé le 29 juin 2005), au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale (1) par la mission d'information (2) sur la nouvelle génération de documents d'identité et la fraude documentaire.
http://www.senat.fr/rap/r04-439/r04-4391.pdf

• Institute for Prospective Technological Studies (European Commission Joint Research Center), *Biometrics at the Frontiers : Assessing the impact on Society*, For the European Parliament Committee on Citizen Freedoms and Rights, Justice and Home affairs (LIBE), 2005
http://europa.eu.int/comm/justice_home/doc_centre/freetravel/doc/biometrics_eur21585_en.pdf

• Ligue des Droits et libertés, *La biométrie : des implications majeures pour nos droits et libertés* - Mémoire présenté à la Commission de l'éthique de la science et de la technologie du Québec -

Novembre 2005.
http://www.liguedesdroits.ca/documents/surveillance/biometrie/ldl_memoire_biometrie_nov05.pdf

• Organisation de Coopération et de Développement Economiques, Direction de la science, de la technologie et de l'industrie, Comite de la politique de l'information, de l'informatique, et des communications, Groupe de travail sur la sécurité de l'information et la vie privée, *Technologies Fondées Sur La Biométrie*, 10 juin 2005.
http://appli1.oecd.org/olis/2003doc.nsf/43bb6130e5e86e5fc12569fa005d004c/d15c6d3ea769bc64c1256e84004c42fc/$FILE/JT00186151.PDF

• United States Visitor and Immigrant Status Indicator Technology Program Office, *US-VISIT Program : Privacy Impact Assessment Update International Live Test*, 15 juin 2005.
http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_livetest.pdf

Avis et délibérations

• Groupe de travail sur la protection des données (Article 29), *Avis n° 7/2004 sur l'insertion d'éléments biométriques dans les visas et titres de séjour en tenant compte de la création du système d'information Visas (VIS)*, 11 août 2004.
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_fr.pdf

• Groupe de travail sur la protection des données (Article 29), *Avis 3/2005 sur l'application du règlement (CE) no 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*, 30 septembre 2005.
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp112_fr.pdf

• Groupe de travail sur la protection des données (Article 29), *Document de travail sur les données génétiques*, 17 mars 2004
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp91_fr.pdf

• Groupe de travail sur la protection des données (Article 29), *Document de travail sur la biométrie*, 1er août 2003, http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_fr.pdf

• Groupe de travail sur la protection des données (Article 29), *Avis n° 3/2007 sur la proposition de règlement du Parlement européen et du Conseil modifiant les instructions consulaires communes adressées aux représentations diplomatiques et consulaires de carrière, en liaison avec l'introduction d'éléments d'identification biométriques et de dispositions relatives à l'organisation de la réception et du traitement des demandes de visa*, 1er mars 2007.
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp134_fi.pdf

• Comité Consultatif National d'Ethique pour les Sciences de la Vie et de la Santé, *Biométrie, données identifiantes et droits de l'homme*, Avis n° 98 du 5 juillet 2007.
http://www.ccne-ethique.fr/francais/pdf/avis098.pdf

Colloques et Conférences

• Ayse CEYHAN, *Identité et identification au prisme de la biométrie*, Séminaire de philosophie du droit 2005-2006 « Sécurité, Sûreté, Surveillance », 8ème séance, Institut des Hautes Etudes sur la Justice, 20 mars 2006. http://www.ihej.org/ressources/ceyhan_20_03_06_2006.pdf

• Georges CHATILLON, *Simplification, efficacité, bon fonctionnement bon rendement de l'administration électronique, l'expérience française*, Kuwait Conference On Electronic Government 2003. http://www.georges-chatillon.eu/spip.php?article51

• Forum des politiques publiques, *La biométrie, incidences et applications pour la citoyenneté et l'immigration*, Actes d'un forum tenu par Citoyenneté et Immigration Canada, Ontario, les 7 et 8 octobre 2003. http://www.cic.gc.ca/francais/pdf/pub/biometrie.pdf

• Marie-Christine PIATTI (dir), *Les libertés individuelles à l'épreuve des NTIC*, Presse Universitaires de Lyon, Lyon 2001.

• Jean-Philippe WALTER, *Quelques aspects de protection des données lors de l'utilisation de données biométriques dans le secteur privé*, 26ème Conférence internationale des Commissaires à la protection des données et à la vie privée Wroclaw, 14-15-16 septembre 2004. http://26konferencja.giodo.gov.pl/data/resources/WalterJF+EN_paper.pdf

Doctrine

• Hal ABELSON and Lawrence LESSIG (dir*) Digital Identity in Cyberspace, White Paper Submitted for 6.805/Law of Cyberspace : Social Protocols*, 10 décembre 1998
http://www.eema.org/downloads/is_industry_papers/digital_id_in_cyberspace.pdf

• Julian ASHBOURN, *The Societal Implications of the Wide Scale Introduction of Biometrics and Identity Management*, Background paper for the Euroscience Open Forum ESOF 2006 in Munich, juillet 2006.
http://www.statewatch.org/news/2005/apr/jrc-biometrics-julian-ashbourn.pdf

• Eric BARBRY, Marie-Charlotte GRASSET, *La biométrie dans les entreprises est permise sous réserve de certaines précautions*, Gazette du Palais, 20 Octobre 2005 n° 293, page 14

• Eric BARBRY, Ségolène ROUILLE-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, page 7.

• Ann CAVOUKIAN et Alex STOIANOV, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*, Information and Privacy Commissioner/Ontario mars 2007. http://www.ipc.on.ca/images/Resources/up-1bio_encryp.pdf

• Sylvie CRAIPEAU, Gérad DUBEY, Xavier GUCHET, *La biométrie, usages et représentations*, février 2004, Rapport final projet incitatif Groupement des écoles de Télécommunication 2003.
http://www.foruminternet.org/telechargement/forum/biometrieint.pdf

• Paul DE HERT, *Biometrics: legal issues and implications, Background paper for the Institute of Prospective Technological Studies*, DG JRC – Sevilla, European Commission, janvier 2005.
http://cybersecurity.jrc.es/docs/LIBE%20Biometrics%20March%2005/LegalImplications_Paul_de_Hert.pdf

• Jacques DELGA, *Tous fiché, tous coupables, réflexion sur la présomption d'innocence de la théorie à la pratique*, Revue Communication Commerce Electronique, février 2007.

• Lucien FLAMENT, *La biométrie dans l'entreprise*, La semaine juridique n°24, 13 juin 2006, 1468

• Claudine GUERRIER, *Immigration et biométrie*, juriscom.net 11 septembre 2005.

http://www.juriscom.net/documents/biom20051109.pdf

• Claudine GUERRIER, *Les cartes d'identité et la biométrie : l'enjeu sécuritaire*, Communication Commerce Electronique n°5 Mai 2004 Etude 13.

• Feng HAO, Ross ANDERSON, John DAUGMAN, *Combining cryptography with biometrics effectively*, Technical Report Number 640, Computer Laboratory, University of Cambridge, juillet 2005. http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-640.pdf

• Pierre LECLERC, *À propos de la biométrie (quelques réflexion après visite de l'exposition Biométrie, le corps identité à la Cité des Sciences).* Communication commerce électronique n°3, Mars 2006, Etude 7.

• Nathalie MALLET-POUJOL, *Les libertés de l'individu face aux nouvelles technologies*, Les libertés publiques, Cahiers Français, La documentation française, mai-juin 2000, n°296.

• Nathalie MALLET-POUJOL, *Traçage électronique et Libertés : les empreintes biométriques*, Problèmes politiques et sociaux, La documentation française, n°925, juin 2006.

• Alice MILANOVA, *Preuve corporelle, vérité scientifique et personne humaine*, Revue de Droit prospectif, R.J.J., 2003-3, n°99

• Florence STIRLING-BELIN, *Traçabilité, liberté de circulation et Union Européenne*, Revue de droit prospectif R.J.J. , 2005-1, n°107

• Irma VAN DER PLOEG, *Biometric Identification technology : Ethical Implications of the Informatisation of the Body* (BITE policy Paper 1), mars 2005 http://www.iss.it/binary/publ/cont/STAMPA%20ANN_07_07%20VD%20Proeg.1180428381.pdf

• Philipe WOLF, *De l'authentification biométrique*, Sécurité informatique, n°46 et 48, CNRS, octobre 2003 et avril 2004.
http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num46.pdf

Divers

• *An Open Letter to the ICAO, A second report on « Towards an International Infrastructure for Surveillance of Movement »*, 30 mars 2004. http://www.statewatch.org/news/2004/mar/icaoletter.pdf

• *Biométrie contre état civil, l'identification du futur*, Droit de la famille, n°12 Décembre 2006, Alerte 86.

• *Combattre le terrorisme à l'aide de la biométrie*, IIJ@l'OEUVRE, été 2004, volume 3 numéro 1 Publication concernant le réseau canadien d'information pour la sécurité publique :

- ANNEXES -

TECHNOLOGIES BIOMÉTRIQUES – SYNTHÈSE

Technologie biométrique	Fiabilité	Facilité d'emploi	Acceptation par l'utilisateur	Stabilité	Coût	Transparence[1]	Applications courantes	Convient aux comparaisons	
								1 : 1	1 : N
Reconnaissance de l'empreinte digitale	Élevée ou très élevée	Élevée	Moyenne à faible	Élevée	* à ***	Visible	Autorisation des voyageurs, permis de conduire, aide sociale	oui	oui
Géométrie de la main	Élevée	Élevée	Moyenne à élevée	Moyenne à élevée	***	Visible	Contrôle d'accès, autorisation des voyageurs, soins de jour	oui	non
Reconnaissance faciale	Moyenne à élevée[2]	Moyenne à élevée	Élevée	Moyenne à faible	***	Dissimulé	Casinos, autorisation des voyageurs	oui	potentiellement[3]
Reconnaissance de l'iris	Très élevée	Moyenne à faible	Moyenne à élevée	Élevée	****	Dissimulé	Prisons, contrôle d'accès, autorisation des voyageurs	oui	oui
Reconnaissance de la rétine	Très élevée	Faible	Faible	Élevée	****	Visible	Contrôle d'accès, autorisation des voyageurs	oui	oui
Géométrie du doigt	Moyenne	Élevée	Moyenne à élevée	Moyenne à élevée	***	Visible	Contrôle d'accès, détenteurs de tickets d'entrée aux parcs d'attraction	oui	non
Reconnaissance vocale	Moyenne	Élevée	Élevée	Moyenne à faible	*	Dissimulé	Applications à basse sécurité, authentification par téléphone	oui	non
Vérification dynamique de la signature	Moyenne	Élevée	Moyenne à élevée	Moyenne à faible	**	Visible	Applications à basse sécurité, applications à signature existante	oui	non

Notes :

1. La transparence désigne la mesure dans laquelle un système peut être exploité à l'insu des personnes concernées. Les systèmes visibles ne peuvent prélever un échantillon biométrique à l'insu de la personne concernée, contrairement aux systèmes dissimulés.
2. La reconnaissance faciale pourrait théoriquement être fort exacte (comme le suggère l'essai récent de reconnaissance faciale mené dans des conditions contrôlées – *Facial Recognition Vendor Test*), mais des projets pilotes récents et des essais en conditions réelles ont fait apparaître des taux d'erreurs beaucoup plus élevés et montré qu'il était très difficile d'obtenir des résultats exacts avec ces systèmes.
3. Ibid.

Source : Author

Loi de l'Ontario 1997, chapitre 25

« Renseignements biométriques » (*Biometric information*) signifie information dérivée des caractéristiques uniques d'un individu ce qui n'inclut ni l'image photographique, ni l'image d'une signature.

Renseignements biométriques

75. (1) Si la présente loi ou les règlements autorisent quiconque à recueillir ou à utiliser des renseignements personnels, des renseignements biométriques ne peuvent être recueillis ou utilisés qu'aux fins suivantes :

1. Veiller à ce qu'un particulier ne soit inscrit qu'une seule fois à titre d'auteur de demande, de bénéficiaire, de conjoint, de partenaire de même sexe ou d'adulte à charge.

2. Authentifier l'identité d'un particulier qui prétend avoir droit à une aide.

3. Permettre à un particulier de recevoir une aide fournie par l'intermédiaire d'une institution financière ou d'un autre fournisseur autorisé et d'en accuser réception.

4. Permettre à un auteur de demande, à un bénéficiaire, à un conjoint, à un partenaire de même sexe ou à un adulte à charge d'obtenir l'accès à des renseignements personnels.

5. Permettre à un particulier de faire une déclaration par un moyen électronique, notamment vocal, à toute fin autorisée aux termes de la présente loi.

6. Comparer des données conformément à une entente conclue en vertu de l'article 71 ou 72 afin de vérifier l'admissibilité à une aide ou à des prestations. 1997, chap. 25, annexe A, par. 75 (1); 1999, chap. 6, par. 50 (7).

(2) Les renseignements biométriques peuvent être recueillis aux termes de la présente loi qu'auprès du particulier auquel ils se rapportent, que conformément à une entente visée à la disposition 6 du paragraphe (1) ou que conformément à l'article 73.

(3) Les renseignements biométriques ne doivent pas être divulgués à un tiers sauf si la divulgation est faite conformément :

a) soit à une ordonnance d'un tribunal ou à un mandat;

b) soit à une entente conclue en vertu de l'article 71 ou 72 afin de vérifier l'admissibilité à un régime de prestations sociales, y compris un régime de prestations sociales visé par la Loi de l'impôt sur le revenu ou la Loi de l'impôt sur le revenu (Canada);

c) soit à l'article 73.

(4) Les renseignements biométriques à recueillir auprès du particulier auquel ils se rapportent doivent être recueillis ouvertement et directement auprès de celui-ci.

(5) L'administrateur veille à ce que seules les personnes qui ont besoin de renseignements biométriques afin d'exercer leurs fonctions aux termes de la présente loi puissent y avoir accès et puissent les utiliser et que ceux-ci ne soient pas utilisés comme identificateur unique de dossiers ou identificateur commun de dossiers personnels, sauf selon ce qui est autorisé aux termes du paragraphe (1).

(6) L'administrateur veille à ce que les renseignements biométriques recueillis aux termes de la présente loi soient codés sans délai après leur collecte, que les renseignements biométriques originaux soient détruits après l'encodage et que les renseignements biométriques codés ne soient stockés ou transmis que sous une forme codée et qu'ils soient détruits de la façon prescrite.

(7) Ni le directeur ni l'administrateur ne doivent mettre en place un système qui permet de reconstituer
l'échantillon biométrique original à partir de renseignements biométriques codés ou de le conserver, ou qui en permet la comparaison avec une copie ou une reproduction de renseignements biométriques qui n'ont pas été obtenus directement du particulier.

(8) Les seuls renseignements personnels qui peuvent être conservés avec les renseignements biométriques concernant un particulier sont le nom, l'adresse, la date de naissance et le sexe du particulier.

(9) Pour l'application de l'article 67 de la Loi sur l'accès à l'information et la protection de la vie privée et de l'article 53 de la Loi sur l'accès à l'information municipale et la protection de la vie privée, le paragraphe (3) est une disposition ayant trait au caractère confidentiel qui l'emporte sur ces lois. 1997, chap. 25, annexe A, par. 75 (2) à (9).

Government Communications Security Bureau
Chris Roberts, Report on Biometrics, November 2005

Most early biometric acquisition and processing interfaces for the PC were based on proprietary technologies. By the mid-1990s some of these proprietary approaches started to merge into industry standards such as HA-API, BioAPI or AIS API. As these developed, further consolidation of these industry standards took place. Some key published standards currently include:

Common Biometric Exchange Formats Framework (CBEFF)

• ISO/IEC 19794-2:2005
Information technology - Biometric data interchange formats - Part 2: Finger minutiae data;
• ISO/IEC 19794-4:2005
Information technology - Biometric data interchange formats - Part 4: Finger image data;
• ISO/IEC 19794-5:2005
Information technology - Biometric data interchange formats - Part 5: Face image data
• ISO/IEC 19794-6:2005
Information technology - Biometric data interchange formats - Part 6: Iris image data;
• Federal Information Processing Standard (FIPS) 201 –
Personal Identity Verification of Federal Employees and Contractors;
• XML Common Biometric Format (XCBF);
• ANSX9.84 Biometric Information Management and Security;
• ANSI BioAPI Specification Version 1.1 (formerly ANSI INCITS 358-2002). Defines the Application Programming Interface and Service Provider Interface for a standard biometric technology interface.
• ITU X.509

Common Biometric Exchange Formats Framework (CBEFF)

CBEFF was first published in January 2001 as a NIST publication, NISTIR 6529 and provides a standard data structure/format for communicating biometric data. On April 5, 2004 -- NISTIR 6529-A was released. This specification is an augmented and revised version of the original CBEFF. It was developed by the CBEFF team based on the specification approved by the Biometrics Interoperability, Performance, and Assurance Working Group (NIST/BC WG) co-sponsored by NIST and the Biometric Consortium. This standard has been submitted to ISO and is in final committee draft discussion as ISO/IEC FCD 19784-1.269. Key features of this format include:

• Facilitating biometric data interchange between different system components or systems;
• Promoting interoperability of biometric-based application programs and systems;
• Providing forward compatibility for technology improvements; and
• Simplifying the software and hardware integration process.

There are three standard sections in the CBEFF format. Each section contains a number of fields that contain detailed information about the CBEFF file. Some of these fields are mandatory while others remain optional.

XML Common Biometric Format (XCBF)
Developed by OASIS and adopted as an OASIS standard in September 2003, this defines a common set of XML coding for formats specified in the CBEFF (NISTIR 6529). These XML encodings are based definitions in ANSI X9.84:2003 Biometrics Information Management and

Security and conform to the XML Encoding Rules (XER) defined in ITU-T Recommendation X.693. They also rely on the security and processing requirements specified in X9.96 XML Cryptographic Message Syntax (XCMS).

ANSX9.84 Biometric Information Management and Security for the Financial Services Industry

Published in 2001 and revised in 2003, this is a US national standard developed by ANSI's X9 Standards Committee on Banking. Developed specifically for the finance industry, it incorporates the XCBF standard. Its framework specifies common processing components and transmission paths within a biometrically enabled system that must be secured and specifies the minimum security requirements for effective management of biometric data including such aspects as:

- Security for the collection, distribution, and processing, of biometric data;
- Life-cycle management of biometric data;
- Usage of biometric technology;
- Application of biometric technology for internal, external logical and physical access control;
- Encapsulation of biometric data;
- Techniques for the secure transmission and storage of biometric data;
- Security of the physical hardware used throughout the biometric data life cycle; and
- Techniques for integrity and privacy protection of biometric data.

Biometrics Application Programming Interface (BAPI)

BAPI was developed by I/O Software in 1998 to be operating system and hardware independent, while maintaining a consistent user interface. Some of the features include unification of encryption, a standardised programming environment, and support for the client-server applications. In December 1998, I/O Software joined the BioAPI Consortium and the BAPI specification was integrated as the lower level of the BioAPI specification. In May 2002, Microsoft acquired BAPI technology with a view to integrating BAPI into Windows operating systems and applications.

BAPI is a multi-level API specification, designed to provide three levels of sophistication, control, and technology dependence. The three BAPI levels are:

- Level 3 working at an abstract level;
- Level 2 working with middleware; and
- Level 3 working at a device level.

Human Authentication API (HA-API)

HA-API was developed by NRI (National Registry Inc, later Saflink) in 1997 through a US Department of Defense contract and sponsored by NSA and the Biometric Consortium. It was a simple high-level API focusing on the easy use and integration of multiple biometrics and placed in the public domain. It merged with BioAPI in March 1999.

IBM's AIS API

IBM developed its own Advanced Identification Services Application Programming Interface (AIS API). However, IBM supports BioAPI and is a member of the BioAPI Consortium. AIS API is now subsumed into the BioAPI.

ANSI BioAPI 1.1

In March 1999 BAPI and HA-API were included in the BioAPI standard. BioAPI was then adopted as ANSI/INCITS 358 in February 2002. This specification does not define security requirements for biometric applications or service providers, although some related information is incorporated into the specification in order to support good security practices.

A new version of BioAPI is about to be approved as an International Standard and was expected to be published by ISO in the second half of 2005. This version (known as BioAPI 2.0, or ISO/IEC 19794-1) has several improvements over the ANSI standard version BioAPI 1.1, formerly ANSI/INCITS 358.

Common Data Security Architecture/Human Recognition Service (CDSA/HRS)
Dating from August 1998, CDSA was developed by The Open Group and provides a security services framework. The Human Recognition Services (CDSA/CSSM Authentication: Human Recognition Service (HRS) API V2) extension to CDSA provides enrolment, verification, and identification functions as well as server and database interfaces, using strong authentication methods. This API is based on the BioAPI Consortium's published standards.

Intel Human Recognition Services (HRS)
Formerly known as User Authentication Services (UAS) this is an extension to the Common Data Security Architecture (CDSA) framework which accommodates biometrics and smartcards. HRS supports user authentication within a security framework and can be used in conjunction with other security modules such as cryptography and digital certificates. It is based on BioAPI.

Speaker Verification API (SVAPI)
SVAPI was released in May 1996 and is one of the older biometric APIs. SVAPI was vendor independent and designed to provide interchangeable microphones in speaker verification systems. Later enhancements allowed data interchange with HA-API76.

X.509
X.509 is a widely used ITU recommendation (not a standard) for an authentication framework and defining attributes of Public Key Infrastructure (PKI) and digital certificates. The current version (Recommendation X.509-08/05) was approved in August 2005.

Other Standards
BAAPI, a commercial API developed by True Touch Technologies and C-API, the architectural basis for the BioAPI Consortium’s work are other historical biometric APIs.

There are also a number of other standards, largely US in origin, applying to specific aspects of biometrics. Again this is not an exhaustive list but includes:

• ANSI/NIST CSL 1a 1997, Data format for the exchange of fingerprint, facial and SMT information;
• ISO 10819-1:1994 Information Technology - Digital compression and coding of continuous tone still images;
• ANSI B10.8 Digital Imaging (driver’s license/identification card);
• ANSI/NIST-CSL 1-1993, Data Format for the Interchange of Fingerprint Information;
• CJIS/FBI IAFIS-IC-0110 - FBI WSQ standard for fingerprint image compression/decompression;
• CJIS-RS-0110 - FBI Appendix F & G, Fingerprint image quality specification;
• FIPS 190: Guideline for the Use of Advanced Authentication Technology Alternatives; and
• INCITS 377, 378, 379, 381, 385 approved data interchange formats.

1. A. Bodo. Method for producing a digital signature with aid of a biometric feature. German patent DE 42 43 908 A1. June 30, 1994 (Priority date: Dec. 23, 1992).

2. G.J. Tomko, C. Soutar, and G.J. Schmidt. Fingerprint controlled public key cryptographic system. U.S. Patent 5541994, July 30, 1996 (Priority date: Sept. 7, 1994).

3. G.J. Tomko, C. Soutar, and G.J. Schmidt. Biometric controlled key generation. U.S. Patent 5680460, Oct. 21, 1997 (Priority date: Sept. 7, 1994).

4. G.J. Tomko and A. Stoianov. Method and apparatus for securely handling a personal identification number or cryptographic key using biometric techniques. U.S. Patent 5712912, Jan. 27, 1998 (Priority date: July 28, 1995).

5. C. Soutar and G.J. Tomko. Secure private key generation using a fingerprint. In CardTech/ SecurTech Conference Proceedings, Vol. 1, pp. 245-252, May 1996.

6. G.J. Tomko. Method and apparatus for securely handling data in a database of biometrics and associated data. U.S. Patent 5790668, Aug. 4, 1998 (Priority date: Dec. 19, 1995).

7. C. Soutar, D. Roberge, A.V. Stoianov, R. Gilroy, and B. V. K. Vijaya Kumar, "Biometric Encryption using image processing," in Proc.SPIE, Optical Security and Counterfeit Deterrence Techniques II, vol. 3314, 1998, pp. 178–188.

8. C. Soutar, D. Roberge, A.V. Stoianov, R. Gilroy, and B. V. K. Vijaya Kumar. Biometric Encryption - Enrollment and Verification Procedures. Proc. SPIE, Optical Pattern Recognition IX, v. 3386, pp. 24 – 35 (1998).

9. C. Soutar, D. Roberge, A. Stoianov, R. Gilroy and B.V.K. Vijaya Kumar, "BiometricEncryption," ICSA Guide to Cryptography, McGrow-Hill, 1999, also available athttp://www.bioscrypt. com/assets/Biometric_Encryption.pdf.

10. C. Soutar, D. Roberge, A.V. Stoianov, R. Gilroy, and B. V. K. Vijaya Kumar. Method for secure key management using a biometric, U.S. Patent 6219794, Apr. 17, 2001 (Priority Date: Apr. 21, 1997).

11. V. Bjorn. Cryptographic key generation using biometric data. U.S. Patent 6035398, Mar. 7, 2000 (Priority date: Nov. 14, 1997).

12. G.I. Davida, Y. Frankel, and B.J. Matt. On enabling secure applications through off-line biometric identification. In Proc. of the IEEE 1998 Symp. on Security and Privacy, pp. 148–157, Oakland, Ca., 1998.

13. G. I. Davida, Y. Frankel, B.J. Matt, and R. Peralta, "On the relation of error correction and cryptography to an off line biometrics based identification scheme," Workshop on Coding and Cryptography, 1999. pp. 129 - 138.

14. F. Monrose, M.K. Reiter, and R. Wetzel, “Password hardening based on keystroke dynamics,” Proceedings of sixth ACM Conference on Computer and Communications Security, CCCS 1999. pp. 73 – 82.

15. F. Monrose, M.K. Reiter, Q. (Peter) Li , and S. Wetzel. Cryptographic Key Generation from Voice (Extended Abstract).In Proceedings of the 2001 IEEE Symposium on Security and

16. F. Monrose, M.K. Reiter, Q. (Peter) Li , and S. Wetzel. Using Voice to GenerateCryptographic Keys. In 2001: A Speaker Odyssey. The Speech Recognition Workshop,Crete, Greece, June, 2001. Six pages.

17. F. Monrose, M.K. Reiter, and S. Wetzel. Password hardening based on keystroke dynamics. International Journal on Information Security, Springer, Volume 1, Number 2, pp. 69–83, 2002.

18. F. Monrose, M. K. Reiter, Q. Li, D. P. Lopresti, and C. Shih, “Toward speech-generated cryptographic keys on resource constrained devices,” in Proc. 11th USENIX Security Symp., 2002, pp. 283–296.

19. A. Juels and M. Wattenbeg. A fuzzy commitment scheme. In Sixth ACM Conference on Computer and Communications Security, pp. 28-36. ACM Press, 1999. New York.

20. P.K. Janbandhu and M.Y. Siyal, “Novel biometric digital signature for Internet based applications,” Information Management and Computer Security, Vol. 9, No. 5, pp. 205–212, 2001.

21. A. Juels and M. Sudan. A fuzzy vault scheme, Proceedings 2002 IEEE International Symposium on Information Theory, Piscataway, NJ, p. 408, 2002.

22. T. C. Clancy, N. Kiyavash, D. J. Lin. Secure Smartcard-Based Fingerprint Authentication. Proc.ACMSIGMM 2003 Multimedia, Biometrics Methods and Applications Workshop (WBMA’03), November 8, 2003, Berkeley, California, USA. pp. 45-52.

23. U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain. Biometric Cryptosystems: Issues and Challenges. Proceedings of the IEEE, v. 92, no. 6, June 2004, pp. 948–960.

24. A. K. Jain, A. Ross, and S. Pankanti. Biometrics: A Tool for Information Security. IEEE transactions on information forensics and security, vol. 1, No. 2, June 2006, pp. 125–143.

25. U. Uludag, S. Pankanti, A. K. Jain. Fuzzy Vault for Fingerprints. AVBPA 2005 : audio- and video-based biometric person authentication (Hilton Rye Town NY, 20-22 July 2005). Springer, 20051973, vol. 3546, p.p. 310-319.

26. S. Yang and I. Verbauwhede, “Secure fuzzy vault based fingerprint verification system.” In Thirty-Eighth Asilomar Conference on Signals, Systems, and Computers (2004), v. 1, pp. 577–581, 2004.

27. A. Nagar, S. Chaudhury. Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme. 18th International Conference on Pattern Recognition (ICPR‘06), 2006. ICPR (4) 2006: pp. 537-540.

28. J.-P. Linnartz and P. Tuyls. New shielding functions to enhance privacy and prevent misuse of biometric templates. In Proc. of the 4th Int. Conf. on Audio and Video Based Biometric Person Authentication, pp. 393– 402, Guildford, UK, 2003.

29. E. Verbitskiy, P. Tuyls, D. Denteneer, and J.-P. Linnartz. Reliable biometric authentication with privacy protection. In Proc. of the 24th Symp. on Inf. Theory in the Benelux, pp. 125–132, Veldhoven, The Netherlands, 2003.

30. P. Tuyls and J. Goseling. Capacity and examples of template protecting biometric authentication systems. Biometric Authentication Workshop, Prague, 15 May 2004 (ECCV2004). pp. 158-170.

31. P. Tuyls, E. Verbitskiy, J. Goseling, D. Denteneer. Privacy protecting biometric authentication systems: an overview. XII European Signal Processing Conference (EUSIPCO 2004, Vienna, Austria), pp. 1397–1400.

32. Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. Proc. Eurocrypt 2004, pp. 523-540, 2004.

33. X. Boyen, "Reusable cryptographic fuzzy extractors," CCS 2004, pp. 82–91, ACM Press. (http://ai.stanford.edu/~xb/ccs04/slides/index.html - presentation slides)

34. A. Burnett, F. Byrne, T. Dowling, and A. Duffy. A Biometric Identity Based Signature Scheme. Applied Cryptography and Network Security Conference, Columbia University, New York, USA, 2005.

35. K. Voderhobli, C. Pattinson, and H. Donelan. A schema for cryptographic keys generation using hybrid biometrics. In: 7th annual postgraduate symposium: The convergence of telecommunications, networking and broadcasting, 26-27 June 2006, Liverpool, UK.

36. F. Hao, C.W. Chan, "Private key generation from on-line handwritten signatures,"Information Management & Computer Security, Issue 10, No. 2, pp. 159–164, 2002.

37. U. Martini, S. Beinlich. Virtual PIN: Biometric Encryption Using Coding Theory. BIOSIG: Biometric and Electronic Signatures, Proceedings of the 1st Conference on Biometrics and Electronic Signatures of the GI Working Group BIOSIG, 24th July 2003 in Darmstadt, Germany, pp. 91–99.

38. P. Tuyls, A. H. M. Akkermans, T. A. M. Kevenaar, G.-J. Schrijen, A. M. Bazen, and R. N. J. Veldhuis. Practical Biometric Authentication with Template Protection, 5th International Conference, AVBPA 2005, Hilton Rye Town, NY, USA, July 20-22, 2005. Lecture Notes in Computer Science, vol. 3546, p.p. 436 - 446, Springer, 2005.

39. A. Goh, D.C.L. Ngo, "Computation of cryptographic keys from face biometrics, "International Federation for Information Processing 2003, Springer-Verlag, in: Lecture Notes in Computer Science (LNCS) v. 2828, pp. 1–13, 2003.

40. M. van der Veen, T. Kevenaar, G.-J. Schrijen, T. H. Akkermans, and Fei Zuo. Face Biometrics with Renewable Templates, Proceedings of SPIE, Volume 6072: Security, Steganography, and Watermarking of Multimedia Contents VIII, Edward J. Delp III, Ping Wah Wong, Editors, 60720J (San Jose, Feb. 15, 2006)

41.T. Kevenaar, G.J. Schrijen, A. Akkermans, M. Damstra, P. Tuyls, and M. van der Veen. Robust and Secure Biometrics: Some Application Examples. Information Security Solutions Europe (ISSE) Conference, Rome, 10 -12 October, 2006.

42. Q. Li, X. Niu, and S. Sun. A Novel Biometric Key Scheme. (Chinese Journal of Electronics. 2005). http://www.paper.edu.cn.

43. F. Hao, R. Anderson, and J. Daugman. Combining Crypto with Biometrics Effectively. IEEE Transactions on Computers, vol.55, no.9, pp. 1081-1088, Sept., 2006. (See also: Technical report No. 640, University of Cambridge, Computer Laboratory, July 2005, available at (http://www.cl.cam.ac.uk/TechReports/)

44. Q. Li, Y. Sutcu, and N. Memon, "Secure sketch for biometric templates", Advances in Cryptology – ASIACRYPT 2006. Lecture Notes in Computer Science, vol. 4284, p.p. 99 - 113, Springer, 2006.

45. Y. Sutcu, Q. Li, and N. Memon, "How to Protect Biometric Templates", SPIE Conf. on Security,Steganography and Watermarking of Multimedia Contents IX, January 2007, San Jose,CA. Proceedings of SPIE, v. 6505. Editors: Edward J. Delp III, Ping Wah Wong, 2007.

46. A. Adler. Vulnerabilities in Biometric Encryption Systems. Audio- and video-based Biometric Person Authentication (AVBPA). 2005: 1100–1109.

47. E.-C. Chang, R. Shen, and F. W. Teo. Finding the Original Point Set Hidden among Chaff. Proceedings of the 2006 ACM Symposium on Information, computer and communications security. ASIACCS'06 March 21-24, 2006, Taipei, Taiwan. pp. 182–188.

48. R.M. Bolle, J.H.Connel, and N.K.Ratha. "System and method for distorting a biometric for transactions with enhanced security and privacy," US Patent 6,836,554. Dec. 28, 2004 (Priority Date: June 16, 2000).

49. N. K. Ratha, J. H. Connell, and R. M. Bolle. Enhancing security and privacy in biometrics-based authentication systems. IBM SYSTEMS JOURNAL, VOL 40, NO 3, pp. 614–634, 2001.

50. R.M.Bolle, J.H.Connel, and N.K.Ratha, Biometric perils and patches, Pattern Recognition 35, No.12 (2002) pp. 2727–2738.

51. N. K. Ratha, J. Connell, R. M. Bolle, and S. Chikkerur: Cancelable Biometrics: A Case Study in Fingerprints. Proceedings of the 18th International Conference on Pattern Recognition (ICPR 2006), 20-24 August 2006, Hong Kong, China. ICPR (4) 2006: 370-373.

52. M. Savvides, B.V.K.Vijaya Kumar and P.K.Khosla. Cancelable biometric filters for face recognition. Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04), Cambridge, England. v.3, 922–925, 2004.

53. M. Braithwaite, U.C. von Seelen, J. Cambier, J. Daugman , R. Glass, R. Moore, and I. Scott. Application-specific biometric templates, IEEE Workshop on Automatic Identification Advanced Technologies, Tarrytown, NY, March 14-15, 2002, pp.167-171.

54. M. Tiberg. "A Method and a System for Biometric Identification or Verification." Swedish patent 0202147-5, Priority date: July 9, 2002. PCT patent no. WO 2004/006495 , PCT/ SE2003/001181. US Patent Application US2005/0210269 A1, Sep. 22, 2005.

55. A. Teoh , D. Ngo, and A. Goh. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognition 37 (2004) 2245–2255.

56. T. Connie, A. Teoh, M. Goh, and D. Ngo. PalmHashing: a novel approach for cancelable biometrics. Information Processing Letters 93 (2005), pp. 1–5.

57. D. C. L. Ngo, A. B. J. Teoh, and A. Goh. Biometric Hash: High-Confidence FaceRecognition. IEEE Transactions on circuits and systems for video technology, vol. 16, No. 6, June 2006, pp.771-775.

58. D. Maio and L. Nanni, "MultiHashing, human authentication featuring biometrics data and tokenised random number: a case study FVC2004," NeuroComputing, vol. 69, pp. 242-249, December 2005. Available at http://bias.csr.unibo.it/gpubs/__docs__/2005_MHA_NeuroC.zip.

59. A. Lumini and L. Nanni, „An improved BioHashing for human authentication", Pattern Recognition , vol.40, no.3, pp.1057-1065, 2006. Available at http://bias.csr.unibo.it/gpubs/__docs__/2006_BioH.zip.

60. L. Nanni and A. Lumini, "Human authentication featuring signatures and tokenised random number," NeuroComputing , vol.69, no.7-9, pp.858-861, March 2006. Available at http://bias.csr.unibo.it/gpubs/__docs__/2006_HAF_NeuroC.zip.

61. L. Nanni and A. Lumini, "An advanced multi-modal method for human authentication featuring biometrics data and tokenised random numbers," NeuroComputing , vol. 69, no. 13, pp. 1706-1710, August 2006. Available at http://bias.csr.unibo.it/gpubs/__docs__/2006_ AMM_NeuroC.zip.

62. R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates". ACISP: Australasian conference on information security and privacy No10, Brisbane , Australia (4-6 July 2005). Lecture Notes in Computer Science, vol. 3574, p.p. 242-252, Springer, 2005.

63. S. Tulyakov, F. Farooq, and V. Govindaraju, "Symmetric hash functions for fingerprint minutiae," in Lecture Notes in Computer Science, vol. 3687, p.p. 30-38, Springer, 2005.

64. A. Sahai and B. Waters, "Fuzzy identity based encryption," in Proceedings of EUROCRYPT'05 on Advances in Cryptoglogy, LNCS 3494, pp. 457–473, Springer-Verlag, 2005.

65. D. Nali, C. Adams, and A. Miri. Using Threshold Attribute-Based Encryption for Practical Biometric-Based Access Control. International Journal of Network Security, Vol.1, No.3, pp.173–182, Nov. 2005 (http://isrc.nchu.edu.tw/ijns/)

DÉCISIONS DE LA CNIL EN MATIÈRE DE BIOMÉTRIE

1) Délibération 2007-080, 2007-04-25, Délibération autorisant la mise en oeuvre par les Hôpitaux Universitaires de Strasbourg d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour fmalité le contrôle de l'accès aux blocs opératoires.

2) Délibération 2007-081, 2007-04-25, Délibération autorisant la mise en oeuvre par la société Fenwick 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 chariots élévateurs.

3) Délibération 2007-082, 2007-04-25, Délibération autorisant la mise en oeuvre par la SCP Regnard - Beder - Denfer & Bodet, titulaire de l'office de greffier du Tribunal de Commerce de Paris, 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 la salle informatique.

4) Délibération 2007-083, 2007-04-25, Délibération refusant la mise en oeuvre par la mairie de Metz 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 la salle informatique.

5) Délibération 2007-084, 2007-04-25, Délibération autorisant la mise en oeuvre par la société Sanofi Pasteur 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 au poste de pilotage des automates de production.

6) Délibération 2007-085, 2007-04-25, Délibération refusant la mise en oeuvre par la société Solymatic France 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.

7) Délibération 2007-086, 2007-04-25, Délibération autorisant la mise en oeuvre par la société TNT Express France 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 au centre de contrôle.

8) Délibération 2007-087, 2007-04-25, Délibération autorisant la mise en oeuvre par la société Sogeti Infrastructure Services 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.

9) Délibération 2007-089, 2007-04-25, Délibération autorisant la mise en oeuvre par la société Maguin 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.

10) Délibération 2007-090, 2007-04-25, Délibération autorisant la mise en oeuvre par le Service Départemental d'Incendie et de Secours du Maine et Loire 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.

11) Délibération 2007-091, 2007-04-25, Délibération refusant la mise en oeuvre par l'Autorité de contrôle des assurances et des mutuelles (ACAM) 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 au réseau informatique (postes de travail fixes et portables).

12) Délibération 2007-093, 2007-04-25, Délibération refusant la mise en oeuvre par la société la société CSV International 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.

13) Délibération 2007-050, 2007-03-21, Délibération autorisant la mise en oeuvre 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.

14) Délibération 2007-051, 2007-03-21, Délibération autorisant la mise en oeuvre 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.

15) Délibération 2007-052, 2007-03-21, Délibération autorisant la mise en oeuvre par le service interacadémique des examens et de concours 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 comportant les sujets nationaux d'examens et de concours.

16) Délibération 2007-054, 2007-03-21, Délibération autorisant la mise en oeuvre 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.

17) Délibération 2007-055, 2007-03-21, Délibération refusant la mise en oeuvre par la société Gestion Location Intervention Exploitation (GLIE) 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.

18) Délibération 2007-056, 2007-03-21, Délibération autorisant la mise en oeuvre 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.

19) Délibération 2007-057, 2007-03-21, Délibération autorisant la mise en oeuvre par le Commissariat à l'Energie Atomique 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 au centre d'étude de Valduc.

20) Délibération 2007-041, 2007-03-08, Délibération portant autorisation de la mise en oeuvre par Aéroports de Paris 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 au sein de la zone réservée du satellite S3 de l'aéroport de Paris-Charles-de-Gaulle.

21) Délibération 2007-025, 2007-02-08, Délibération autorisant la mise en oeuvre par l'Etablissement Public du Musée du Louvre 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 clés de certains locaux du Musée du Louvre.

22) Délibération 2007-006, 2007-01-18, Délibération autorisant la mise en oeuvre 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.

23) Délibération 2007-007, 2007-01-18, Délibération autorisant la mise en oeuvre par la société Sagem Défense Sécurité d'un traitement automatisé de données à caractère personnel ayant pour finalité principale le développement d'algorithmes de reconnaissance du visage en trois dimensions.

24) Délibération 2007-002, 2007-01-11, Délibération portant autorisation unique de mise en oeuvre de traitements automatisés de données à caractère personnel relatifs à la gestion d'infractions à la police des services publics de transports terrestres.

25) Délibération 2006-296, 2006-12-21, Délibération autorisant la mise en oeuvre par la Commission bancaire 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 au contenu de clés USB.

26) Délibération 2006-298, 2006-12-21, Délibération autorisant la mise en oeuvre par l'Autorité de contrôle des assurances et des mutuelles (ACAM) 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 au contenu de clés USB.

27) Délibération 2006-265, 2006-12-05, Délibération autorisant la mise en oeuvre d'un dispositif biométrique reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sut un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès au casino Cagnes-sur-Mer Loisirs SAS.

28) Délibération 2006-262, 2006-12-05, Délibération autorisant la mise en oeuvre d'un 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 au casino de Bagnères-de-Bigorre Loisirs SAS.

29) Délibération 2006-263, 2006-12-05, Délibération autorisant la mise en oeuvre d'un 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 au GIE casinos Conseil et Service.

30) Délibération 2006-264, 2006-12-05, Délibération autorisant la mise en oeuvre d'un dispositif biométrique reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sut un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès au casino Amneville Loisirs SAS.

31) Délibération 2006-266, 2006-12-05, Délibération autorisant la mise en oeuvre d'un 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 au casino Luc-sur-Mer SAS.

32) Délibération 2006-267, 2006-12-05, Délibération autorisant la mise en oeuvre d'un dispositif biométrique reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sut un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès au casino de Grau du Roi Loisirs SAS.

33) Délibération 2006-268, 2006-12-05, Délibération autorisant la mise en oeuvre d'un 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 au casino Dunkerque Loisirs SAS.

34) Délibération 2006-269, 2006-12-05, Délibération autorisant la mise en oeuvre d'un 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 au casino Pau Loisirs SAS.

35) Délibération 2006-270, 2006-12-05, Délibération 2006 autorisant la mise en oeuvre d'un 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 au casino Neris Loisirs SAS.

36) Délibération 2006-271, 2006-12-05, Délibération autorisant la mise en oeuvre d'un disposition biométrique reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée su un support individuel détenu par la personne concernée et ayant pour finalité le contrôle d l'accès au casino Roscoff Loisirs SAS.

37) Délibération 2006-272, 2006-12-05, Délibération autorisant la mise en oeuvre d'un 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 au casino de Saint Gervais Loisirs SAS.

38) Délibération 2006-274, 2006-12-05, Délibération autorisant la mise en oeuvre d'un dispositif biométrique reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée si un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès au casino Sète Loisirs SAS.

39) Délibération 2006-275, 2006-12-05, Délibération autorisant la mise en oeuvre d'un 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 au casino Valras plage Loisirs SAS.

40) Délibération 2006-276, 2006-12-05, Délibération autorisant la mise en oeuvre d'un 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 au casino Villers-sur-Mer Loisirs SAS.

41) Délibération 2006-277, 2006-12-05, Délibération autorisant la mise en oeuvre d'un 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 au casino Yport Loisirs SAS.

42) Délibération 2006-278, 2006-12-05, Délibération autorisant la mise en oeuvre d'un 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 au casino Argelès-Gazost Loisirs SAS.

43) Délibération 2006-273, 2006-12-05, Délibération autorisant la mise en oeuvre d'un 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 au casino Pougues Loisirs SAS.

44) Délibération 2006-232, 2006-10-17, Délibération autorisant la mise en oeuvre par la société l'Oréal SA d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité l'identification des personnes à l'occasion de la signature de documents électroniques.

46) Délibération 2006-217, 2006-09-28, Délibération portant autorisation de la mise en oeuvre par Aéroport de Paris SA d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité d'assurer la confidentialité et la protection des données stockées dans un ordinateur portable.

47) Délibération 2006-172, 2006-06-27, Délibération portant autorisation de la mise en oeuvre par la société Sanofi Chimie d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des accès logiques au système d'information.

49) Délibération 2006-153, 2006-05-30, Délibération portant refus d'autorisation de la mise en oeuvre par la société Rothschild et Compagnie Banque 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 de l'accès aux locaux.

50) Délibération 2006-154, 2006-05-30, Délibération portant refus d'autorisation de la mise en oeuvre par la société Rothschild & Compagnie 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 de l'accès aux locaux.

51) Délibération 2006-155, 2006-05-30, Délibération portant refus d'autorisation de la mise en oeuvre par la société Rothschild & Compagnie Gestion 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 de l'accès aux locaux.

52) Délibération 2006-156, 2006-05-30, Délibération portant refus d'autorisation de la mise en oeuvre par la société Rothschild Gestion 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 de l'accès aux locaux.

53) Délibération 2006-157, 2006-05-30, Délibération portant refus d'autorisation de la mise en oeuvre par la société Murano Urban Resort 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 de l'accès aux chambres de l'hôtel.

54) Délibération 2006-158, 2006-05-30, Délibération portant autorisation de la mise en oeuvre 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.

55) Délibération 2006-132, 2006-05-09, Délibération portant autorisation de la mise en oeuvre par la société Atos Worldline 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.

56) Délibération 2006-133, 2006-05-09, Délibération portant autorisation de la mise en oeuvre par la société Sodebo 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 de l'accès à certains locaux.

57) Délibération 2006-134, 2006-05-09, Délibération portant autorisation de la mise en oeuvre par la Caisse d'Allocations Familiales de la Seine Saint-Denis d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des accès aux locaux.

58) Délibération 2006-135, 2006-05-09, Délibération portant autorisation de la mise en oeuvre par la société Visual 102 d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des accès à un site de tournage.

59) Délibération 2006-136, 2006-05-09, Délibération portant autorisation de la mise en oeuvre par la banque Finama d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle des accès logiques au poste de travail.

60) Délibération 2006-101, 2006-04-27, Délibération portant autorisation unique de mise en oeuvre 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.

61) Délibération 2006-102, 2006-04-27, Délibération portant autorisation unique de mise en oeuvre 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.

62) Délibération 2006-103, 2006-04-27, Délibération portant autorisation unique de mise en oeuvre 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.

63) Délibération 2006-106, 2006-04-27, Délibération portant autorisation de mise en oeuvre par le lycée Léon Chiris d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire.

64) Délibération 2006-107, 2006-04-27, Délibération portant autorisation de mise en oeuvre par l'O.G.E.C Sainte-Marie/Saint-Vincent d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire.

65) Délibération 2006-108, 2006-04-27, Délibération portant autorisation de mise en oeuvre par l'Ensemble Scolaire Catholique Rochois Sainte-Marie/Sainte-Famille d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire.

66) Délibération 2006-109, 2006-04-27, Délibération portant autorisation de la mise en oeuvre par le Service Départemental Incendie et Secours de la Haute Corse 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.

67) Délibération 2006-092, 2006-04-06, Délibération portant autorisation de mise en oeuvre par le lycée Paul Augier de Nice d'un traitement automatisé 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 demi-pension.

68) Délibération 2006-093, 2006-04-06, Délibération portant autorisation de mise en oeuvre par le collège Gérard Philipe de Martigues d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire.

69) Délibération 2006-094, 2006-04-06, Délibération portant autorisation de mise en oeuvre par le collège Louisa Paulin de Muret d'un traitement automatisé 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 demi-pension.

70) Délibération 2006-095, 2006-04-06, Délibération portant autorisation de mise en oeuvre par le lycée Henri Matisse de Trappes d'un traitement automatisé 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 demi-pension.

71) Délibération 2006-096, 2006-04-06, Délibération portant autorisation de la mise en oeuvre par la société ALSATEL S.A. 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 et à la salle informatique.

72) Délibération 2006-097, 2006-04-06, Délibération portant autorisation de la mise en oeuvre par la société APELEM 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.

73) Délibération 2006-098, 2006-04-06, Délibération portant autorisation de la mise en oeuvre par la société Carrefour 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 de l'accès à certains locaux.

74) Délibération 2006-099, 2006-04-06, Délibération portant autorisation de la mise en oeuvre par la société Diagnostic Medical Systems (DMS) 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.

75) Délibération 2006-068, 2006-03-16, Délibération portant autorisation de la mise en oeuvre par la société Assistance Totale en Maintenance (ATM) 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.

76) Délibération 2006-069, 2006-03-16, Délibération portant autorisation de la mise en oeuvre 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.

77) Délibération 2006-070, 2006-03-16, Délibération portant autorisation de la mise en oeuvre 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.

78) Délibération 2006-071, 2006-03-16, Délibération portant autorisation de la mise en oeuvre 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.

79) Délibération 2006-065, 2006-03-16, Délibération portant avis sur un projet de décret modifiant le 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.

80) Délibération 2006-058, 2006-03-02, Délibération portant autorisation de la mise en oeuvre par l'Etablissement Public Administratif Euroméditerranée 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 d'accès aux locaux et le contrôle des horaires des employés.

81) Délibération 2006-059, 2006-03-02, Délibération portant autorisation de la mise en oeuvre par la SCM Imagerie Rouen-Elbeuf-Le Neubourg 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.

82) Délibération 2006-049, 2006-02-23, Délibération portant autorisation de mise en oeuvre par le lycée Maurice Ravel d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire.

83) Délibération 2006-021, 2006-02-02, Délibération portant autorisation de la mise en oeuvre par la Caisse d'Allocations Familiales de la Seine Saint-Denis d'un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle des accès aux locaux par reconnaissance des empreintes digitales.

84) Délibération 2006-022, 2006-02-02, Délibération portant autorisation de la mise en oeuvre par la banque FINAMA d'un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle des accès aux locaux informatiques par reconnaissance des empreintes digitales.

85) Délibération 2006-023, 2006-02-02, Délibération portant autorisation de la mise en oeuvre par la SCM Imagerie Médicale Jeanne d'Arc 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.

86) Délibération 2006-024, 2006-02-02, Délibération portant autorisation de la mise en oeuvre par la société TAGG INFORMATIQUE 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 d'une part le contrôle de l'accès aux locaux, et d'autre part, le contrôle des horaires.

87) Délibération 2006-025, 2006-02-02, Délibération 2006 portant autorisation de la mise en oeuvre par la société TOTAL S.A. 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 de l'accès aux passes d'étages et aux clefs des locaux à risques.

88) Délibération 2006-026, 2006-02-02, Délibération portant autorisation de la mise en oeuvre par la société ARMATIS S.A. 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 de l'accès aux locaux.

89) Délibération 2006-027, 2006-02-02, Délibération portant autorisation de la mise en oeuvre par la société GONESDIS 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 de l'accès aux locaux.

90) Délibération 2006-028, 2006-02-02, Délibération portant autorisation de la mise en oeuvre par la SNC ARMATIS Ile-de-France 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 de l'accès aux locaux.

92) Délibération 2006-031, 2006-02-02, Délibération portant autorisation de mise en oeuvre par le collège Roland Garros d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire.

93) Délibération 2006-002, 2006-01-12, Délibération portant refus d'autorisation de la mise en oeuvre par la société Air Promotion Group 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 de l'accès aux locaux.

94) Délibération 2006-003, 2006-01-12, Délibération portant refus d'autorisation de la mise en oeuvre par le cabinet Breese - Derambure et Majerowicz 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 de l'accès aux locaux.

95) Délibération 2006-004, 2006-01-12, Délibération portant refus d'autorisation de la mise en oeuvre par la Société du Marché d'Intérêt National d'Avignon (SMINA) 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 de l'accès aux locaux.

96) Délibération 2006-005, 2006-01-12, Délibération portant refus d'autorisation de la mise en oeuvre 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.

97) Délibération 2006-006, 2006-01-12, Délibération portant autorisation de mise en oeuvre par le lycée de la Vallée de Chevreuse d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire.

98) Délibération 2006-007, 2006-01-12, Délibération portant autorisation de mise en oeuvre par le lycée Thierry Maulnier d'un traitement automatisé de données à caractère personnel reposant sur la

reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire.

99) Délibération 2005-313, 2005-12-20, Délibération portant avis sur le projet de décret modifiant le 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.

100) Délibération 2005-279, 2005-11-22, Délibération portant avis sur le projet de décret instituant le passeport électronique et sur les modifications apportées au traitement DELPHINE permettant l'établissement, la délivrance et la gestion des passeports.

101) Délibération 2005-281, 2005-11-22, Délibération portant autorisation de la mise en oeuvre par la Cité des Sciences et de l'Industrie 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 de l'accès aux locaux.

102) Délibération 2005-282, 2005-11-22, Délibération portant autorisation de la mise en oeuvre par la Direction Régionale des Services Pénitentiaires (DRSP) de Marseille 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 de l'accès à l'armurerie.

103) Délibération 2005-283, 2005-11-22, Délibération portant autorisation de la mise en oeuvre par le Conseil Général de la Côte d'Or 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 de l'accès aux locaux.

104) Délibération 2005-253, 2005-11-10, Délibération portant autorisation de mise en oeuvre par le lycée Jules Fil d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire.

105) Délibération 2005-244, 2005-11-03, Délibération portant autorisation de la mise en oeuvre par le lycée professionnel de Vedène d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire.

106) Délibération 2005-245, 2005-11-03, Délibération portant autorisation de la mise en oeuvre par la société Keynectis 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 de l'accès aux locaux.

107) Délibération 2005-246, 2005-11-03, Délibération portant autorisation de la mise en oeuvre par la société FCI France d'un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle des accès par reconnaissance des empreintes digitales.

108) Délibération 2005-247, 2005-11-03, Délibération portant autorisation de la mise en oeuvre par la société lnfo Service Europe 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 de ses employés.

109) Délibération 2005-248, 2005-11-03, Délibération portant autorisation de la mise en oeuvre par la société Ferma 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 avant pour finalité le contrôle de l'accès aux locaux.

110) Délibération 2005-249, 2005-11-03, Délibération portant autorisation de la mise en oeuvre par le Cabinet Lexvia d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité de sécuriser l'accès aux documents ainsi que leur envoi par courrier électronique.

111) Délibération 2005-250, 2005-11-03, Délibération portant autorisation de la mise en oeuvre par la société Bouygues Telecom 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 de l'accès aux locaux.

112) Délibération 2005-251, 2005-11-03, Délibération portant autorisation de la mise en oeuvre par la société Aeromecanic 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 de l'accès aux zones dites réservées.

113) Délibération 2005-252, 2005-11-03, Délibération portant autorisation de la mise en oeuvre par la société Plastic Omnium 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 de l'accès aux locaux.

114) Délibération 2005-206, 2005-09-22, Délibération portant autorisation de mise en oeuvre d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité de contrôler l'accès logique à un service d'informations financières de la société Bloomberg L.P.

115) Délibération 2005-169, 2005-07-05, Délibération portant autorisation de mise en oeuvre par le collège "Les Mimosas" d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance du contour de la main et ayant pour finalité de contrôler l'accès au restaurant scolaire.

116) Délibération 2005-185, 2005-07-05, Délibération portant autorisation de mise en oeuvre par la société Claranet d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de la forme de la main et ayant pour finalité de contrôler l'accès à la salle d'hébergement informatique.

117) Délibération 2005-186, 2005-07-05, Délibération portant autorisation de mise en oeuvre par la société Carrefour Hypermarchés France d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de la forme de la main et ayant pour finalité de contrôler l'accès à certains locaux de l'établissement de la Valette du Var.

118) Délibération 2005-162, 2005-06-21, Délibération autorisant la mise en oeuvre par la société Reichen et Robert & associés architectes urbanistes 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 de l'accès aux locaux.

119) Délibération 2005-163, 2005-06-21, Délibération autorisant la mise en oeuvre par la mairie de Gagny 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 de ses employés.

120) Délibération 2005-135, 2005-06-14, Délibération autorisant la mise en oeuvre par le Centre hospitalier de Hyères 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 de ses employés.

121) Délibération 2005-136, 2005-06-14, Délibération portant autorisation de mise en oeuvre à titre expérimental par La Poste à Vigneux-sur-Seine d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité de contrôler l'accès aux locaux.

122) Délibération 2005-137, 2005-06-14, Délibération portant autorisation de mise en oeuvre à titre expérimental par La Poste à Palaiseau d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité de contrôler l'accès aux locaux.

123) Délibération 2005-138, 2005-06-14, Délibération portant autorisation de mise en oeuvre à titre expérimental par La Poste à Aubervilliers d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité de contrôler l'accès aux locaux.

124) Délibération 2005-139, 2005-06-14, Délibération portant autorisation de mise en oeuvre à titre expérimental par La Poste à Noisy-le-Sec d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de la forme de la main et ayant pour finalité de contrôler l'accès aux locaux.

125) Délibération 2005-140, 2005-06-14, Délibération portant autorisation de mise en oeuvre par La Poste à Argenteuil d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de la forme de la main et ayant pour finalité de contrôler l'accès aux locaux.

126) Délibération 2005-148, 2005-06-14, Délibération portant autorisation de la mise en oeuvre par la Cité des sciences et de l'industrie d'un traitement automatisé de données à caractère personnel ayant pour finalité l'expérimentation de dispositifs de reconnaissance biométrique dans le cadre d'une exposition pédagogique.

127) Délibération 2005-149, 2005-06-14, Délibération portant autorisation de la mise en oeuvre par l'Institut National des Hautes Etudes de Sécurité (INHES) d'un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle des accès par reconnaissance des empreintes digitales.

128) Délibération 2005-113, 2005-06-07, Délibération portant autorisation de la mise en oeuvre par le groupe Imprimerie Nationale d'un traitement automatisé de données à caractère personnel ayant pour finalité le contrôle des accès par reconnaissance des empreintes digitales.

129) Délibération 2005-115, 2005-06-07, Délibération portant autorisation de la mise en oeuvre par la Chambre de Commerce et d'Industrie de Nice-Côte d'Azur d'un traitement automatisé de données à caractère personnel ayant pour finalité la gestion d'une carte de fidélité impliquant l'utilisation d'un dispositif biométrique de reconnaissance des empreintes digitales.

130) Délibération 2005-064, 2005-04-20, Délibération portant autorisation de la mise en oeuvre par la direction des Monnaies et Médailles d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de la forme de la main et ayant pour finalité de contrôler l'accès aux locaux sensibles.

131) Délibération 2005-023, 2005-02-17, Délibération portant autorisation de la mise en oeuvre par la Banque de France d'un traitement automatisé de données à caractère personnel ayant pour finalité de contrôler l'accès aux locaux sensibles.

132) Délibération 2005-031, 2005-02-17, Délibération portant refus d'autorisation de la mise en oeuvre 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.

133) Délibération 2005-034, 2005-02-17, Délibération portant refus d'autorisation de la mise en oeuvre 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.

134) Délibération 2005-035, 2005-02-17, Délibération portant refus d'autorisation de la mise en oeuvre 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.

135) Délibération 2005-036, 2005-02-17, Délibération portant refus d'autorisation de la mise en oeuvre 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.

136) Délibération 2005-037, 2005-02-17, Délibération portant refus d'autorisation de la mise en oeuvre 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.

137) Délibération 2005-020, 2005-02-10, 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 effectués lors du passage de la frontière à l'aéroport Roissy-Charles-de-Gaulle.

138) Délibération 2005-001, 2005-01-13, Délibération portant autorisation d'un traitement automatisé de données à caractère personnel présenté par la société TF1 et concernant la mise en oeuvre d'un système de contrôle des accès par biométrie.

139) Délibération 04-075, 2004-10-05, Délibération portant avis sur le projet de décret en Conseil d'Etat pris pour l'application de l'article 8-4 de l'ordonnance 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 de données à caractère personne relatives aux ressortissants étrangers sollicitant la délivrance d'un visa.

140) Délibération 04-068, 2004-06-24, Délibération portant avis sur le projet de décret du ministre de l'intérieur modifiant le décret du 8 avril 1987 relatif au fichier automatisé des empreintes digitales.

141) Délibération 04-017, 2004-04-08, Délibération relative à une demande d'avis de l'établissement public Aéroports de Paris concernant la mise en oeuvre d'un contrôle d'accès biométrique aux zones réservées de sûreté des aéroports d'Orly et de Roissy.

142) Délibération 04-018, 2004-04-08, Délibération relative à une demande d'avis présentée par le Centre hospitalier de Hyères concernant la mise en oeuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion du temps de travail de ses personnels.

143) Délibération 03-065, 2003-12-16, Délibération portant avis sur le traitement automatisé d'informations nominatives, mis en oeuvre par la mairie de Levallois-Perret, destiné à contrôler l'accès au "Roller-Parc" par la reconnaissance des empreintes digitales.

144) Délibération 03-036, 2003-07-01, Délibération portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique

145) Délibération 03-027, 2003-05-22, Délibération portant avis sur le projet d'arrêté du ministre de la justice portant avis sur le projet d'arrêté du ministre de la justice portant création d'une application informatique destinée à vérifier l'identité des détenus en établissement par reconnaissance de la morphologie de la main

146) Délibération 03-029, 2003-05-22, Délibération concernant la création par la direction générale des douanes et droits indirects d'un système d'information de lutte contre la fraude

147) Délibération 03-015, 2003-04-24, Délibération portant avis sur les articles 4 et 5 d'un projet de loi relatif à l'immigration

148) Délibération 02-070, 2002-10-15, Délibération portant avis sur le traitement automatisé d'informations nominatives, mis en oeuvre par le collège Joliot Curie de Carqueiranne, destiné à contrôler l'accès au restaurant scolaire par la reconnaissance de la géométrie de la main

149) Délibération 02-045, 2002-06-18, Délibération portant avis sur un projet de décision du directeur de l'URSSAF de la Corse relatif à la mise en oeuvre d'un dispositif de reconnaissance de l'empreinte digitale destiné à contrôler les accès aux locaux professionnels de l'URSSAF

150) Délibération 02-033, 2002-04-23, Délibération relative à la demande d'avis présentée par la mairie de Goussainville concernant la mise en oeuvre d'un dispositif de reconnaissance de l'empreinte digitale ayant pour finalité la gestion des horaires de travail des personnels communaux

151) Délibération 02-034, 2002-04-23, Délibération portant avis sur un projet de décision du directeur général de l'établissement public aéroports de Paris relative à une expérimentation de trois dispositifs biométriques de contrôle des accès aux zones réservées de sûreté des aéroports d'Orly et Roissy

152) Délibération 02-022, 2002-04-02, Délibération relative à la demande d'avis présentée par la mairie de Vandoeuvre-les-Nancy concernant l'expérimentation d'un dispositif de vote électronique par internet à l'élection présidentielle

153) Délibération 02-015, 2002-03-14, Délibération portant avis sur un projet d'arr^eté présenté par la mairie de Mérignac concernant l'expérimentation d'un dispositif de vote électronique reposant sur l'utilisation de cartes à microprocesseur comportant les empreintes digitales des électeurs

154) Délibération 02-001, norme simplifiée 42, 2002-01-08, Délibération concernant les traitements automatisés d'informations nominatives relatifs mis en oeuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration

155) Délibération 01-006, 2001-01-25, Délibération 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.

156) Délibération 00-056, 2000-11-16, Délibération portant avis sur un projet d'arrêté présenté par le ministre de l'éducation 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'éducation nationale, pour certains locaux de la cité académique de Lille.

157) Délibération 00-057, 2000-11-16, Délibération 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.

159) Délibération 98-033, 1998-03-31, Délibération portant avis sur un projet d'arrêté présenté par l'Office Français de Protection des Réfugiés et Apatrides relatif au fichier informatisé des empreintes digitales des demandeurs du statut de réfugié

160) Délibération 98-034, 1998-03-31, Délibération portant avis sur un projet d'arrêté modificatif concernant la gestion des formalités administratives relevant de l'Office Français de Protection des Réfugiés et Apatrides

161) Délibération 98-012, 1998-03-03, Délibération portant avis sur projet d'arrêté relatif au traitement automatisé d'informations nominatives de gestion électronique de documents (GED) mis en oeuvre par le ministère de l'intérieur français au sein du bureau national SIRENE

162) Délibération 97-044, 1997-06-10, Délibération portant avis sur un projet d'arrêté présenté par la Banque de France concernant un traitement automatisé d'informations nominatives ayant pour finalité la gestion des contrôles d'accès des agents par empreintes digitales.

163) Délibération 95-126, 1995-10-24, (AFFAIRES ETRANGERES, POLICE). Délibération portant avis sur une demande modificative présentée par l'Office français de protection des réfugiés et apatrides (OFPRA) relative à la durée de conservation des informations enregistrées dans le fichier dactyloscopique des demandeurs du statut de réfugié

164) Délibération 94-095, 1994-11-15, (APPLICATION DE LA LOI). Délibération 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.

165) Délibération 92-052, 1992-05-26, (AFFAIRES ETRANGERES, POLICE). Délibération portant avis sur la mise en oeuvre permanente d'un fichier dactyloscopique des demandeurs du statut de réfugiés par l'Office français de protection des réfugiés et apatrides

166) Délibération 92-026, 1992-03-17, (POLICE, INTERIEUR). Délibération portant avis sur un traitement automatisé d'informations nominatives mis en oeuvre par le ministère de l'intérieur relatif à la gestion automatisée de la délivrance des cartes nationales d'identité et des passeports.

167) Délibération 92-027, 1992-03-17, (AFFAIRES ETRANGERES, POLICE). Délibération portant sur une vérification sur place du fichier dactyloscopique des demandeurs du statut de réfugiés mis en oeuvre et géré par l'office français de protection des réfugiés et apatrides (O.F.P.R.A.).

168) Délibération 89-110, 1989-10-10, (AFFAIRES ETRANGERES, APPLICATION DE LA LOI). Délibération portant prorogation de l'avis favorable n° 87-106 du 3 novembre 1987 portant avis sur la mise en place par l'office français de protection des réfugiés et apatrides d'un traitement automatisé relatif à la dactyloscopie des demandeurs du statut de réfugié

169) Délibération 87-106, 1987-11-03, (AFFAIRES ETRANGERES). Délibération portant avis sur la mise en place par l'Office français de protection des réfugiés et apatrides d'un traitement automatisé relatif à la dactyloscopie des demandeurs du statut de réfugié

170) Délibération 86-105, 1986-10-21, (INTERIEUR, POLICE). Délibération portant avis sur le relevé d'une empreinte digitale à l'occasion d'une demande de carte nationale d'identité

171) Délibération 86-102, 1986-10-14, (INTERIEUR, POLICE). Délibération concernant un projet de décret relatif au fichier automatisé des empreintes digitales géré par le Ministère de l'Intérieur

172) Délibération 86-76, 1986-07-01, (INTERIEUR, POLICE). Délibération portant avis sur un projet de décret relatif à la création d'un système de fabrication et de gestion informatisée des cartes nationales d'identité

173) Délibération 84-18, 1984-05-03, (INTERIEUR, POLICE). Délibération relative à la mise en oeuvre par le Ministère de l'Intérieur d'un traitement automatisé d'empreintes digitales

Une carte de plus en plus sécurisée

1921, la première carte.
Création de la «carte d'identité de Français» par le préfet de police de la Seine Robert Leuillier. Il veut remédier aux problèmes liés à l'hétérogénéité des différents papiers (livret ouvrier, livret de famille, acte de naissance, etc).

Octobre 1940, les sous-citoyens.
Réclamée par l'autorité allemande et par les institutions vichystes, la mention «juif» est apposée sur la carte d'identité pour rendre visible une sous-citoyenneté.

1955, les musulmans d'Algérie.
Circulaire «confidentielle» du ministère de l'Intérieur qui détermine les dispositions à appliquer pour toute demande émanant de musulmans d'Algérie.

1987, la carte informatisée.
La carte nationale d'identité informatisée, créée par le décret du 19 mars 1987, remplace la carte d'identité «papier». Plus petite, plastifiée, elle est délivrée sur l'ensemble du territoire national depuis décembre 1995.

2008, la carte biométrique.
Projet de carte d'identité biométrique.

En Europe, une carte à géométrie variable

De Londres, où la carte d'identité n'existe pas, à Rome, où elle a autant de valeur qu'un permis de chasse, l'utilisation des papiers varie radicalement.

La France n'est pas le seul pays d'Europe où les citoyens doivent posséder une carte d'identité. La plupart de nos voisins y ont recours, avec cependant des usages et une rigueur différents.

Outre-Rhin, la carte d'identité est une obligation. A partir de 16 ans, les citoyens allemands doivent s'inscrire sur un registre et faire la demande d'une carte, à moins de détenir un passeport valable. Celle-ci est demandée pour toute démarche administrative. En Belgique, la carte d'identité est également obligatoire, dès l'âge de 15 ans. D'ici à 2009, la détention d'une carte devenue électronique sera imposée à tout citoyen âgé de plus de 12 ans. Contrairement au cas allemand, d'autres documents peuvent être utilisés en Belgique pour prouver son identité dans la vie courante.

Biométrique. Beaucoup plus utilisée qu'en France, la carte d'identité est le seul document officiel permettant de justifier son identité en Espagne. Ni permis de conduire ni autre papiers administratifs ne sont acceptés. Elle est obligatoire dèsl'âge de14 ans. Il est prévu que toutes les cartes délivrées à partir de 2008 seront électroniques et intégreront des composants biométriques. Si la carte d'identité existe en Italie, elle n'est, en revanche, pas obligatoire. Assez peu utilisée, les Italiens lui préfèrent le passeport, le permis de conduire ou même le permis de chasse. Les nouvelles cartes délivrées seront, comme dans les autres pays européens, des cartes électroniques.

«Fake ID». La Grande-Bretagne possède peut-être un quart des caméras de sécurité du monde, mais personne ni détient de carte d'identité. Le passeport, le permis de conduire ou pratiquement n'importe quelle carte munie d'une photo peut-être utilisée pour prouver son identité, avec plus ou moins de rigueur selon la situation. Ainsi beaucoup de jeunes peuvent facilement se procurer des *«fake ID»* (faux papiers d'identité) pour rentrer dans les bars interdits aux moins de 18 ans. Un projet de loi est cependant en cours, ainsi qu'une étude auprès de la population pour introduire la fameuse carte électronique. La carte d'identité restera cependant facultative, ou limitée à certains groupes tel que les nouveaux immigrants, et ne sera pas créée avant 2012. ◂▸

MÉLANIE GOUBY
avec les correspondants étrangers

Pierre Piazza, professeur de sciences politiques, revient sur l'histoire des papiers d'identité :

«Une carte d'inspiration policière»

Pierre Piazza est maître de conférences en sciences politiques à l'université de Cergy-Pontoise. Spécialiste des questions d'identification, il est l'auteur d'une *Histoire de la carte nationale d'identité* (Odile Jacob, 2004).

Comment en est-on arrivé à cette idée de carte nationale d'identité pour justifier de sa nationalité?

Au départ, la carte est d'inspiration purement policière. Elle procède d'une volonté d'identification et descend en droite ligne des techniques d'Alphonse Bertillon, commis à la préfecture de police de Paris qui participera à la mise en place en 1912 de carnets anthropométriques pour les nomades. La césure, c'est vraiment la IIIe République avec l'avènement de l'Etat-nation. Avant, il existait bien des documents prouvant l'identité comme le passeport intérieur ou le livret ouvrier, mais ils n'étaient pas vraiment fiables. A partir des années 1870-80, la question de la nationalité prend de plus en plus d'importance. On commence à vouloir distinguer les Français des étrangers qui étaient munis d'une carte d'identité depuis 1916. En 1921 naît ainsi la première véritable «Carte d'identité de Français», instaurée pour le seul département de la Seine à l'initiative du préfet de police Robert Leullier. Dès lors, la carte matérialise une appartenance commune à un même corps, la nation.


Pierre Piazza.

Sous couvert d'être un symbole d'intégration, la carte n'est-elle pas aussi un instrument de contrôle?

Ces deux problématiques sont en effet intimement mêlées: d'un côté, la carte atteste d'une appartenance légitime à un corps social national. Mais de l'autre, elle a un aspect répressif lié à l'usage que la police peut faire des données contenues par la carte. Ces deux aspects n'ont d'ailleurs pas cessé de ressurgir au cours de l'histoire. En 1955, dans un souci de rupture avec le fichage de Vichy, un décret rend notamment la carte facultative. Le discours officiel est d'en faire un outil d'intégration, mais officieusement, on s'en sert au même moment pour contrôler les Français musulmans d'Algérie. Plus récemment, en 1993, l'Etat a profité du passage à la nouvelle carte informatisée, dite «carte Pasqua» pour durcir notamment les contrôles à l'égard des Français nés à l'étranger ou de parents étrangers. En considérant que le passage de la carte papier à la nouvelle était équivalent à une première demande de carte, l'Etat a mis beaucoup de citoyens français dans l'obligation de prouver leur nationalité. On a ainsi jeté l'opprobre sur de nombreux Français qui se sont sentis considérés comme des citoyens de seconde zone.

Comment expliquer le succès de cette carte alors qu'elle n'est pas obligatoire?

C'est en effet un peu paradoxal. C'est d'autant plus étonnant que cet objet n'a pas franchement une histoire démocratique. Car jamais aucune carte n'a été discutée devant le Parlement. Depuis la première, elles sont toutes le fait de décrets ou de directives émanant soit de la préfecture de police, soit du ministère de l'Intérieur. Seule exception, le projet de carte d'identité biométrique porté depuis 2002 par Nicolas Sarkozy et gelé en 2005 après un débat porté sur la place publique. C'était d'ailleurs un des rares projets à vouloir rendre la carte d'identité obligatoire. Malgré cet aspect non démocratique, la carte est aujourd'hui totalement rentrée dans les mœurs.

Beaucoup de gens pensent même qu'elle est obligatoire. Certains apprécient son aspect pratique, d'autres estiment qu'elle valide une appartenance à la nation et qu'elle est un gage de respectabilité. Mais cette adhésion s'explique aussi par tous les discours de persuasion que les pouvoirs publics ont mis en place pour rendre populaire cette carte. Comme en 1993: pour le passage à la carte informatisée, l'Etat avait lancé de grandes campagnes de communication pour vanter les mérites d'une carte dite infalsifiable. Qu'il veut pourtant à nouveau remplacer. ◂▸

recueilli par CHRISTOPHE LEHOUSSE

«LIBÉRATION»