

**Université de Droit Paris I Panthéon – Sorbonne
12, Place du Panthéon
75005 PARIS**

UFR 01

**MASTER 2 – DROIT DE L’INTERNET – ADMINISTRATION –
ENTREPRISES**



MEMOIRE

La protection de la donnée biométrique

Présenté et soutenu par

Alban REBRION

Président du jury

Monsieur le Professeur Georges CHATILLON, Directeur du Master

Membres du jury

Monsieur le Professeur Georges CHATILLON, Directeur du mémoire
Maître Garance Mathias, Maître de stage (Avocat à la Cour)

REMERCIEMENTS

Je tiens tout d'abord à remercier monsieur Georges CHATILLON, mon directeur de mémoire, mais également le directeur du Master, pour m'avoir donné la chance de suivre cette formation universitaire.

Je tiens à remercier ma famille et mes amis, qui ont toujours été près de moi dans les moments difficiles. Je dédie une pensée toute particulière à mon oncle Gilles COULANJON, docteur en gastro-entérologie, qui nous a quitté le 10 avril 2006, et à ma grand-mère Simone REBRION, la meilleure mamie qu'on peut espérer avoir, qui nous a quitté le 12 juin 2006. Tous deux auront combattu la maladie, sans jamais faillir.

Enfin, je n'oublie pas Claire FROITZHEIM, qui par sa présence fait que tout est toujours meilleur.

PLAN DETAILLE

REMERCIEMENTS	2
PLAN DETAILLE	3
INTRODUCTION	4
TITRE PREMIER. LE DEVELOPPEMENT DE LA BIOMETRIE : VERS UNE CRIMINALISATION DE LA SOCIETE	9
<i>Chapitre Premier : La mise en place de l'identité biométrique par les autorités nationales</i>	10
Section Première : Historique de la technique d'identification	10
Section deuxième : Les motivations de l'utilisation de ce procédé extrême ..	21
<i>Chapitre deuxième : La pertinence de la solution biométrique : l'arbre qui cache la forêt</i>	29
Section première : La remise en cause de l'utilité d'un tel système d'identification	29
Section seconde : Vers un nouveau partage de pouvoirs au profit des entreprises	39
TITRE DEUXIEME. L'URGENCE ET LA NECESSITE D'UNE PROTECTION PARTICULIERE	47
<i>Chapitre premier : L'adoption d'un corpus législatif : la délicate question du niveau de protection</i>	48
Section première : Une lente construction dans un souci de protection	48
Section seconde : Les limites de la législation actuelle : une protection amoindrie	57
<i>Chapitre deuxième : La perfectibilité d'une législation appliquée par une pluralité d'acteurs</i>	64
Section première : Une utilisation de la biométrie sous le contrôle d'institutions nationales	64
Section seconde. Les solutions pour un meilleur encadrement de la biométrie	75
CONCLUSION	81
BIBLIOGRAPHIE	83

INTRODUCTION

La biométrie est-elle la technologie du futur ? Dans certains films de science-fiction¹, la place laissée à la biométrie est importante, et ce en dehors de toute application judiciaire². Mais il semblerait que nous ayons rattrapé le futur.

Le terme « biométrie » regroupe aujourd'hui les procédés techniques d'identification basés sur des caractères biologiques de la personne. Ce terme aurait été introduit dans le vocabulaire scientifique à la fin du XIX^{ème} siècle sous la forme anglo-saxonne de « biometry » puis « biometrics ». ³ Remarquons que le terme français « anthropométrie »⁴ apparaît comme une traduction plus fidèle des termes anglais susvisés.

Pris dans son sens le plus commun, la biométrie désigne « l'application des méthodes mathématiques, statistiques notamment à la description, à l'inventaire et à l'analyse des données biologiques ». ⁵ En résumé, la biométrie désigne une méthode scientifique d'évaluation, de mesure et de traitement des caractéristiques physiques, biologiques ou comportementales d'une personne, méthode utilisée dans l'anthropométrie.

A l'heure actuelle, les éléments mesurables par une machine sont regroupés en deux catégories⁶. D'une part, nous avons les techniques de reconnaissance anatomique (ou caractéristiques statiques⁷), qui regroupent l'empreinte digitale⁸, la géométrie de la main, la reconnaissance par l'iris⁹, la rétine¹⁰, la reconnaissance faciale¹¹, et enfin l'ADN¹², et d'autre part les techniques reconnaissance dynamique, à savoir la reconnaissance vocale et l'écriture

¹ Bienvenue à Gattaca (Film d'Andrew NICCOL, 1998) et Minority Report (Film de Steven SPIELBERG ; 2003)

² Dans « Bienvenue à Gattaca », l'accès aux bâtiments donne lieu à une identification de la personne grâce à une goutte de sang.

Dans « Minority Report », l'identification des individus se fait par l'iris. Pour échapper aux nombreux capteurs (fixes ou bien mobiles, tels les petits robots), Tom CRUISE subit une douloureuse opération pour changer ses yeux. A n'importe quel moment, les individus sont reconnus par les capteurs. Par exemple, dès qu'il rentre dans un magasin, le personnage interprété par Tom CRUISE est immédiatement reconnu et accueilli par une phrase personnalisée à son nom.

³ Daniel GUINIER ; « Biométrie : classification au vu des nouveaux motifs » ; *Expertises* ; février 2005 ; pages 62 à 68 ; page 62, note 3.

⁴ Cf. infra Titre1, Chapitre 1, section 1, §2, A/.

⁵ *Encyclopédie BORDAS* ; page 655.

⁶ Distinction opérée dans le rapport du député CABAL. CABAL, Christian. Rapport « Méthodes scientifiques d'identification des personnes à partir des données biométriques ». Rapport n° 958, déposé à l'Assemblée Nationale le 16 juin 2006. Disponible sur le site internet de l'Assemblée Nationale : <http://www.assemblee-nationale.fr/12/rap-oecest/i0938.asp>

⁷ Daniel GUINIER ; « Biométrie : classification au vu des nouveaux motifs » ; *Expertises* ; février 2005 ; pages 62 à 68.

⁸ Empreinte d'une partie de la main.

⁹ La partie externe avant de l'œil

¹⁰ Le fond de l'œil

¹¹ Largeur de la mâchoire, du front etc.

¹² Acide DésoxyriboNucléique

dynamique¹³. Chacune de ces caractéristiques présente un niveau d'efficacité, en terme d'identification, différent dans la mesure où les risques de confusion entre divers sujets sont plus ou moins probables. La reconnaissance par l'ADN se voit attribuer une meilleure efficacité que la reconnaissance vocale, car un ADN correspond à une seule et unique personne, sauf dans le cas de jumeaux.

Mais chaque élément du corps humain, chaque geste n'est pas forcément mesurable par la biométrie. Tous les éléments biométriques ont en commun plusieurs caractéristiques.

- L'universalité : l'élément biométrique doit exister chez toutes les personnes.
- L'unicité : l'élément biométrique doit être distinct d'une personne à une autre. À cet égard, tous les éléments biométriques ne sont pas équivalents et le taux de discrimination d'une personne à une autre est très différent selon la biométrie en cause. La reconnaissance par l'ADN se voit attribuer une meilleure efficacité que la reconnaissance vocale.
- La permanence : la propriété du biométrique doit rester permanente dans le temps pour chaque personne.
- L'accessibilité et la quantifiabilité : l'élément biométrique doit être collectable et mesurable afin de pouvoir être comparé.

L'intérêt du développement actuel de la biométrie réside dans les facilités, les commodités d'usage de cette technique, face au problème récurrent de l'identification des personnes. Une journée de travail est rythmée par l'utilisation d'appareils nécessitant tous une identification, et pour certains une authentification¹⁴ : le digicode de l'immeuble, le login et le mot de passe pour démarrer l'ordinateur au bureau, le code PIN de la carte bancaire... L'identification consiste à déclarer son identité, l'authentification va plus loin puisqu'elle consiste à prouver l'identité. La biométrie permet en effet non seulement d'identifier une personne mais aussi de prouver que la personne qui se présente est bien titulaire de cette identité. Il n'y a qu'un pas à franchir, et il a été franchi, pour que le corps humain devienne un mot de passe.

Toutes ces facilités ont été rendues possible avec le développement de l'informatique. La biométrie n'a plus rien à voir avec la biométrie des débuts, quand il fallait comparer une empreinte digitale avec les milliers d'empreintes contenues dans un fichier de police. Grâce à l'informatique, la biométrie évolue radicalement. Elle devient désormais la technique permettant d'acquérir une donnée brute (caractéristiques physique ou comportementale) et de la traduire en une empreinte numérique, en une donnée numérique. Une donnée numérique est la représentation d'une information sous une forme conventionnelle (codage en système binaire) destinée à faciliter son traitement¹⁵. L'informatique permet également un stockage de ces données permettant de comparer la donnée brute saisie (par un capteur, ou lecteur) aux données préalablement enregistrées.

Mais il ne faut pas oublier que le développement de l'informatique a connu des débuts difficiles, notamment avec l'affaire SAFARI. Le développement de l'informatique a créé des facilités nouvelles de stocker, traiter, diffuser et échanger des données personnelles. Dans les années 70, la crainte d'un fichage général de la population se posait essentiellement par rapport aux fichiers des administrations, et il se trouve qu'en 1974, le gouvernement a eu le

¹³ La dynamique du tracé étant ainsi mesurable comme la dynamique des frappes sur un clavier.

¹⁴ Méthode qui dans un contexte autre que le contexte biométrique consiste à utiliser une double-clé identifiant/mot de passe afin de pouvoir accéder à l'information protégée.

¹⁵ Définition disponible sur internet : <http://www.celog.fr/silex/tome1/termino1.htm#def43>

projet d'identifier chaque citoyen par un numéro et d'interconnecter sur la base de cet identifiant tous les fichiers publics.

A partir de cette affaire, l'opinion publique, les médias et les milieux politiques ont pris conscience des dangers qui pouvaient découler de certaines utilisations de l'informatique. De là est née la loi du 6 janvier 1978¹⁶ (modifiée le 6 août 2004) relative à l'informatique, aux fichiers et aux libertés. Depuis presque trente ans s'est développé un droit à la protection des données à caractère personnel qui font l'objet d'un traitement automatisé d'informations.

Dès le départ, le législateur semble avoir voulu protéger largement et efficacement les droits et libertés individuelles, conscient des dangers et des risques qui découlent de l'usage de l'informatique. D'une part, l'article 1^{er} de la loi dispose que: « l'informatique doit être au service du citoyen, elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques ». D'autre part le législateur a confié à une autorité administrative indépendante la tâche de veiller au respect des dispositions de la loi. Cette autorité a été dénommée la Commission Nationale de l'Informatique et des Libertés (ci-après la CNIL).

La loi « Informatique et Libertés » a été réformée par une loi du 6 août 2004¹⁷. Le principal apport de cette modification réside dans l'allègement de certaines obligations notamment en matière de déclaration des traitements d'informations. En contrepartie, la loi est venue renforcer les pouvoirs d'investigation et de sanction de la CNIL.

La nouvelle rédaction de la loi instaure la protection des données à caractère personnelle, notion plus large que celle de données nominatives. La donnée à caractère personnelle est définie par le deuxième article de la loi comme « 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. 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 ».

Une donnée à caractère personnel bénéficie de la protection mise en place par la loi dans la mesure où elle fait l'objet d'un traitement (automatisé ou non), c'est-à-dire qu'elle fait l'objet d'une « opération ou tout ensemble d'opérations [...], quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction »¹⁸.

Tous les fichiers informatisés qui appréhendent l'identité de la personne humaine font ainsi l'objet d'une analyse par la CNIL. Et les fichiers de ce type ne manquent pas, qu'ils

16 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 ; JORF du 7 août 2004 ; Disponible sur internet :

<http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm>

Pour une plus grande facilité de lecture, nous attirons l'attention du lecteur sur l'existence d'une version de la loi annotée et consolidée, disponible sur le site de la Commission Nationale de l'Informatique et des Libertés :

http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf

Ci-après la loi « Informatique et Libertés »

¹⁷ Loi n° 2004-801 du 6 août 2004

¹⁸ Article 2 al3 de la loi « Informatique et Libertés » précitée

soient entre les mains et utilisés par des organismes publics¹⁹ ou par les services de la police nationale ou de la gendarmerie dans le cadre de leur mission.²⁰ Mais le développement de la biométrie ne concerne pas exclusivement que les pouvoirs publics. Des entreprises mettent en place des solutions biométriques pour contrôler l'accès à certains locaux, et sont par conséquent amenés à traiter des fichiers qui appréhendent l'identité de la personne humaine.

Le développement, ainsi que la banalisation, de la biométrie entraîne donc une multiplication des fichiers contenant des données biométriques, fichiers détenus par les pouvoirs publics, les employeurs, ou bien par les individus eux-mêmes. Mais cette multiplication de ces données va à l'encontre même d'un principe sacré en matière d'informatique : la minimisation des données. Selon l'adage, on ne peut sécuriser que ce qu'on tient dans la main (dans la pratique, un informaticien ne peut sécuriser que ce qu'il peut effectivement contrôler lui-même). Puisque les données vont être amenées à transiter un réseau, la force de ce réseau tiendra à la force de son maillon le plus faible. On dehors de tout échange, une même donnée pourra se retrouver dans plusieurs systèmes informatiques différents, détenus par des personnes différentes. Il suffira pour une personne mal intentionnée d'identifier le système le moins protégé et de l'attaquer.

Une étape a été franchie avec l'annonce du projet INES (Identité Nationale Electronique Sécurisée). Ce projet vient du besoin accru des Etats d'identifier de manière certaine les individus présents sur son territoire. Ce besoin de contrôle des individus n'est évidemment pas sans rapport avec le contexte international. L'attaque du World Trade Center le 11 septembre 2001 mais aussi la vague d'attentats qui a frappé et frappe encore l'Europe avec force²¹ ont accru le désir de sécurité. Une sécurité au service de laquelle semblent se mettre les nouvelles possibilités d'identification humaine combinées aux systèmes informatiques.

Le mot « sécurité » est lâché. Les aspects attrayants de la biométrie passent au second plan. Mais dans cette course à l'équipement biométrique utilisé à des fins sécuritaires l'on ne peut que s'inquiéter de voir la liberté des individus réduite. En effet l'identification humaine devient un outil stratégique important dans la lutte contre la criminalité en permettant d'identifier des individus ayant porté ou soupçonnés de vouloir porter atteinte à l'ordre public. Mais l'utilisation de la biométrie à des fins sécuritaires par l'Etat est troublante dans la mesure où elle est combinée à l'identité civile²² de tous les individus.

La biométrie crée alors un lien unique et perpétuel entre les caractéristiques biométriques d'une personne, caractéristiques qui sont numérisées et conservées, et des informations relatives à cette personne, qui permettent de l'identifier directement ou indirectement.

¹⁹ Cf. Répertoire National d'Identification des Personnes Physiques (RNIPP) dont l'Institut National de la Statistique et des Etudes Economiques (INSSE) est responsable et qui est utilisé par les organismes de sécurité sociale ou l'administration fiscale. Ce fichier permet de préciser si une personne est décédée ou non et de connaître son Numéro d'Inscription au Répertoire (NIR). <http://www.cnil.fr/index.php?1804>

²⁰ Quelques exemples connus : FAED (Fichier Automatisé des Empreintes Digitales) ; FNAEG (Fichier National Automatisé des Empreintes Génétiques) ; ou bien encore STIC (Système de Traitement des Infractions Constatées).

²¹ Attentat à la station parisienne de RER Saint-Michel en 1995, ceux de Madrid en mars 2004, de Londres en juillet 2005 et récemment au mois d'août 2006.

²² Cf. infra Titre1, Chapitre 1, section 1, §1

La question récurrente de notre sujet est donc de savoir en quoi la biométrie nécessiterait-elle une protection particulière ? Pouvons-nous nous contenter d'un traitement commun à toutes les données à caractère personnel, quelque soit leur nature ?

La réponse ne peut être que négative. Il ne faut pas oublier ce pourquoi la biométrie a été développée, sa finalité première. Et nous ne pouvons que rester sceptique face à son application dans les titres d'identité. Le rapprochement entre la biométrie et la vie quotidienne en société nous amène à croire que nous sommes tous des criminels en puissance, que la société est criminelle (Titre Premier). Face à ces idées, à ces projets, il est urgent et nécessaire d'instaurer des garde-fous afin d'éviter des dérives aux conséquences gravissimes (Titre second)

TITRE PREMIER. LE DEVELOPPEMENT DE LA BIOMETRIE : VERS UNE CRIMINALISATION DE LA SOCIETE

Depuis les trente dernières années, la nature des données collectées par les différentes entités (publiques ou privées) a changé : aux données objectives telles que l'état civil, l'adresse ou le numéro de sécurité sociale, s'ajoutent des données subjectives de traitement. Sont apparus des traitements retraçant les capacités, les comportements, les habitudes ou les goûts.

De nouvelles formes de traitements apparaissent, permettant de dresser un profil des personnes fichées en fonction de la finalité à atteindre. Face à la multiplication des attentats depuis le début de ce millénaire, les Etats ont rapidement compris cette évolution et s'en sont emparés. Les éléments d'identification jouent alors un rôle privilégié dans cette logique sécuritaire.

Les attentats du 11 septembre 2001 aux Etats-Unis ont remis en cause la sécurité aérienne, le premier réflexe a donc été d'essayer de trouver le moyen d'identifier les futurs terroristes au moyen d'informations personnelles sur les passagers. Par ailleurs, l'importance de connaître l'identité réelle des passagers, et au-delà des citoyens, a fait naître dans l'esprit des autorités nationales un besoin de créer des titres d'identité plus sécurisés.

La tendance aux titres d'identité infalsifiables est lancée²³. La biométrie est apparue comme le moyen idéal d'identification, et c'est pourquoi les autorités nationales ont décidé de la mise en place de nouvelles cartes d'identité, qui seront dotées de puces électroniques renfermant toute une série d'informations sur leur titulaire, et notamment des données biométriques. Notre société entre maintenant dans l'ère de l'identité numérique (Chapitre Premier).

Mais face aux efforts mis en œuvre par les autorités nationales pour faire accepter cette méthode d'identification, nous nous devons de rester attentifs. Le produit qu'on nous présente est attirant, mais il ne s'agit pas de foncer tête baissée. Nous devons nous interroger sur la pertinence de la solution biométrique, et essayer de voir la forêt qui se cache derrière l'arbre (Chapitre Second).

²³ Bien que cette tendance soit récurrente : en 1996, la nouvelle carte était déjà présentée comme infalsifiable.

Chapitre Premier : La mise en place de l'identité biométrique par les autorités nationales

Il n'aura échapper à personne que les procédés d'identification biométriques ont été développés juste après les attentats du 11 septembre. Mais cette croisade anti-terroriste n'est qu'une justification parmi d'autres (Section seconde).

Les Etats ne jurent plus que par la biométrie pour identifier les individus sur leurs territoires. Mais ce moyen d'identification s'est substitué à d'autres moyens qui auraient montré leurs limites. Il est donc nécessaire de s'intéresser à l'historique de la technique d'identification (Section première) pour mieux comprendre le raisonnement qui a conduit à mettre en place l'identité biométrique.

Section Première : Historique de la technique d'identification

Depuis toujours, l'Homme a eu besoin de nommer les choses, et par le terme « chose » nous entendons également les êtres humains. Des méthodes, des moyens d'identification ont alors été imaginés afin d'individualiser les membres d'une société, dans un but non judiciaire. L'identité civile s'est donc développée en premier lieu (Paragraphe premier).

Depuis plus d'un siècle, l'identification judiciaire des individus a fait un bond en avant, et ce grâce aux progrès de la science, et en particulier de la biométrie. Ainsi cette technique est liée depuis le départ à l'identification judiciaire (Paragraphe second).

Dès lors, la biométrie, bien que liée à l'identification judiciaire, se trouve appliquée à l'identification civile. La biométrie, qui est à l'origine une science, entre donc désormais dans la définition même de l'identité.

Paragraphe Premier : Identité civile et identification

L'identité civile, telle que nous la connaissons aujourd'hui, résulte d'un long processus, que nous décrirons dans un premier temps (A.). Un individu est reconnu aux yeux des autres selon des critères précis.

L'individu peut communiquer son identité à d'autres individus. Dès lors il s'identifie auprès d'eux. Le droit à encadrer cette communication afin d'élaborer une liste des éléments identifiants à communiquer, et cette communication prend le nom d'identification (B.).

Mais il semblerait que l'identification des individus souffre de problème tels que seule la biométrie pourrait en être le remède. Mais l'identité biométrique est-elle la source d'une meilleure identification (C.) ?

A. La lente construction de la notion l'identité civile

Il est tout d'abord important de s'arrêter sur la précision de la notion d'identité avant de poursuivre plus en avant sur la notion d'identité civile.

La racine latine du terme « Identité » est « *identitas* », qui découle de « *idem* », qu'on traduit par « le même ». Dans le vocabulaire juridique de Monsieur CORNU²⁴, le terme « identité » comprend deux notions distinctes, à savoir l'identité pour une personne physique et l'identité pour un objet. Cette dernière correspond à la racine latine, puisque les synonymes employés sont « Similitude » et « Unité »²⁵.

- Pour ce qui est de la similitude, l'identité de deux objets est ce qui fait qu'ils se ressemblent.
- Pour l'unité, l'identité entre deux éléments est ce qui fait qu'ils n'en font qu'un seul et même.

L'identité de deux objets suppose dès lors des points communs entre ces deux objets.

Mais appliquée à la personne, la notion d'identité prend un tout autre sens : elle est désormais source d'unicité, d'individualisation. Selon Monsieur CORNU, l'identité pour une personne physique est « ce qui fait qu'une personne est elle-même et non une autre ; par extension ce qui permet de la reconnaître et de la distinguer des autres ; l'individualité de chacun, par extension, l'ensemble des caractères qui permettent de l'identifier ».

Par conséquent, l'identité d'une personne comprend les différents éléments qui lui sont propres et qui permettent de la distinguer des autres, et non plus de la rapprocher au point de la confondre, comme le voudrait le sens étymologique du terme « Identité ». Dès maintenant, nous pouvons faire un rapprochement avec la biométrie, dans la mesure où elle permet d'identifier des personnes à partir de mesures corporelles qui sont propres à chaque personne.

L'identité biologique est le fondement de toute identité, puisque le premier critère de distinction était le sexe des individus. Dès la naissance, et même avant avec l'échographie, l'individu est classé d'emblée d'un côté ou de l'autre de la dichotomie opérée par la nature.

Mais à cette identité biologique, très limitée, est venue se superposer l'identité civile des individus. Le développement des rapports sociaux nécessitait plus qu'une simple distinction selon le sexe des individus.

Dès lors, différents signes ont été inventés pour préciser au mieux l'identité d'une personne, afin de ne pas la confondre avec une autre, et par extension pour mieux la situer par rapport à d'autres. Les différents éléments objectifs que nous pouvons citer sont le nom et le prénom, ainsi que la filiation. Ces éléments étaient créés lors d'événements religieux (baptême, mariage ...), puisque c'était l'Eglise qui gérait les différents registres de l'état des personnes. D'autres éléments s'attachant plus aux particularités physiques ou comportementales étaient aussi utilisés.

A travers cette notion d'état des personnes a été recherchée une certaine stabilité dans la manière d'attribuer une identité à une personne, de dégager les différents éléments qui lui sont propres.

²⁴ CORNU Gérard ; *Vocabulaire juridique* ; Editions Presse Universitaire de France ; Collection Quadrige Dicos Poche ; 7^{ème} édition ; Paris 2005 ; 970 pages ; page 453.

²⁵ CORNU Gérard ; *Vocabulaire juridique* ; Editions Presse Universitaire de France ; Collection Quadrige Dicos Poche ; 7^{ème} édition ; Paris 2005 ; 970 pages ; page 453.

La laïcisation progressive de l'état civil, après la Révolution de 1789 et avec le Code Napoléon de 1804, n'a pas totalement rompu avec cette logique. Les événements religieux ont été abandonnés au profit d'autres événements, tels que la naissance. La supériorité du mariage civil sur le mariage religieux a été clairement énoncée.

La loi civile a donc imposée les différents éléments de l'identité civile, qui est définie par Monsieur CORNU comme « l'ensemble des éléments qui, [...], concourent à l'identification d'une personne physique (dans la société au regard de l'état civil) : nom, prénom, date de naissance, filiation etc. »

Ces différents éléments sont déterminés pour la première fois lors de la naissance de la personne. Ils sont exprimés dans l'acte de naissance, qui devient un véritable titre fondateur. Nous verrons que la délivrance d'une carte nationale d'identité ne se fait que sur présentation d'une copie de cet acte de naissance. A ce stade de notre étude, il nous faut bien identifier les différentes informations contenues dans ce titre²⁶ :

La rédaction de ce titre fondateur est alors un processus par lequel l'individu se voit reconnaître son identité civile, selon des caractères précis définis par l'Etat, le groupe auquel il appartient. La reconnaissance de l'identité civile est donc la toute première relation entre l'Etat et l'individu. Ce titre fondateur est appelé à ne jamais évoluer, sauf cas exceptionnels²⁷, et l'individu le conservera jusqu'à sa mort.

Mais ce processus de reconnaissance de l'identité ne s'intéresse aucunement à l'identité biologique de l'individu, mis à part bien sûr son sexe. Autrement dit, l'individu est reconnu selon des éléments objectifs non corporels, entendons par là que les différents éléments biométriques n'ont aucune incidence sur la reconnaissance de l'identité. Le titre fondateur ne contient aucun élément biométrique.

B. L'identification des individus

Selon Monsieur CAPRIOLI²⁸, « identifier consiste à exprimer l'identité d'une personne ». Nous sommes donc dans une seconde étape, postérieure au processus de reconnaissance de l'identité d'une personne. A partir d'éléments extrinsèques, il est possible de retrouver l'identité qui a été conférée à une personne. Cette même personne peut déclarer son identité en énonçant ces différents éléments.

Nous venons de voir que le régime d'attribution de l'identité est mis en place par le droit civil²⁹, mais pour ce qui est du problème de l'identification d'une personne, il faut se retourner vers le droit administratif. Monsieur PIAZZA, dans sa contribution sur le projet de la carte nationale d'identité électronique³⁰, reprend l'historique de notre carte nationale d'identité.

²⁶ Article 34 du Code Civil

²⁷ Nous pouvons citer comme exemple le changement de nom, le changement de sexe ... La femme mariée conservera son nom de jeune fille, le nom de son mari étant apposé en marge de l'acte de naissance.

²⁸ Avocat à la Cour de Paris

²⁹ Cf supra Titre 1, Chapitre 1, Section 1, §1, A.

³⁰ Contribution de Monsieur PIAZZA au débat sur la Carte Nationale d'Identité Electronique (CNIE), disponible sur le site internet du Forum sur les Droits de l'Internet (FDI) : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnief.pdf> ; page 3 et suivantes.

L'instauration de cette carte d'identité par les pouvoirs publics était conçue comme « le moyen de rompre avec des modes traditionnels de reconnaissance considérés comme inefficients ». Il cite alors la preuve par témoins patentés, formalité réclamée pour toute démarche administrative, mais qui a donné lieu à de très nombreux abus. Cette formalité remonte au Moyen Age, où l'identité n'était qu'une « rumeur » faisant consensus³¹. L'identité d'une personne était attestée par sa famille ou des proches.

En presque un siècle d'existence, la carte nationale d'identité a pris plusieurs formes afin de suivre les évolutions de la société. Elle a été fiabilisée au fil du temps pour déjouer les faussaires. Sa procédure d'attribution a été renforcée, et ce parfois au détriment de certains individus.

La carte nationale d'identité fait partie des différents papiers d'identité, dont nous retiendrons comme définition celle de Monsieur CORNU, c'est-à-dire un « document écrit (généralement une carte) qui énonce et atteste l'identité civile d'une personne physique »³².

Le papier d'identité devient donc l'instrument qui permet à une personne de prouver son identité³³ à tout moment, en toute occasion puisqu'elle le détiendra sur elle. Ce papier pourra revêtir plusieurs formes : carte nationale d'identité, mais également passeport, permis de conduire ...

Malheureusement, des faussaires viennent rompre le lien entre ces papiers d'identité et l'identité civile des personnes telle que reconnue par l'Etat dans leur état civil. Aujourd'hui, il existe des « vrais faux papiers », ce qui démontre une faille dans le procédé de distribution de ces papiers, mais également dans le processus d'identification.

Face à de tels comportements, il est évident que l'authenticité du papier d'identité n'est plus ce qui est recherché. La simple présentation du papier d'identité, aussi conforme soit-il, apparaît insuffisante pour rattacher la personne à son identité. Il nous faut donc passer à une troisième étape, qui consiste pour la personne qui détient le papier d'identité en question, de prouver qu'elle en est le véritable porteur.

C'est dans l'optique de ce troisième processus que plusieurs Etats ont eu l'idée de conférer à l'identité un fondement biologique.

C. L'identité biométrique : source d'une meilleure identification ?

Le projet INES pour Identité Nationale Electronique Sécurisée³⁴ modifiera la façon d'obtenir une carte nationale d'identité, qui sera désormais électronique.

Cette nouvelle carte aura le format d'une carte bancaire, et seront écrites dessus les mêmes informations qui figurent sur les cartes d'identité actuelles. La différence tiendra dans

³¹ 22^{ème} rapport d'activité : 2001 ; Paris ; La Documentation française ; 2002 ; 352 pages ; page 97. Disponible sur internet : <http://lesrapports.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf>

³² CORNU Gérard ; *Vocabulaire juridique* ; Editions Presse Universitaire de France ; Collection Quadrige Dicos Poche ; 7^{ème} édition ; Paris 2005 ; 970 pages ; page 453.

³³ Présuimée jusqu'à preuve du contraire. « Identité : ensemble des composantes grâce auxquelles il est établi qu'une personne est bien celle qui se dit ou que l'on présume telle (nom ; prénom ; nationalité ; filiation) ». Cf. *Lexique des termes juridiques* ; Dalloz ; 1999, page 275.

³⁴ Nous renvoyons le lecteur à la présentation du projet INES publié sur le site du FDI : <http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf>

le fait que cette nouvelle carte comportera une puce électronique. Sur cette puce seront enregistrées différents éléments, dont la photographie numérisée de l'individu ainsi que deux empreintes digitales numérisées.

Dans le projet, il est prévu que ces deux éléments ne seront accessibles qu'aux « seules autorités habilitées ». Il faut entendre par là les services de police.

Un tel projet est la démonstration implicite de la préoccupation de l'Etat pour les failles de son dispositif d'identification des individus. C'est la reconnaissance que le risque de fausse identité est devenu trop important, et en conséquence inacceptable.

En matière d'identification, les pouvoirs publics semblent avoir décidé de ne plus supporter aucun risque de se tromper ou du moins de réduire la marge d'incertitude. La volonté de réduire cette marge d'incertitude est légitime pour les Etats à l'heure du développement constant des facilités de transports, et donc de la croissance des flux migratoires.

Selon Monsieur TRUDEL³⁵, l'identification est « un processus destiné à réduire l'incertitude. Il vise à procurer la quantité optimale d'information à l'égard d'une personne afin de pouvoir procéder à la transmission avec un niveau de risque acceptable ». Il poursuit en déclarant qu'il « sera parfois nécessaire d'avoir recours à des mécanismes de validation ou de corroboration des informations pouvant permettre d'accroître le degré de certitude à l'égard de l'identité d'une personne ». La finalité de l'identification serait donc de réduire l'incertitude.

Il est vrai que les procédés biométriques d'identification répondent mieux à la définition de l'identité. Nous pouvons ainsi imaginer une meilleure individualisation de chaque personne puisque son identité serait fondée sur des caractères qui lui sont intimement liés, et qui sont uniques, contrairement aux éléments objectifs actuels.

Mais la biométrie est-elle la seule solution qui confère à l'identification la stabilité qui semble lui faire de plus en plus défaut au fur et à mesure que la société de l'information se développe ? La réponse à cette question dépend aujourd'hui des choix technologiques qui seront faits par les pouvoirs publics.

Les pouvoirs publics semblent s'être convaincus, ou avoir été convaincus³⁶, de l'efficacité des techniques biométriques en matière d'identification. Désormais, ils tentent de convaincre pour l'instant, avant d'imposer, les citoyens de l'efficacité des méthodes d'identification biométriques et de leurs bienfaits³⁷.

Mais ce faisant, les pouvoirs publics appliquent à l'identité civile des principes élaborés dans le cadre de l'identité judiciaire.

Paragraphe second : L'identification judiciaire

³⁵ Contribution de Monsieur TRUDEL au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cniet.pdf> ; contribution page 66 et s.

³⁶ cf infra Titre 1, Chapitre 2, Section 2.

³⁷ cf infra Titre 1, Chapitre 1, Section 2.

Selon Monsieur CARBONNIER³⁸, « qu'un individu puisse rester sans identité met le droit mal à l'aise », mais ne le rend pas sans effet, surtout en matière pénale. Dans une décision rendue par le tribunal correctionnel du Puy, en date du 11 janvier 1966³⁹, il a été décidé que « lorsque le prévenu à qui doit s'appliquer un jugement se trouve matériellement indiqué par la détention de sa personne, le mystère dont il parvient à s'envelopper, en dissimulant sa véritable identité, ne peut être un motif de le soustraire à la peine qui réprime l'infraction qu'il a commise ».

Les juges, malgré l'absence d'identité civile, ont retenu qu'il n'y avait aucun doute sur l'identité physique de l'individu. L'individu était l'auteur certain de l'infraction. Dès lors, si aucune difficulté ne s'oppose à la condamnation d'un individu « corps présent », la solution est totalement différente en l'absence de l'auteur de l'infraction.

C'est le travail des services de police judiciaire que d'identifier et d'arrêter les délinquants et les criminels. Différentes techniques ont été élaborées afin d'identifier les auteurs d'infraction, et la plus célèbre est la biométrie (A.)

Néanmoins, si ces procédés d'identification biométriques ont été bien accueillis par la population pour identifier des criminels, il en va autrement quand ces mêmes procédés sont destinés à des contrôles d'identité applicables à l'ensemble des personnes civiles, en dehors de toute procédure pénale (B.).

A. La biométrie : une science développée pour la matière pénale

Comme le relève Monsieur GUINIER⁴⁰, « les applications de la biométrie se sont développées dans le cadre judiciaire avec les empreintes digitales et génétiques aux fins d'identification des criminels [...] ».

A la différence de la procédure civile, la procédure pénale admet le principe de la liberté de la preuve⁴¹. La raison essentielle qui commande l'exigence de ce principe est l'intérêt supérieur de la manifestation de la vérité. Face à des coupables qui s'efforcent de cacher leurs méfaits, il est impératif de tout mettre en œuvre pour procéder à leur identification. Dans cette quête de la vérité, la science est venue aider les services de police en élaborant plusieurs techniques scientifiques

Ces différentes techniques avaient donc une seule et unique finalité : l'identification de criminels. Il est très important de garder ceci à l'esprit à l'heure où les gouvernements, mais également les entreprises, et même les cantines scolaires, envisagent d'autres finalités pour ces applications.

A l'origine, le terme biométrie n'était pas employé. La science criminelle intéressant la recherche et l'établissement de preuves est connue sous le nom de criminalistique⁴². Elle

³⁸ CARBONNIER Jean ; *Droit civil Tome 1* ; Editions Presse Universitaire de France ; Collection Quadrige ; 1^{ère} édition, Paris 2004 ; 1496 pages ; page 421

³⁹ Trib. corr. Le Puy, 11 janvier 1966 ; Min. pub. c. N... (cf. J.C.P. 1966, 2, 14803)

⁴⁰ GUINIER Daniel ; « Biométrie : classification au vu des nouveaux motifs » ; *Expertises* ; février 2005 ; pages 62 à 68 ; page 63.

⁴¹ Article 427 du Code de Procédure Pénale : « Hors les cas où la loi en dispose autrement, les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction »

⁴² Créée par le pénaliste autrichien Hans Gros (1847 - 1915)

permet d'établir la matérialité de l'infraction, et souvent la culpabilité ou l'innocence de telle personne soupçonnée. Elle utilise différents moyens, qui sont la police scientifique, la police technique et la psychologie judiciaire⁴³.

La police scientifique a pour objet l'application de diverses sciences exactes et des connaissances médicales à l'administration de la preuve de la culpabilité des auteurs d'infractions. Elle comprend la médecine légale criminelle, l'anthropométrie criminelle et la police scientifique proprement dite.

Tout d'abord utilisées pour l'identification des récidivistes, les mesures des caractéristiques physiques des individus vont devenir une nouvelle méthode d'identification des délinquants et criminels qui va se généraliser et se montrer particulièrement efficace pour les services de police judiciaire.

En 1877, le médecin turinois Cesare LUMBROSO expose ses théories sur le « criminel né » dans l'*Uomo delinquente*. Selon lui, certains traits physiques (front large, yeux très écartés...) seraient en fait les marques d'une aptitude naturelle au crime. Son travail répond aux difficultés que connaît la police dans l'établissement de l'identité judiciaire des malfaiteurs. L'abolition de la marque au fer rouge⁴⁴ des condamnés a permis à ces derniers de dissimuler leur véritable état civil pour échapper aux rigueurs de la loi sanctionnant la récidive.

Pourtant la police parisienne a mis en place un dispositif de fiches pour favoriser l'identification des récidivistes. En 1879 la police disposait d'informations sur plus de cinq millions de personnes⁴⁵. Le principal défaut résultait du classement strictement alphabétique, qui interdisait toute recherche sérieuse à partir d'un signalement.

La reconnaissance des caractéristiques physiques des criminels et des possibilités d'exploitation de celles-ci à des fins d'identification a été progressive. Derrière l'idée farfelue de HUVET⁴⁶, qui consistait à établir une « galerie des perturbateurs de la société » grâce à un « physionotrace » (il s'agissait d'enregistrer la projection donnée par les contours de l'ombre du corps humain), se manifeste le besoin d'ajouter l'image de la personne au signalement écrit. Cette idée va s'imposer d'elle-même avec l'invention de la photographie.

La « photographie signalétique » est ainsi très vite adoptée dans la police française. Les photographies de l'époque sont inexploitablement techniques par les services de l'identité judiciaire. Mais cette expérience est un premier pas vers le portrait robot, lui aussi basé sur la reconnaissance des traits physiques d'une personne.

Il faut attendre l'arrivée d'Alphonse BERTILLON à la préfecture de police en 1879 pour que les techniques d'identification des récidivistes fassent un bond en avant. Fils du docteur Louis-Alphonse BERTILLON, directeur de la statistique à la préfecture de la Seine et cofondateur de l'École d'anthropologie, il s'intéresse rapidement à la mesure du squelette humain. Il entreprend des études de médecine qui s'achèveront rapidement. Néanmoins, sa

⁴³ PRADEL, Jean. *Manuel droit pénal général*. Paris : Editions Cujas, 15^{ème} édition 2004. 756 pages, page 68

⁴⁴ Par une loi du 31 août 1832. Source : DIAZ, Charles. *La police technique et scientifique*. Paris : Editions Presse Universitaire de France, 2000. 127 pages

⁴⁵ Ibidem

⁴⁶ En 1819. Source : DIAZ, Charles. *La police technique et scientifique*. Paris : Editions Presse Universitaire de France, 2000. 127 pages

passion « pour le pied à coulisse » s'en trouve en découvrant les travaux du statisticien belge Quételet, qui affirme qu'il « n'existe pas sur Terre de mensurations de l'ossature humaine complètement identiques pour deux personnes données ».

A partir de cette théorie, Alphonse BERTILLON met à jour un « signalement anthropométrique ». Chaque détenu est identifié grâce à diverses mesures osseuses parmi lesquelles celle de la taille, de l'envergure, de la largeur de la tête, de la coudée, du pied et de l'oreille.

L'anthropométrie est bien l'ancêtre de la biométrie, qui désigne la étude mathématique des variations biologiques au sein d'un groupe déterminé⁴⁷ (physiques, morphologiques, anthropométriques, physiologiques, génétiques ou comportementales).

Face au système anthropométrique de BERTILLON va se développer un autre moyen d'identification plus simple et plus fiable : la dactyloscopie (l'identification par les empreintes digitales). William J. Herschel publie en 1880, dans la revue *Nature*, un article présentant l'empreinte digitale comme caractéristique et qui interdit toute fraude sur l'identité. Cet article passera inaperçu.

En 1888, Sir Francis GALTON reprend les observations de HERSCHEL dans le but d'élaborer un nouveau mode de reconnaissance des récidivistes. Ses études confirmeront l'immuabilité et l'individualité du dessin épidermique.

La technique sera perfectionnée en Argentine en 1891 par Juan VUCETICH⁴⁸, et connaîtra un succès en Europe grâce au préfet de police de Londres, Edward HeENRY⁴⁹, en 1897. BERTILLON décidera rapidement d'inclure dans le signalement des détenus parisiens l'empreinte des doigts de leur main droite. En 1902, BERTILLON réussira la première identification formelle « à distance » d'un criminel, Henri Léon SCHEFFER, déjà fiché par la police pour vol, et dont il relèvera les empreintes digitales dans un appartement cambriolé où a été commis l'assassinat d'un domestique.

Les techniques d'identification des criminels vont encore évoluer jusqu'à la fin du XXème siècle, avec l'utilisation de l'empreinte génétique. Ce procédé a été appelé ainsi en référence à l'empreinte digitale. Les travaux sur l'ADN (acide désoxyribonucléique) ont d'abord trouvé des applications dans le milieu médical avant qu'Alec JEFFREYS⁵⁰ n'en comprenne et détermine toutes les possibilités offertes au plan criminalistique.

Tous ces procédés d'identification humaine ont été bien accueillis par les personnes civiles, puisqu'ils permettent l'identification de récidivistes et de criminels grâce aux traces que ces derniers laissent sur les lieux de l'infraction.

Sans l'outil informatique, tous ces procédés d'identification perdraient de leur intérêt. Tous les éléments recueillis par les services de police ont longtemps été répertoriés dans des fichiers manuels. Ces fichiers étaient cloisonnés géographiquement et fonctionnellement. Face

⁴⁷ BORRICAND, Jacques *et alii*. *Problèmes actuels de sciences criminelles*. Volume XVII. Aix-en-Provence : Presses universitaires d'Aix-Marseille, 2001. 171 pages. Page 46.

⁴⁸ Directeur du bureau de la statistique de la police territoriale de Buenos Aires (1858 - 1925)

⁴⁹ Inspecteur de police générale au Bengale, puis préfet de police de Londres (1850 - 1931)

⁵⁰ Professeur à l'université de Leicester, 1985.

à un grand nombre de fiches (9 millions⁵¹ sur l'ensemble du territoire en 1989), ces différents fichiers interdisent des recherches rapides et exhaustives.

Avec le traitement de ces données par l'informatique, la procédure s'en est retrouvée accélérée et fiabilisée. La France a donc décidé de recourir à l'informatique pour exploiter les données recueillies sur une scène de crime dès 1984⁵² pour les empreintes digitales et en 1998⁵³ pour les empreintes génétiques.

B. Les traitements automatisés d'informations identifiantes mis en place par la Police

Ce n'est qu'à partir des années 70 que les citoyens français ont compris l'importance des fichiers établis et détenus par la police, plus généralement les autorités nationales. En 1974, le ministère de l'Intérieur avait pour projet de mettre à jour un fichier regroupant des millions de fiches de police. Le nom de ce projet était « SAFARI ».

Ce projet n'a jamais abouti. La population a vivement réagi face à cette tentative de « recensement » général, refusant d'être traitée comme un criminel. Les parlementaires ont également réagi ont adopté la loi « Informatique et Libertés » le janvier 1978⁵⁴.

L'actualité des fichiers dits de police s'est en grande partie rapportée au fameux STIC⁵⁵. Néanmoins, au cours des vingt dernières années, ce sont trois fichiers majeurs qui ont été mis en place : le FAED en 1984 (1/), le STIC en 1994 (2/) et le FNAEG en 1998 (3/).

1/ Le Fichier Automatisé des Empreintes Digitales

Le ministre de l'Intérieur, par arrêté du 6 septembre 1984, autorise « la conclusion des marchés nécessaires à l'étude et à la mise au point de matériels et logiciels de saisie et de traitement d'empreintes digitales en vue de leur reconnaissance à partir de points caractéristiques ». C'est l'entreprise Morpho Systèmes qui réalisera le Fichier Automatisé des Empreintes Digitales (FAED)

L'article 3 du décret du 8 avril 1987⁵⁶ dresse la liste des personnes soumises à signalisation au FAED. Peuvent être enregistrées « les empreintes relevées dans le cadre d'une enquête pour crime ou délit flagrant, d'une enquête préliminaire, d'une commission rogatoire ou de l'exécution d'un ordre de recherche délivré par une autorité judiciaire, lorsqu'elles concernent des personnes contre lesquelles des indices graves et concordants de

⁵¹ DIAZ, Charles. *La police technique et scientifique*. Paris : Editions Presse Universitaire de France, 2000. 127 pages. Page 72.

⁵² Arrêté n° du 6 septembre 1984, publié au Journal officiel "Lois et Décrets" du 15/09/1984, page 2921

⁵³ Loi n°98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ainsi qu'à la protection des mineurs ; JORF du 18 juin 1998 ; <http://www.legifrance.gouv.fr/texteconsolide/PJECZ.htm>
Article 706-54 du Code de procédure pénale.

⁵⁴ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 ; JORF du 7 août 2004 ; Disponible sur internet :

<http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm>
http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf

⁵⁵ Système de Traitement des Infractions Constatées

⁵⁶ Décret n° 87-249 du 8 avril 1987, JORF du 9 avril 1987 ; Disponible sur internet :
<http://www.legifrance.gouv.fr/texteconsolide/PPHEP.htm>

nature à motiver leur inculpation auront été réunis, ou des personnes mises en cause dans une procédure pénale, dont l'identification s'avère certaine. »

S'y ajoutent « les empreintes relevée dans les établissements pénitentiaires, en vue de s'assurer de l'identité des détenus qui font l'objet d'une procédure ou crime ou délit et d'établir les cas de récidive ».

Ces dispositions ont été modifiées avec l'adoption de la loi pour la sécurité intérieure⁵⁷ en 2003. L'article 55-1 du Code de procédure pénale dispose que « l'officier de police judiciaire peut procéder, ou faire procéder sous son contrôle, sur toute personne susceptible de fournir des renseignements sur les faits en cause ou sur toute personne à l'encontre de laquelle il existe une ou plusieurs raisons plausibles de soupçonner qu'elle a commis ou tenté de commettre l'infraction, aux opérations de prélèvements externes nécessaires à la réalisation d'examens techniques et scientifiques de comparaison avec les traces et indices prélevés pour les nécessités de l'enquête.

Il procède, ou fait procéder sous son contrôle, aux opérations de relevés signalétiques et notamment de prise d'empreintes digitales, palmaires ou de photographies nécessaires à l'alimentation et à la consultation des fichiers de police selon les règles propres à chacun de ces fichiers. »

Cet article s'applique également dans l'hypothèse d'une enquête préliminaire⁵⁸.

Avec cette rédaction, les victimes comme les simples témoins sont donc traités comme les personnes soupçonnées.

Au 1^{er} janvier 2005⁵⁹, le comptait 1.981.615 empreintes digitales enregistrées et 151.992 traces non identifiées. Ce fichier ne cesse d'être enrichi, puisqu'un décret du 27 mai 2005⁶⁰ permet désormais d'y archiver des clichés anthropométriques ainsi que des empreintes et traces palmaires.

2/ Le Système de Traitement des Infractions Constatées

Ce même problème se retrouve dans le fichier « STIC ». A l'origine, le Système de Traitement de l'Information Criminelle⁶¹ devait recenser toutes les informations relatives aux personnes « mises en cause » dans des procédures judiciaires.

Dans le projet STIC initial, l'intégralité des procès verbaux de la police judiciaire devait y figurer. Il était prévu que ce fichier de police soit consultable par les agents de police mais aussi par les autorités administratives.

Le STIC devait enregistrer et conserver certaines informations :

⁵⁷ Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure. JORF du 19 mars 2003.

<http://www.legifrance.gouv.fr/texteconsolide/PPED1.htm>

⁵⁸ Article 76-2 du Code de Procédure Pénale

⁵⁹ Présentation du projet INES publié sur le site du FDI :

<http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf>

⁶⁰ Décret n° 2005-585 du 27 mai 2005 modifiant le décret n° 87-249 du 8 avril 1987 relatif au fichier automatisé des empreintes digitales géré par le ministère de l'intérieur. JORF du 29 mai 2005.

<http://www.legifrance.gouv.fr/texteconsolide/PRHUV.htm>

⁶¹ Le nom d'origine a été modifié en 1998 en Système de Traitement des Infractions Constatées

- les délits et crimes, ainsi que certaines contraventions de 5^{ème} classe, telles que l'intrusion dans un établissement scolaire ;
- l'identité de la personne (nom, adresse, filiation, nationalité) ;
- le signalement et la photographie de la personne ;
- les faits et les modes opératoires observés pendant la procédure.

La catégorie des personnes « mises en cause » était imprécise, de sorte que l'auteur, la victime et le témoin de l'infraction devait figurer au même titre dans ce fichier. Dès le départ, les problèmes dus à un tel système étaient clairement identifiés. Le traitement rendait suspect toute personne y figurant, quelque soit les raisons qui ont justifié cet enregistrement.

Dans un communiqué du 3 décembre 1998, la Commission Nationale de l'Informatique et des Libertés (CNIL) apportait plusieurs précisions quant :

- au contenu du STIC (aucun témoin ne devant être fiché) ;
- à sa consultation ;
- à la durée de conservation des données ;
- au droit d'accès et de rectification des informations par les personnes concernées.

La CNIL a réitérée sa position dans un communiqué du 25 octobre 2002, après la mise en place du fichier par un décret du 5 juillet 2001.

La CNIL entend exercer son droit de contrôle sur ces fichiers. Elle dispose également d'un pouvoir d'investigation dont les résultats ont été exposés lors de la « conférence de printemps des commissaires à la protection des données » d'avril 2003. Dans son 24^{ème} rapport d'activité pour l'année 2003⁶², la CNIL publie les chiffres relatifs au droit d'accès aux fichiers de police, dont le STIC. Deux ans après son entrée en vigueur, le STIC se voit attribuer une mauvaise note puisque la CNIL a constaté un taux d'erreur de 23 % dans les contrôles qu'elle a effectués. Elle a ainsi fait procéder à des mises à jour ou même à la suppression des signalements erronés, manifestement non justifiés ou dont le délai de conservation était expiré.

3/ Le Fichier National Automatisé des Empreintes Génétiques

Le cadre législatif général relatif à l'identification d'une personne par ses empreintes génétiques a été mis en place par la loi du 29 juillet 1994⁶³ relative au respect du corps humain. Elle n'autorise une telle identification que « dans le cadre de mesures d'enquête ou d'instruction diligentées lors d'une procédure judiciaire ou à des fins médicales ou de recherche scientifique ».

Monsieur DIAZ⁶⁴ souligne qu'un « des effets de la vulgarisation de la méthode d'identification par l'ADN a été de conduire dans certaines circonstances l'autorité judiciaire à ordonner la pratique de tests génétiques sur une large population parmi laquelle on espère démasquer l'auteur d'un crime que les recherches n'ont pas permis jusque-là d'identifier ».

⁶² « 24^{ème} rapport d'activité : 2003 ». Paris : La Documentation française, 2004. 538 pages. Disponible sur internet : <http://lesrapports.ladocumentationfrancaise.fr/BRP/044000252/0000.pdf>. Page 49 et suivantes.

⁶³ Loi n° 94-653 du 29 juillet 1994 relative au respect du corps humain ; JORF du 30 juillet 1994. Disponible sur internet : <http://www.legifrance.gouv.fr/texteconsolide/AREBK.htm>

⁶⁴ DIAZ, Charles. *La police technique et scientifique*. Paris : Editions Presse Universitaire de France, 2000. 127 pages. Page 80.

En France, suite au meurtre de la jeune anglaise Caroline DICKINSON, une expertise de masse a été pratiquée, en vain sur des centaines d'hommes à Pleine-Fougères en 1996.

L'Angleterre s'est dotée dès 1993 d'un fichier national génétique, suivie par l'Allemagne en 1996. En France, le FNAEG a été instauré avec la loi du 17 juin 1998⁶⁵ relative à la prévention et à la répression des infractions sexuelles. Ce fichier centralise :

- les empreintes génétiques des personnes condamnées pour certaines infractions énumérées⁶⁶ (viol, agissements pédophiles ...)
- les traces génétiques tirées des produits biologiques de toute nature découverts sur les lieux où a été commise une infraction énumérée.

Avec ces fichiers, les services de police ont à leur disposition une quantité non négligeable d'information sur la population, quantité qui va en s'accroissant chaque fois qu'une infraction est commise par une personne non fichée.

Tous ces fichiers font appel à des procédés d'identification biométriques, qui ont été vulgarisés auprès de la population dans une optique criminelle, sécuritaire. Aujourd'hui, l'Etat souhaite généraliser ces procédés, rappelons-le développés à l'origine pour l'identification des criminels, à la vie quotidienne de chaque français. Pour ce faire, il lui faut motiver l'usage d'un tel procédé, avouons-le, extrême.

Section deuxième : Les motivations de l'utilisation de ce procédé extrême

Les autorités nationales doivent justifier aux yeux de la population l'utilisation des procédés biométriques d'identification. Pour cela, elles avancent différentes menaces (Paragraphe premier), menaces qui sont largement relayées par les médias.

Mais finalement, nous pouvons nous demander si les autorités nationales ne chercheraient pas à cacher des motifs à la population. Néanmoins, cette stratégie participe du renforcement du pouvoir des Etats (Paragraphe second)

Paragraphe premier : Les différentes menaces avancées par les autorités nationales

Les attentats du 11 septembre, par leur impact médiatique, psychologique, ont lancé les Etats dans la course à la technologie, et au développement de titres d'identité sécurisés contenant des données biométriques. En complémentarité à cette lutte contre le terrorisme (A.), les Etats instaure des titres d'identité sécurisés pour lutter contre la fraude à l'identité (B.). Les terroristes se servent de fausses identités pour commettre leurs actes.

A. La lutte contre le terrorisme

Depuis les attentats du 11 septembre 2001 contre les deux tours du World Trade Center, le désir des Etats de contrôler l'identité des individus s'est considérablement accru.

⁶⁵ Loi n° 98-468 du 17 juin 1998 relative à la prévention et à la répression des infractions sexuelles ; JORF du 18 juin 1998. Disponible sur internet : <http://www.legifrance.gouv.fr/texteconsolide/PJECZ.htm>

⁶⁶ Article 706-65 du Code de Procédure Pénale

Cinq ans après, le contexte international ne s'est toujours pas apaisé avec des vagues d'attentats réguliers⁶⁷, avec cette dernière tentative déjouée de justesse par les autorités britanniques.⁶⁸

Aux Etats-Unis, deux lois importantes ont été votées et posent le principe d'une utilisation des techniques biométriques pour assurer le contrôle des frontières :

- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act en 2001, plus connu sous le nom de « USA PATRIOT Act » ;
- The Enhanced Border Security and Visa Entry Reform Act de 2002.

L'Organisation de l'Aviation Civile Internationale (OACI), par l'intermédiaire de son président Monsieur KOTAITE le 5 décembre 2001⁶⁹, a évoqué la biométrie pour « restaurer la confiance du public après les attentats du 11 septembre » en faisant allusion à un usage judicieux de ces nouvelles technologies⁷⁰. L'OACI souligne la nécessité d'assurer la fluidité en maintenant le plus haut niveau de sécurité, en partie à travers les nouvelles technologies telles que l'identification biométrique.

Au niveau européen est entré en vigueur EURODAC⁷¹, système européen de collecte et de comparaison des empreintes digitales des demandeurs d'asile et, dans certaines conditions des étrangers en situation irrégulière.

Le règlement du 13 décembre 2004⁷² impose d'insérer dans une puce la photographie du titulaire du passeport d'ici à juin 2006, et ses empreintes digitales dans un second temps.

La biométrie est présentée officiellement comme un moyen de lutte contre le terrorisme. Le Ministre de l'Intérieur, Monsieur de VILLEPIN, a ainsi déclaré lors de son intervention à l'Institut des Hautes Etudes de la Sécurité Intérieure (IHESI) : « [...] la lutte contre le terrorisme exige des efforts nouveaux : dans le domaine du renseignement [...] ; dans le domaine des technologies en développant des programmes de biométrie et de photographies numérisées [...] ».⁷³

Une des justifications du programme INES⁷⁴ est la lutte contre le terrorisme, sous l'impulsion de l'OACI et de l'Union Européenne.

B. La lutte contre la fraude à l'identité

⁶⁷ Les attentats de Madrid en mars 2004 et ceux de Londres en juillet 2005.

⁶⁸ 10 août 2006

⁶⁹ Discours prononcé à Montréal le 5 décembre 2001

⁷⁰ CABAL, Christian. Rapport « Méthodes scientifiques d'identification des personnes à partir des données biométriques ». Rapport n° 958, déposé à l'Assemblée Nationale le 16 juin 2006. Disponible sur le site internet de l'Assemblée Nationale : <http://www.assemblee-nationale.fr/12/rap-ocst/i0938.asp>. Page 39

⁷¹ Sur la base d'une proposition de la Commission, le Parlement européen a été consulté et le Règlement du Conseil concernant cette création a été adopté (règlement n° 2727/2000 du 11 décembre 2000), complété par le règlement (CE) n° 407/2002 du Conseil du 28 février 2002

⁷² Règlement (CE) n° 2133-2004 du Conseil du 13 décembre 2004.

⁷³ Cf. article sur le site du ministère de l'Intérieur et de la réforme de l'Etat

http://www.interieur.gouv.fr/rubriques/c/c1_le_ministre/c18_discours_de_villepin/2004_06_16_ihesi

⁷⁴ Présentation du projet INES, publiée sur le site du FDI :

<http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf>

Cet argument est le premier argument cité dans le rapport du Forum des droits sur l'internet sur le Projet de carte nationale d'identité électronique⁷⁵. Selon ce rapport, une très grande majorité des Français (presque 75 %) accueille favorablement la carte d'identité électronique, dans la mesure où elle permettrait de lutter contre la fraude à l'identité.

Mais il est également rappelé que les Français se sont prononcés en l'absence même des chiffres sur la fraude et l'usurpation d'identité en France. Les chiffres avancés dans le débat concernent des études sur la fraude à l'identité dans des pays étrangers, tels que le Royaume-Uni où il n'existe pas de carte d'identité⁷⁶. Dès lors, nous pouvons légitimement nous demander l'intérêt d'un tel sondage puisque les personnes sondées ont répondu sans vraiment connaître le problème.

Le débat français a été entamé alors même que les chiffres sur la fraude n'étaient pas encore connus. Les autorités nationales ont donc présenté la carte nationale d'identité électronique, qui s'accompagne de la biométrie, comme une solution à un problème qu'elles n'ont pas identifié précisément.

Il faut attendre la publication du rapport de la mission d'information sur la nouvelle génération de documents d'identité et la fraude documentaire du 29 juin 2005⁷⁷. Selon ce rapport, « la fraude à l'identité est en pleine croissance », et suit une avalanche de chiffres :

- Entre 1999 et 2004, 84 464 titres vierges (carte d'identité, 14 700 passeports, 9 000 permis de conduire ...) ont été volés dans les préfectures et lors de leur transport ;
- Le nombre de faux documents saisi par les douanes a augmenté de plus de 65 % en deux ans, passant de 671 à 3 157 en 2003 ;
- Le nombre d'inscriptions pour fraude au fichier des personnes recherchées⁷⁸ a augmenté de 476 % entre 2000 et 2003

Le rapport termine sur l'évaluation du coût de cette fraude. Le rapport cite les pertes subies par la Régie Autonome des Transports Parisiens, ainsi qu'une estimation du coût de la fraude dans le versement des allocations et des prestations sociales.

Tout en avouant disposer de peu de chiffres pertinents, qui s'avèrent pourtant significatifs⁷⁹, le rapport désigne la biométrie comme un « surcroît de sécurité » et comme la « seule technologie permettant l'identification de millions de personnes de façon sûre [pouvant] constituer une réponse efficace aux usurpations d'identité ». Le sénateur LECLERF préconise donc la constitution d'une base centrale de données biométriques considérant que

⁷⁵ Forum sur les Droits de l'Internet. Rapport : « Projet de carte nationale d'identité électronique ». Paris, 16 juin 2005. 45 pages. Disponible sur internet :

<http://www.foruminternet.org/telechargement/documents/rapp-cnle-20050616.pdf>. Page 5.

⁷⁶ Source : Présentation du projet INES, publiée sur le site du FDI :

<http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf>

⁷⁷ LECERF, Jean-René. « Rapport d'information sur la nouvelle génération de documents d'identité et la fraude documentaire ». Rapport d'information n° 239, déposé au Sénat le 29 juin 2005. Disponible sur le site internet du Sénat : <http://www.senat.fr/rap/r04-439/r04-4391.pdf>

⁷⁸ Recensant toutes les personnes faisant l'objet d'une mesure de recherche ou de vérification de leur situation juridique (450.000 au 1er janvier 2005), ce fichier est tenu conjointement par les ministères de l'intérieur et de la défense. Il peut être consulté par les autorités judiciaires, les services de police et de gendarmerie, les autorités administratives pour des recherches relevant de leurs attributions et les services de police d'Etats liés à la France pas accord international.

⁷⁹ Rapport d'information sur la nouvelle génération de documents d'identité et la fraude documentaire, précité. Page 24

« le problème n'est pas tant la création d'un fichier des Français [mais les] conditions de son utilisation ».

Mais ces différents apparaissent comme légers, voire infondés. L'instauration de débats avec la population n'est en rien une assurance de voir le projet accepté. Ainsi, l'Observatoire des Usages de l'Internet (OUI), dans sa contribution au débat sur la carte nationale d'identité électronique⁸⁰, pose plusieurs questions.

- S'agit-il de s'entendre sur les objectifs d'un dispositif à concevoir ou de faire avaliser un dispositif déjà conçu et d'en suggérer de nouveaux usages ?
- Le dossier ne propose-t-il pas une réponse avant que ne soient clairement posées les questions ?
- Le débat ne serait alors qu'un artifice pour médiatiser un service et un produit déjà « ficelé » ?

Monsieur LAMARCHE⁸¹ dénonce « une crise de l'Etat, de sa légitimité et de ses moyens d'action [...] ». Ainsi nous pouvons nous demander si les autorités nationales ne tentent-elles pas, avec l'utilisation massive de la biométrie, de réaliser un tout autre objectif que ceux avancés jusque là, à savoir une affirmation de l'autorité des Etats sur leurs citoyens.

Paragraphe second : Le renforcement de l'autorité de l'Etat

Il apparaît très facile de contrer les arguments avancés par les autorités nationales, et repris dans le rapport du sénateur LECLERF. Selon Monsieur LAMARCHE⁸², « le discours sécuritaire [des autorités nationales] surfe sur des peurs réelles et imaginaires, les renforce pour proposer des visions simplistes et visibles ».

Les autorités nationales en sont amenées à manipuler l'opinion afin de montrer qu'elles agissent pour le bien de la population. Derrière une certaine opacité dans la prise de décision (A) se cache en réalité une perte du pouvoir de décision (B).

A. Une opacité dans la prise de décision

Cette opacité se ressent tout d'abord au travers du discours de certaines personnes publiques, notamment dans la présentation du projet INES⁸³, il est clairement indiqué que certains pays introduisent des données biométriques dans leurs cartes d'identité, leurs passeports et leurs visas « sous l'impulsion de l'Organisation de l'Aviation Civile et de l'Union Européenne ».

⁸⁰ Contribution de l'Observatoire des Usages de l'Internet (OUI) au débat sur la Carte Nationale d'Identité Electronique (CNIE), disponible sur le site internet du Forum sur les Droits de l'Internet (FDI) : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnie.pdf> ; page 48 et suivantes.

⁸¹ Contribution de Monsieur LAMARCHE au débat sur la Carte Nationale d'Identité Electronique (CNIE), disponible sur le site internet du Forum sur les Droits de l'Internet (FDI) : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnie.pdf> ; page 64 et suivantes.

⁸² Contribution de Monsieur LAMARCHE, précité.

⁸³ Présentation du projet INES, publiée sur le site du FDI : <http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf>

Face à cette affirmation, nous pouvons répondre que les cartes d'identité ne sont pas expressément visées, les Etats ont vite fait une assimilation avec les titres de voyages.

Deux institutions internationales sont donc visées, et nous aurions pu nous attendre à ce que les Etats-Unis le soient également. Simple oubli, ou bien volonté de ne pas reconnaître ce qui appartient à César, cette absence a toutefois été remarquée et soulignée⁸⁴. Ce n'est que dans le rapport du sénateur LECLERF sur la fraude documentaire que les Etats-Unis sont expressément nommés.

Trois institutions, et donc trois contraintes qui imposent la mise en place de passeports et de visas biométriques :

- le règlement du 13 décembre 2004⁸⁵ impose aux Etats membres de délivrer des passeports biométriques au plus tard le 28 août 2006 ;
- la recommandation de l'OACI du 9 mai 2003 prévoit l'intégration avant 2015 d'au moins une donnée biométrique dans les documents de voyages ;
- les Etats-Unis imposent aux pays (dont la France) qui bénéficient du programme américain d'exemption de visa, une échéance précise pour la mise aux normes de l'OACI des passeports. Fixée au 26 octobre 2006, cette échéance est sanctionnée par le rétablissement des visas à l'encontre des ressortissants détenteurs d'un passeport, délivré après cette date, ne comportant pas au minimum une donnée biométrique (la photographie faciale).

La carte nationale d'identité n'est donc aucunement visée. Pourtant, le ministère de l'Intérieur continue de faire comme ci c'était le cas. Cette façon de procéder est typique des autorités françaises. Dans l'hypothèse où un projet risque de ne pas être accepté par la population, il est facile de ne pas engager sa responsabilité d'homme politique en affirmant que la décision vient « d'en haut »⁸⁶. La construction européenne a bon dos tout de même.

Ensuite, il est clairement établi que les autorités nationales se fondent sur des chiffres non pertinents, dans la mesure où ils intéressent d'autres pays⁸⁷, ou bien trop vagues. De telles estimations font que les problèmes ne sont pas clairement définis. Par voie de conséquence, comment le législateur peut-il justifier, au titre du principe de proportionnalité, l'utilisation de ces procédés biométriques ? Aucune étude d'impact n'a été publiée, de sorte que le législateur se prononcera sur un système dont le coût n'est pas précisément évalué, et qui peut au final se révéler bien plus élevé que le coût de la fraude.

Enfin, le rapport du sénateur LECLERF⁸⁸ mentionne une « chaîne de l'identité défaillante ». Il énonce deux raisons principales dans cette défaillance.

Tout d'abord, il est possible d'obtenir une vraie carte d'identité en produisant de faux justificatifs. Dès lors, le projet INES prévoit une sécurisation de la procédure de délivrance

⁸⁴ Contribution de Monsieur DAMASIO au débat sur la Carte Nationale d'Identité Electronique (CNIE), disponible sur le site internet du Forum sur les Droits de l'Internet (FDI) : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnief.pdf> ; page 23 et suivantes

⁸⁵ Règlement (CE) n° 2133-2004 du Conseil du 13 décembre 2004.

⁸⁶ Il est aujourd'hui de tradition, en France, de couvrir la mauvaise gestion d'un problème en rejetant la faute sur l'Union Européenne.

⁸⁷ Les chiffres de la fraude au Royaume-Uni dans la présentation CNIE

⁸⁸ LECLERF, Jean-René. « Rapport d'information sur la nouvelle génération de documents d'identité et la fraude documentaire ». Rapport d'information n° 239, déposé au Sénat le 29 juin 2005. Disponible sur le site internet du Sénat : <http://www.senat.fr/rap/r04-439/r04-4391.pdf>. Page 28

des justificatifs⁸⁹. Cette nouvelle procédure permettra aux services concernés de prendre directement contact avec les services sources, tels que la mairie de naissance, afin d'obtenir les justificatifs nécessaires. Rappelons que cette solution est préconisée par la CNIL depuis 1986⁹⁰.

Pour que cette procédure puisse être appliquée, il faut attendre que le ministère de la Justice ait fini de numériser tous les actes d'état civil.

A ce niveau de notre réflexion, nous pouvons sans peine entrevoir la faiblesse du système. En effet, pour arriver à une meilleure sécurité dans la délivrance des cartes d'identité, il faut l'élaboration de deux projets, chacun par un ministère bien distinct. Mais le projet INES est dépendant du projet du ministère de la Justice. Si ce dernier est mis en place après, les données sur lesquelles se fonderont les différents titres d'identité ne seront toujours pas fiables.

Derrière ce dysfonctionnement se cache un problème récurrent de l'Administration française : l'interministérialité. L'expression « Les silos parlent aux silos » est encore d'actualité.

Ensuite Monsieur LECLERF dénonce une gestion trop lourde dans la délivrance des titres d'identité⁹¹, avec l'intervention de nombreux intervenants et le non-respect par ceux-ci des procédures mises en place. Monsieur LECLERF signale que le passeport peut être remis à un tiers, alors qu'il y a une obligation de le remettre en personne⁹².

Implicitement, nous pouvons déceler une critique du travail de certains agents. Monsieur DAMASIO⁹³ parle de « syndrome du trou dans le grillage ». Selon lui, les autorités pourront développer toutes les protections techniques qu'elles souhaitent, elles resteront sans effet du moment où l'intervention humaine est faillible. Le projet INES garanti seulement l'habilitation des agents, en rien leur honnêteté ou leur éthique.

Ce malaise existe déjà dans la procédure actuelle. Comment expliquez que des titres vierges soient volés dans des préfectures⁹⁴ ?

Dès lors, les autorités nationales se trompent de coupables. La fraude et l'usurpation à l'identité existent, nous ne pouvons le nier. Mais ce phénomène reste marginal, comparé aux 60 millions d'habitants que compte la France. Les autorités nationales ont donc le choix entre appliquer à la population entière une technologie onéreuse ou bien surveiller au mieux le

⁸⁹ Forum sur les Droits de l'Internet. Rapport : « Projet de carte nationale d'identité électronique ». Paris, 16 juin 2005. 45 pages. Disponible sur internet : <http://www.foruminternet.org/telechargement/documents/rapp-cnle-20050616.pdf>. Page 17.

⁹⁰ Délibération n° 86-076 du 1^{er} juillet 1986, rappelée dans l'avis sur la CNIE du 30/05/05.

⁹¹ LECERF, Jean-René. « Rapport d'information sur la nouvelle génération de documents d'identité et la fraude documentaire ». Rapport d'information n° 239, déposé au Sénat le 29 juin 2005. Disponible sur le site internet du Sénat : <http://www.senat.fr/rap/r04-439/r04-4391.pdf>. Page 35.

⁹² Rapport d'information sur la nouvelle génération de documents d'identité et la fraude documentaire, précité. Page 36

⁹³ Contribution de Monsieur DAMASIO au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnle.pdf> ; page 23 et suivantes

⁹⁴ Rapport d'information sur la nouvelle génération de documents d'identité et la fraude documentaire, précité. Page 21

travail des agents publics. Bien sûr, le choix dicté par la logique économique, du point de vue de l'argent public, consiste dans la deuxième solution.

Mais il faut croire qu'une autre logique a prévalu, ce qui nous amène à penser que l'Administration n'est pas vraiment le maître de ses décisions.

B. La perte de pouvoir de décision

Face à la technicité de la question des procédés biométriques d'identification, de qui émanent réellement les différentes solutions proposées ?

Cette question est sous-jacente dans la contribution de l'Observatoire des Usages de l'Internet⁹⁵ : « la démarche inverse qui serait de partir d'innovations technologiques et de se demander comment en forcer l'utilisation pour le contrôle de l'identité serait dangereuse ».

Au final, nous pouvons nous demander si la démocratie⁹⁶ dans laquelle nous vivons ne cache-t-elle pas une technocratie ? La technocratie est un système politique ou économique dans lequel les experts techniciens et fonctionnaires supplantent, en fait ou en droit les responsables politiques de la prise de décision⁹⁷.

Plus généralement, un des principaux enjeux est l'évolutivité des choix qui seront faits, tant en matière de techniques, de logiciels et de terminaux. Le choix d'un système exclusif⁹⁸ pourrait avoir des conséquences néfastes, alors que le logiciel libre semble faire l'unanimité⁹⁹.

Les procédés biométriques d'identification ont comme finalité première l'identification de criminels. Il ne faudrait pas, en plus de ce handicap, que ces procédés soient aux mains d'un très petit nombre de personnes, qui plus est non élues. Dès lors, la population n'aurait plus aucun moyen de contrôle sur celles-ci.

Nous retrouvons également cette logique de privatisation dans les certificats utilisés par l'Administration, comme le rappelle le Club de l'Hyper République¹⁰⁰. Selon lui, « les fournisseurs de certificats suivent une logique économique qui les conduit à proposer la technologie de l'environnement dominant, et les administrations s'adaptent à l'état du marché en n'utilisant que cette technologie ».

⁹⁵ Contribution de l'Observatoire des Usages de l'Internet au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnief.pdf>. Page 48 et suivantes.

⁹⁶ « La démocratie est un régime politique où la souveraineté appartient au peuple, ce qui implique que les droits de l'homme et du citoyen soient reconnus. Les élections au suffrage universel direct sont la base des démocraties modernes, qui tendent à imposer l'égalité des droits dans toutes les sphères de la vie sociale. Fondée sur la liberté et l'égalité des citoyens et sur des aspirations à l'universalité, la démocratie correspond aux impératifs de fonctionnement des sociétés modernes, où priment l'individu et les idéaux de la raison ». *Encyclopédie Bordas*, page 1422.

⁹⁷ *Encyclopédie Larousse en un volume* ; page 1376

⁹⁸ « Système d'exploitation ou architecture conçu pour un matériel ou un ensemble de matériels d'un constructeur donné ». Définition sur internet : <http://www.coges.fr/index.php?action=glossaire&lettre=S>

⁹⁹ cf synthèse du rapport « Projet de carte nationale d'identité électronique », disponible sur le site du FDI : <http://www.foruminternet.org/telechargement/documents/synth-cnief-20050616.pdf>

¹⁰⁰ Contribution du Club de l'Hyper République au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnief.pdf> ; page 55 et suivantes.

Pour en revenir aux procédés biométriques d'identification, la technique la plus utilisée en France est celle des empreintes digitales. Nous verrons plus tard que cette technologie est maîtrisée par une entreprise française¹⁰¹. Il faut donc être très vigilant, car l'utilisation d'un système exclusif, avec le secret qui l'accompagne, empêche ainsi tout contrôle démocratique.

Les autorités nationales joueraient-elles plus le jeu des entreprises que celui affiché de la sécurité ? Derrière cette question, nous devons nous interroger sur la pertinence même de la solution biométrique, et voir la forêt qui est cachée par l'arbre (Chapitre second)

¹⁰¹ Cf. infra : Titre 1, Chapitre 2, Section 2

Chapitre deuxième : La pertinence de la solution biométrique : l'arbre qui cache la forêt

Les procédés biométriques d'identification sont présentés comme le remède aux maux des anciens systèmes d'identification. Mais nous devons nous demander quelle pourrait être l'utilité d'un tel système d'identification. Notre société a-t-elle vraiment besoin de la biométrie pour identifier les individus ? Nous verrons que les fonctionnalités biométriques de la future carte d'identité électronique ne seront presque pas utilisées. Nous devons donc remettre en cause l'utilité d'un tel système d'identification (Section première).

Mais derrière tous ces projets se cachent de très fortes pressions de la part des entreprises du marché de la biométrie, qui ont tout à gagner de la généralisation des procédés biométriques d'identification qu'elles vendent. Les entreprises obtiennent dès lors une certaine part du pouvoir de décision (Section seconde).

Section première : La remise en cause de l'utilité d'un tel système d'identification

Les autorités nationales se trompent de cheval de bataille. La généralisation des procédés biométriques d'identification à toute une population est une solution certainement extrême. Mais nous doutons sur son utilité (Paragraphe premier).

En plus d'être une solution extrême, elle est également très coûteuse. La mise en place de ce système d'identification ne se fera pas sans difficultés (Paragraphe seconde).

Paragraphe premier : Des solutions extrêmes mais inutiles

Les Etats européens ont suivi les Etats-Unis dans leur lutte contre le terrorisme, et s'en servent pour justifier les procédés biométriques d'identification. Hélas, il semblerait que les différents projets, et notamment le projet français sur l'Identité Nationale Electronique Sécurisée (projet INES), soient totalement inefficaces dans cette lutte (A.) Sans aller si loin, nous verrons qu'il est possible de se contenter des titres d'identité actuels, quoiqu'en disent les autorités nationales. Il nous faudra examiner attentivement comment il est procédé aux vérifications d'identité aujourd'hui (B.)

A. Le mauvais exemple de la lutte contre le terrorisme

Nous commencerons notre raisonnement avec une question de bons sens : en quoi la délivrance d'une carte d'identité électronique, comportant les empreintes digitales et une photographie numérisées de son porteur, l'empêcherait-il de commettre un acte de terrorisme ?

A cette question les autorités nationales n'apportent bien évidemment aucune réponse. Elles ont plutôt intérêt à ce que cette question ne soit jamais posée. Il faut convaincre la

population que la biométrie est la seule solution pour la protéger des attaques terroristes, et ce sans en faire la moindre démonstration.

Cette absence de démonstration est rappelée par Monsieur PIAZZA¹⁰². Selon lui, « l'idée selon laquelle la rationalisation des procédures d'encartement des Français permettrait de lutter plus efficacement contre le terrorisme mériterait d'être rigoureusement démontrée ».

Prenons l'exemple des attentats commis à Londres au mois de juillet 2004. Les terroristes étaient des immigrés qui se sont parfaitement intégrés dans la société. La plupart était marié, certains étaient père de plusieurs enfants. Le fait de disposer de leurs empreintes digitales dans une base de données nationales aurait seulement pu empêcher la délivrance de plusieurs titres d'identité à une seule personne.

Le mode opératoire des terroristes a changé, et c'est pourquoi le recours à la biométrie dans les titres de transports est inefficace. De terroristes immigrants, nous sommes passés à des terroristes nationaux, entendons par là qu'ils détiennent la nationalité de l'Etat où ils commettent leur acte terroriste.

Au-delà du terrorisme, cette promesse de sécurité intéresse tous les actes criminels, comme le rappelle Madame GUERRIER¹⁰³ : « Quant à la sécurité, elle n'est pas garantie par une carte biométrique ; un étranger, un résident est en mesure de commettre un acte délictueux ou criminel, malgré la carte d'identité biométrique ».

B. De la vérification de l'identité aujourd'hui

Il nous faut distinguer la vérification d'identité effectuée par les forces de police¹⁰⁴ (1/) de celle effectuée dans les rapports juridiques (2/).

1/ Par les forces de police

La question des contrôles, relevés et vérifications d'identité est très délicate au regard des libertés individuelles. Conformément aux principes généraux de l'article préliminaire du Code de Procédure Pénale, ces opérations, lorsqu'elles supposent l'exercice d'une contrainte¹⁰⁵, doivent être strictement limitées aux nécessités de la procédure, proportionnées à la gravité de l'infraction et ne pas porter atteinte à la dignité de la personne.

En vertu du principe selon lequel toute personne présente sur le territoire national doit être en mesure de justifier son identité¹⁰⁶, des contrôles d'identité peuvent être pratiqués par les officiers et les agents de police judiciaire.

¹⁰² Contribution de Monsieur PIAZZA au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnle.pdf> ; page 3 et suivantes.

¹⁰³ Contribution de Madame GUERRIER au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnle.pdf> ; page 51 et suivantes.

¹⁰⁴ Services de police et gendarmerie nationale

¹⁰⁵ Pour la vérification d'identité, la personne peut être conduite au poste de police et retenue tant qu'il n'a pas été procédé à la vérification.

¹⁰⁶ Article 78-1 Code de Procédure Pénale

Il nous faut distinguer deux justifications à ces contrôles. Tout d'abord, ces contrôles peuvent se faire dans un but de prévention, c'est-à-dire prévenir toute atteinte à l'ordre public, notamment à la sécurité des personnes ou des biens, quel que soit le comportement de l'intéressé.¹⁰⁷ Mais ces contrôles peuvent également se faire dans un but judiciaire, dans la mesure où ils se feront sur la foi d'un soupçon. De tels contrôles ne sont dès lors possibles qu'à l'égard de certaines personnes. Il nous faut ici noter la loi du 18 mars 2003¹⁰⁸ a modifié les conditions d'application des contrôles d'identité. Les contrôles sont désormais possibles à l'encontre des personnes pour lesquelles il existe « une ou plusieurs raisons plausibles de soupçonner qu'elles ont commis une infraction (...) »¹⁰⁹ alors qu'auparavant ils ne concernaient que les personnes contre lesquelles il existait un « indice faisant présumer la commission d'une infraction ».

Dans l'hypothèse d'un échec du contrôle d'identité (l'individu a refusé ou s'est trouvé dans l'impossibilité de prouver son identité sur place), l'individu peut être à l'endroit de la vérification ou dans un local de police pour procéder à une recherche de l'identité¹¹⁰. Un officier de police judiciaire le met alors en mesure d'établir par tout moyen son identité. Le plus souvent, l'individu recourra aux témoignages de ces proches, de son employeur. Les limites d'un tel système sont évidentes.

Si l'individu refuse toujours d'établir son identité, y compris par des déclarations manifestement inexactes, une prise d'empreintes et de photographies est possible, avec l'accord du procureur de la République ou du juge d'instruction, si c'est l'unique moyen d'établir son identité. Les empreintes relevées seront comparées avec celles contenues dans le FAED¹¹¹. Il doit être fait mention dans un procès-verbal des motifs justifiant la prise d'empreintes digitales.

Or dans le monde informatique, nous distinguons identification (donner son identité) et authentification (prouver son identité). Donc, traduits dans le langage informatique, les contrôles d'identité correspondraient à la phase d'identification alors que les vérifications d'identité consistent à authentifier l'individu appréhendé. Si les procédés biométriques sont utilisés plus à des fins d'authentification, nous pouvons légitimement nous demander où est la limite entre contrôle et vérification d'identité en matière policière.

Ajoutons que l'utilisation de la biométrie ne garantit pas à 100% une bonne identification (ou plutôt une bonne authentification) de la personne. La biométrie impliquerait donc plus de vérifications d'identité au sens du Code de Procédure Pénale.

Nous avons vu que la prise d'empreinte digitale dans le cadre d'une procédure judiciaire n'est autorisée qu'en cas de refus ou de défaut de preuve de d'identité. Il est alors intéressant de se demander dans quelle mesure le relevé préalable de l'empreinte digitale inséré dans des titres d'identité électroniques ne remet pas en cause cette disposition procédurale.

¹⁰⁷ Article 78-2 alinéa 3 du Code de Procédure Pénale

¹⁰⁸ Loi n°2003-239 du 18 mars 2003 pour la sécurité intérieure. JORF du 19 mars 2003.

<http://www.legifrance.gouv.fr/texteconsolide/PPED1.htm>

¹⁰⁹ Article 78-2 du Code de Procédure Pénale

¹¹⁰ Article 78-3 alinéa 1 du Code de Procédure Pénale

¹¹¹ Fichier Automatisé des Empreintes Digitales

2/ Dans les rapports juridiques

Dans une relation contractuelle, les parties procèdent-elles systématiquement à la vérification de leur identité ? Pour répondre à cette question, il nous faut dès maintenant distinguer entre la théorie et la pratique.

En ce qui concerne la théorie, je reprendrai une question de Monsieur PIETTE-COUDOL¹¹² : « Qui a dit que la connaissance de l'identité de l'autre était une des conditions essentielles à la formation des contrats ? ». L'article 1108 du Code Civil traite des conditions de formations des contrats, qui sont au nombre de quatre : le consentement, la capacité, la cause et l'objet.

Le commerce de détail se déroule très souvent entre cocontractants réciproquement inidentifiés. Mais il existe des cas où la loi impose cette identification réciproque.

Un commerçant qui accepte un règlement par chèque est ainsi tenu de vérifier l'identité de la personne qui remet le chèque¹¹³. Or, bien souvent en pratique, le commerçant ne procède pas à une vérification attentive (par manque de temps peut-être, ou par excès de confiance), ou bien refuse la présentation de la pièce d'identité, de sorte qu'il se contentera de recopier au dos du chèque le numéro de la pièce d'identité, sa date et son lieu de délivrance.

Dans l'hypothèse où le commerçant procède à une vérification, celle-ci ne peut être que sommaire. Le commerçant ne dispose pas des moyens, ni des connaissances des services spécialisés dans la détection de fausses pièces d'identité, tels que la Police Aux Frontières.

A la Poste, il est expressément indiqué que toute opération bancaire nécessite la présentation d'une pièce d'identité, mais le contrôle effectué par l'agent ne porte que sur le nom du titulaire du compte, qui doit correspondre à celui du titulaire de la pièce d'identité, ainsi que sur la photographie.

Avec la future carte d'identité électronique, le commerçant sera toujours dans la même situation. Les vérifications qu'il effectuera porteront toujours sur les éléments inscrits sur la carte, sans s'intéresser aux données biométriques contenues dans la carte. En conséquence, une personne qui se sera procurée une carte d'identité vierge volée pourra induire le commerçant en erreur.

Un notaire a l'obligation de vérifier l'identité des parties, selon le décret du 26 avril 1971. Pour ce faire, il contacte directement les mairies de naissance de chaque partie afin de se faire délivrer directement une copie de l'acte de naissance. Il ne lui reste plus qu'à comparer avec les pièces apportées par les parties.

Un banquier doit vérifier l'identité et l'adresse de celui à qui il va ouvrir un compte et remettre un chéquier¹¹⁴.

¹¹² Contribution de Monsieur PIETTE-COUDOL au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnief.pdf> ; page 10 et suivantes.

¹¹³ Article 12-2 du décret loi du 30 octobre 1935 : « Toute personne qui remet un chèque en paiement doit justifier de son identité au moyen d'un document officiel portant sa photographie. »

¹¹⁴ Versailles, 29 avril 1988 (cf. Dalloz 1989, 251) et loi n°90-614 du 12 juillet 1990 sur la blanchiment des capitaux, JORF du 14 juillet 1990. Disponible sur internet : <http://www.legifrance.gouv.fr/texteconsolide/AFEAB.htm>

Au vu des ces indications, rien ne permet d'affirmer que la carte d'identité électronique sera la solution. Comme indiqué précédemment, il sera certes impossible de se faire délivrer plusieurs titres sous plusieurs identités, mais nous ne pouvons être aussi catégoriques pour ce qui est de l'obtention d'un vrai titre sur présentation de faux justificatifs ou bien du vol d'un titre vierge.

Dès lors que les cocontractants décident se s'identifier réciproquement, c'est-à-dire vérifier leurs identités, comment peuvent-ils ne pas faire confiance dans des titres délivrés par l'Etat ? Si le système est faussé à la base, implanter dans la carte d'identité des éléments biométriques pour une vérification en bout de chaîne est inutile.

Paragraphe second : Les difficultés de mise en place d'un tel système

La mise en place de la Carte Nationale d'Identité Electronique aura des conséquences qui sont difficilement acceptables (A.) A ces difficultés s'ajoute le fait que les procédés biométriques d'identification ne sont pas infaillibles et illimités (B.).

A. Des conséquences de la CNIE

Dans le projet INES, arrêté le 1^{er} mars 2005¹¹⁵, il est prévu que la future carte d'identité électronique ne sera pas obligatoire. Nous pouvons donc nous interroger sur la valeur du discours sécuritaire sensé justifier la mise en place d'une telle carte, accompagné de procédés d'identification biométriques.

Comment lutter contre la fraude et l'usurpation d'identité si les malfaiteurs peuvent se contenter de leurs anciennes fausses cartes ? Comment arrêter les terroristes ? Ce caractère non obligatoire est la meilleure solution pour proroger les fraudes actuelles.

Il est certain qu'une carte non obligatoire serait mieux accueillie, mais elle ne serait donc pas à même de remplir les objectifs qui ont été fixés. Si elle n'est pas obligatoire en droit, rien n'interdit qu'elle le soit dans les faits. Dès lors, il serait possible d'exiger la présentation d'une carte d'identité électronique pour accéder à certains services.

Obligatoire ou non, le projet souffre d'un problème plus important : la création d'une immense base de données¹¹⁶ biométriques. Le fonctionnement en est très simple :

- Il faut tout d'abord commencer par l'acquisition de la caractéristique physique (échantillon qui servira de référence) par la machine. Il s'agit de l'enrôlement.
- Ensuite, cette empreinte est transformée en donnée qui pourra faire l'objet d'un traitement informatique et qui sera conservée sur un support¹¹⁷ en vue de leur réutilisation.

¹¹⁵ Présentation du projet INES, publiée sur le site du FDI :

<http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf>

¹¹⁶ Base de données : « On entend par base de données un recueil d'oeuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen ». Article L 112-3 du Code de la Propriété Intellectuelle

¹¹⁷ Disque dur, cd rom, disquette

La création d'une telle base de donnée est indispensable pour empêcher des personnes de déposer plusieurs demandes de carte d'identité sous plusieurs identités. Ne pas prévoir de base de données revient au même que de ne pas rendre cette carte obligatoire. Cela revient à condamner à l'échec ce système.

Dans la très grande hypothèse de la constitution d'une base de données biométriques, il nous faut dès maintenant préciser que son accès et son utilisation devront être réglementés conformément à la loi « Informatique et Libertés »¹¹⁸, comme nous le verrons dans la seconde partie. Nous nous tiendrons seulement à faire la lumière sur les inconvénients résultants de la mise en place d'une telle base de données.

Tout d'abord sur le coût. La mise en place de systèmes d'identification biométriques reste très coûteuse, même si la plupart des sociétés commercialisant de tels produits pratiquent une politique axée sur la réduction des prix. Chiffre en France.

Cependant, l'enrôlement de toute une population (60 millions d'habitants pour la France), qui consiste en la collecte et l'enregistrement des empreintes digitales, ainsi que l'élaboration d'une base de données et le fonctionnement du système avec l'achat de nombreux lecteurs de cartes font peser sur les finances publiques, et donc sur le contribuable, des sommes colossales.

En plus du coût se pose le problème de la conservation des données. Ainsi, pour empêcher toute tentative de fraude, les données seront conservées perpétuellement. De même, pour faire face aux problèmes posés par la perte d'une carte ou la casse de la puce, un agent habilité pourra contrôler l'identité de la personne par rapport aux données biométriques enregistrés dans la base et redélivrer une autre carte d'identité. Effacer les données au bout d'un certain temps revient à ne pas avoir de base de données.

Sur ce point, le projet apparaît en totale contradiction avec la loi Informatiques et Libertés, qui limite dans le temps la conservation des données à caractère personnel.

Il faut ajouter aux deux précédents inconvénients le risque d'interconnexion. Cette base de données aura pour finalité unique l'identification de personnes lors de l'établissement de titres d'identité. Mais si nous nous référons au promoteur du projet INES, le ministère de l'Intérieur, nous sommes en droit d'être perplexe. Selon Monsieur DAMASIO¹¹⁹, « il apparaît impossible de croire qu'un ministère dans la vocation même est de veiller aux délinquances puisse avoir conçu un système sans deviner de quelle façon il serait tourné ».

Certaines garanties sont d'ores et déjà apportées par le ministère, au conditionnel tout de même, et reprises dans la synthèse effectuée par le Forum des Droits sur l'Internet (FDI).

- Seules les autorités habilitées (police, gendarmerie, douanes) auraient accès aux informations stockées dans la base, et ce sous contrôle judiciaire.
- Les accès aux bases seraient journalisés pour prévenir tout abus, et les peines en cas d'accès non autorisés seraient aggravés.

¹¹⁸ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 ; JORF du 7 août 2004 ; Disponible sur internet :

<http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm>

http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf

¹¹⁹ Contribution de Monsieur DAMASIO au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnle.pdf> ; page 23 et suivantes

- Les vérifications pour des demandes de titre seraient automatiques, sans que l'agent n'ait accès à la base.

Pour l'instant, il ne s'agit que de propositions. Il reste maintenant à savoir quel sera le véritable contenu du projet de loi. Avec de tels inconvénients, il est légitime de penser que le projet subira quelques modifications.

Mais en plus de ces inconvénients, nous ne devons pas oublier que l'usage d'un tel procédé d'identification est faillible, et donc imparfait.

B. Un procédé faillible et imparfait

La technologie de la biométrie fascine, que ce soit grâce à sa commodité d'usage, par l'image développée par les médias ou bien par l'absence d'analyse des failles. Cette fascination amène une certaine vulgarisation de cette technologie. Dès lors nous assistons à une floraison de sites internet et de forums sur ce sujet. Les critiques, fondées ou non, se multiplient, mais la plupart émane de personnes non expertes¹²⁰ en la matière, du moins dont les connaissances n'ont pas été reconnues.

Il en va différemment quand des personnes spécialistes en matière de sécurité mettent en garde contre une mauvaise utilisation de la biométrie. Dès lors, la défiance de spécialistes de la sécurité vis-à-vis des procédés biométriques d'identification devrait davantage inquiéter les pouvoirs publics.

Cette faillibilité des systèmes biométriques résulte dans le traitement statistique qu'ils opèrent (1/), auquel il ne faut pas oublier d'ajouter les conséquences de la confusion entre l'identification et l'authentification (2/)

1/ Les taux d'erreur des systèmes biométriques

L'existence d'erreur est inévitable du fait du fonctionnement des systèmes biométriques que la biométrie repose sur le principe que chaque élément biométrique est unique.

La question de l'unicité recouvre en fait deux problèmes : l'unicité de l'élément biométrique choisi et l'unicité de la mesure (représentation sous forme de données numériques) de cet élément, l'un comme l'autre devant être propres à une seule personne.

L'unicité d'un élément biométrique n'ayant jamais été démontré scientifiquement, la biométrie repose sur des méthodes statistiques destinées à déterminer la probabilité que deux personnes présentent la même donnée¹²¹.

¹²⁰ <http://ecolesdifferentes.free.fr/JEUDES1000BORNES.htm>,
http://yonne.lautre.net/article.php3?id_article=1520.

¹²¹ CABAL, Christian. Rapport « Méthodes scientifiques d'identification des personnes à partir des données biométriques ». Rapport n° 958, déposé à l'Assemblée Nationale le 16 juin 2006. Disponible sur le site internet de l'Assemblée Nationale : <http://www.assemblee-nationale.fr/12/rap-ocst/i0938.asp>. Page 31

L'unicité d'une donnée biométrique¹²² n'est pas assurée, et ce pour la simple raison que les techniques biométriques ne sont qu'approximatives, même si les caractéristiques humaines prises en compte étaient uniques. « Cette approximation résulte des imprécisions des techniques appliquées et des différentes circonstances dans lesquelles les caractéristiques humaines sont présentées et mesurées »¹²³.

Les taux d'erreur¹²⁴ varient en fonction de la technique utilisée, ainsi les systèmes utilisant l'empreinte digitale sont beaucoup plus fiables que ceux utilisant la reconnaissance faciale.

Mais ce taux d'erreur n'est pas nul¹²⁵. Il existe et pose problème lorsque les techniques sont utilisées à une aussi grande échelle que la population d'un pays. Monsieur CABAL reprend des chiffres publiés par le National Physical Laboratory britannique¹²⁶. Si nous nous intéressons seulement à la technique des empreintes digitales, le taux de fausse acceptation va de 0,008 % à 0,45 % à et celui de faux rejet de 2,5 % à 11 %.

Néanmoins la question des erreurs technologiques reste un point important en droit. Rappelons en effet ce qu'est l'erreur en droit.

Selon le vocabulaire juridique de Monsieur CORNU¹²⁷, l'erreur au sens général est le fait de se tromper « sur l'existence, le sens ou la portée d'un droit ou d'une règle de droit »¹²⁸ ou « sur l'existence d'un fait ou dans l'appréciation d'une situation juridique »¹²⁹.

Mais en matière pénale, la qualification d'erreur de droit ou de fait est d'une importance capitale, dans la mesure où l'erreur de droit¹³⁰ est en principe sans influence sur la réalisation de l'infraction, alors qu'une erreur de fait¹³¹ exclut la culpabilité dans le cadre d'une infraction intentionnelle.

L'existence d'un risque d'erreur crée un doute sur l'identité de la personne. Il n'en faut pas plus pour un juge américain¹³², qui a remis en cause la fiabilité du système d'identification par empreinte digitale. Face à une probabilité de certitudes qui n'est pas de 100 %, le risque de se tromper existe toujours.

¹²² cf Introduction

¹²³ CABAL, Christian. Rapport « Méthodes scientifiques d'identification des personnes à partir des données biométriques ». Rapport n° 958, déposé à l'Assemblée Nationale le 16 juin 2006. Disponible sur le site internet de l'Assemblée Nationale : <http://www.assemblee-nationale.fr/12/rap-ocst/i0938.asp>. Pages 31 et 32

¹²⁴ Faux rejet (une personne n'est pas reconnue par un système biométrique alors qu'elle aurait dû l'être) ou fausse acceptation (une personne est acceptée par un système biométrique alors qu'elle n'aurait pas dû l'être)

¹²⁵ BWG, « Tolerance of zero errors is inachievable ». Source : CABAL, Christian. Rapport « Méthodes scientifiques d'identification des personnes à partir des données biométriques ». Rapport n° 958, déposé à l'Assemblée Nationale le 16 juin 2006. Disponible sur le site internet de l'Assemblée Nationale : <http://www.assemblee-nationale.fr/12/rap-ocst/i0938.asp>. Page 31.

¹²⁶ Rapport Cabal précité, pages 35, 36.

¹²⁷ CORNU, Gérard. *Vocabulaire juridique*. Paris : Editions Presse Universitaire de France, 2005 (7^{ème} édition). 970 pages. Page 362.

¹²⁸ Erreur de droit

¹²⁹ Erreur de fait

¹³⁰ Erreur sur l'existence ou le sens de dispositions légales ou réglementaires

¹³¹ Erreur sur l'existence de la situation dans laquelle l'auteur s'est trouvé

¹³² Monsieur POLLAK, juge fédéral de Philadelphie, arrêt « United States vs Piazza » du 7 janvier 2002, Manuel de criminalistique moderne

Le risque d'erreur, aussi infime soit-il, ne doit pas nous empêcher de nous demander qui supporte l'erreur.

Pour le moment, la question ne semble être abordée que dans le cadre des autres techniques d'authentification que sont la signature et le certificat électroniques. Monsieur CAPRIOLI¹³³ a ainsi eu l'occasion d'émettre son avis lors des débats sur la carte d'identité électronique. Il considère que l'Etat, en tant qu'autorité de certification, est responsable de la fiabilité du procédé de signature électronique (l'outil de signature et le certificat).¹³⁴ En revanche, l'une de ses collègues, Madame LAFFAIRE, limite cette responsabilité « à la délivrance des certificats et pour une durée limitée ». ¹³⁵

Sachant que les procédés biométriques sont aussi contrôlés et mis au point par l'Etat, peut-on envisager une telle responsabilité dans le cas, même rare, où des erreurs système provoqueraient une mauvaise ou inadéquate identification d'un individu ? Autrement dit, l'Etat peut-il être tenu responsable de la fiabilité des procédés biométriques ?

Il est tout de même possible de réduire l'erreur, et ce de deux façons :

- D'une part en croisant des données biométriques de types différents ;
- D'autre part avec l'établissement d'un droit d'accès et de rectification. L'erreur pourra être corrigée, mais ce contrôle n'intervient qu'*a posteriori*.

L'existence d'un risque d'erreur est la première raison de la faillibilité des systèmes biométriques, et la seule selon le portail français <http://www.biometrie.online.fr>. Ce site tente de convaincre des avantages de la biométrie en matière d'authentification, par exemple en remplacement du mot de passe. Ainsi, il y a une confusion entre l'identification et l'authentification, ce qui a des conséquences dangereuses.

2/ Les conséquences de la confusion Identification - Authentification

Il faut nous référer à l'article¹³⁶ de Monsieur WOLF, expert en sécurité et membre de la DCSSI¹³⁷ remet méthodiquement en cause l'efficacité de dispositifs sécuritaires fondés uniquement sur la biométrie. Ce spécialiste de la sécurité informatique met en exergue les faiblesses technologiques des procédés biométriques.

L'analyse négative de monsieur WOLF quant à la sécurité des procédés biométriques ne peut en outre être comprise que si l'on prend en compte la manière dont il définit les notions d'identification et d'authentification : « s'identifier c'est communiquer son identité, s'authentifier c'est apporter la preuve de son identité ».

¹³³ Contribution de Monsieur CAPRIOLI au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnief.pdf>. Page 80 et suivantes

¹³⁴ Forum sur les Droits de l'Internet. Rapport : « Projet de carte nationale d'identité électronique ». Paris, 16 juin 2005. 45 pages. Disponible sur internet :

<http://www.foruminternet.org/telechargement/documents/rapp-cnief-20050616.pdf>. Page 24.

¹³⁵ Ibidem.

¹³⁶ WOLF, Philippe. « De l'authentification biométrique ». *Sécurité des systèmes d'information*, n° 46, octobre 2003 : 6 pages.

Egalement disponible sur internet : <http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num46.pdf>

¹³⁷ Direction Centrale de la Sécurité des Systèmes d'Information. Cf. infra Titre 2, Chapitre 2, Section 1, §2, B.

Monsieur WOLF essaie de mettre en garde contre l'authentification biométrique, car elle souffre de limites techniques, qu'il reprend à travers deux exemples pratiques.

Monsieur WOLF traite tout d'abord de « l'usurpation de la donnée biométrique », qui consiste à se doter de la caractéristique biométrique d'une autre personne. Un chercheur japonais a réussi à fabriquer de « vraies-fausse » empreintes digitales avec de la gélatine alimentaire, et à tromper onze des quinze principaux lecteurs biométriques du marché¹³⁸. La diffusion de cette technique sur internet, ainsi que son prix très abordable, compromet gravement son utilisation comme moyen d'authentification dans le cadre d'une politique de sécurisation d'un système d'information.

Ensuite, Monsieur WOLF insiste sur le fait que la divulgation de la donnée biométrique est « inévitable ». Selon lui, « ce qui fait l'intérêt d'une donnée biométrique dans l'identification, à savoir le lien quasi unique entre cette donnée et son propriétaire devient dans le cadre de l'authentification une vulnérabilité majeure »¹³⁹.

L'authentification consiste à prouver l'identité annoncée lors de la phase d'identification. Cette authentification peut se faire de plusieurs manières : avec un secret partagé par le titulaire et qui peut être énoncé, un objet, un caractère de la personne, un savoir faire¹⁴⁰.

Utilisée à des fins d'authentification, la donnée biométrique vient remplacer le mot de passe¹⁴¹, ce qui renforce la commodité du système. Elle sera donc divulguée à de nombreuses reprises, aussi bien pour l'identification (en remplacement du login) que pour l'authentification (mot de passe). Mais contrairement à un mot de passe, il est difficile de changer la donnée biométrique d'un individu.

La donnée biométrique ne peut pas être modifiée à la suite d'une compromission qui devient de ce fait définitive. Un mot de passe compromis peut-être modifié, un certificat compromis est révoqué, mais va-t-on greffer de nouveaux doigts à la personne dont les empreintes auront été volées ?

Le système peut également être poussé plus loin. Or, la biométrie aurait tendance à confondre login et mot de passe : alors que la solution classique requiert la validation des deux paramètres, les procédés biométriques n'en demandent trop souvent qu'un seul.

Les systèmes d'authentification impliquent par nature la comparaison entre le relevé effectué et la base de données dans lequel le profil de l'individu est stocké. Dès lors, les données biométriques deviennent publiques dans la mesure où elles sont connues et accessibles par des tierces personnes qui sont habilitées à y accéder.

Se pose donc le problème de la sécurité des bases de données biométriques. Un piratage de ces bases de données aurait de terribles conséquences puisque la totalité des données s'en retrouverait compromise. Imaginons le piratage de la base de données qui sera mise en place dans le cadre du projet INES pour comprendre l'ampleur du problème.

¹³⁸ <http://cryptome.org/gummy.htm> et <http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf>. Source : WOLF, Philippe. « De l'authentification biométrique », précité.

¹³⁹ WOLF, Philippe. « De l'authentification biométrique », précité. Page 3

¹⁴⁰ WOLF, Philippe. « De l'authentification biométrique », précité.

¹⁴¹ cf. KURP, Youzec. « Carte, puce et biométrie ». *Banque Stratégie*, n° 179, février 2001 : pages 24 à 25

La confusion entre les fonctions d'identification et d'authentification des procédés biométriques est donc dangereuse en terme de sécurité. En présence d'une base de données biométriques, qui plus est à caractère national, la faiblesse du système repose sur la question d'une bonne gestion des données biométriques conservées.

- Qui aura accès à ces données ?
- Le réseau sur lequel transiteront les données sera-il sécurisé ?

Les données biométriques enregistrées dans la puce de la future carte d'identité ne serviront donc que pour les services de police, lors d'un contrôle d'identité, donc pour un usage marginal. De surcroît, les procédés biométriques d'identification souffrent de défaillances. Comment les autorités nationales peuvent-elles envisager une généralisation de ces procédés alors qu'elles ont connaissance de tous ces problèmes, si ce n'est peut-être qu'elles ne décident plus toutes seules.

Section seconde : Vers un nouveau partage de pouvoirs au profit des entreprises

Avec de nouvelles utilisations, le marché de la biométrie s'est octroyé une assurance contre les difficultés économiques. Avec un marché de la biométrie en plein essor (Paragraphe premier), nous assistons en réalité à l'émergence d'un nouvel acteur dans la prise de décisions des Etats (Paragraphe second).

Paragraphe premier : Le marché de la biométrie en plein essor

Notre analyse sera plus économique que juridique, néanmoins elle est nécessaire face aux enjeux économiques de la mise en œuvre des procédés biométriques d'identification.

A titre d'exemple, nous citerons le rapport de l'Office parlementaire, qui qualifie les enjeux économiques de « considérables »¹⁴². Le rapport cite également plusieurs montants (chiffres d'affaires), qui varient selon les sources¹⁴³.

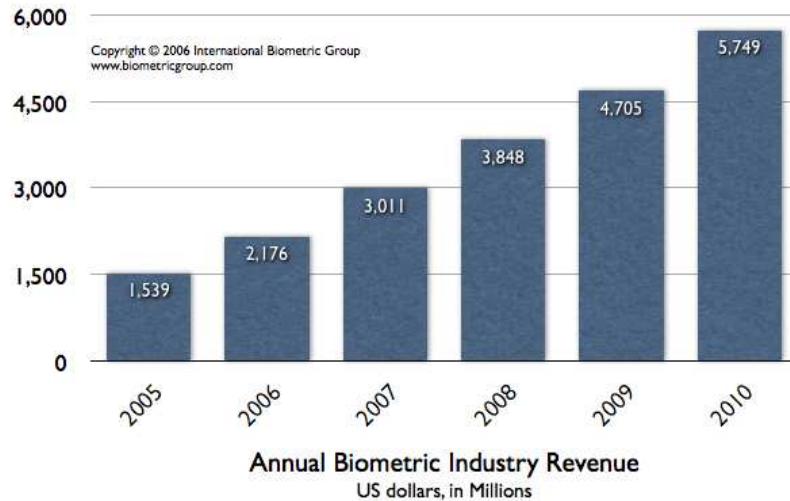
Nous nous référerons au site internet français <http://www.biometrie.online.fr>, qui se reporte au site de l'International Biometric Group (IBG)¹⁴⁴. Ainsi, les revenus mondiaux générés par le secteur de la biométrie seraient presque multipliés par trois entre 2006 et 2010.

Illustration n°1 : Evolution mondiale du marché de la biométrie de 2005 à 2010

¹⁴² CABAL, Christian. Rapport « Méthodes scientifiques d'identification des personnes à partir des données biométriques ». Rapport n° 958, déposé à l'Assemblée Nationale le 16 juin 2006. Disponible sur le site internet de l'Assemblée Nationale : <http://www.assemblee-nationale.fr/12/rap-ocgst/i0938.asp>. Page 47

¹⁴³ Rapport CABAL, précité. Page 48

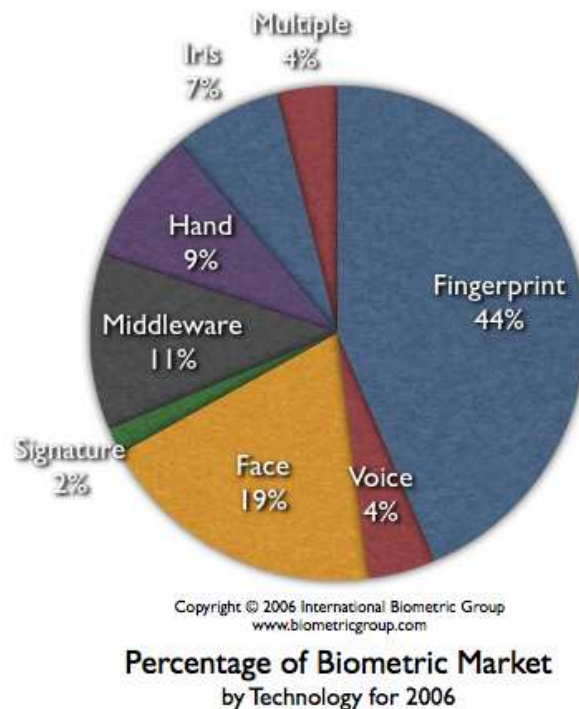
¹⁴⁴ <http://www.biometricgroup.com/>



Source : International Biometric Group, janvier 2006
http://www.biometricgroup.com/reports/public/market_report.html

Des études ont également été menées afin de déterminer les parts de marché calculées en fonction de la technologie biométrique utilisée.

Illustration n°2 : parts de marché de chaque technologie biométrique en 2006



Source : International Biometric Group, janvier 2006
http://www.biometricgroup.com/reports/public/market_report.html

Le marché reste largement dominé par la technologie de reconnaissance des empreintes digitales, bien qu'elle subisse le développement d'autres technologies. Elle est

passée 48 % en 2004 à 44 % en 2006¹⁴⁵. Il nous faut noter que ces chiffres ne prennent pas en compte les applications judiciaires.

En France, plusieurs sociétés se partagent le marché de la biométrie. Nous ne manquerons pas de citer un important groupe industriels : Sagem. Le groupe Sagem, avec sa branche « Systèmes Sécurisés & Multibiométrie » est désigné comme le leader mondial dans le secteur de l’empreinte digitale avec le rachat en 1993 de l’application « Morpho ».

L’analyse des produits proposés par les entreprises montre une réelle volonté de rendre la technologie biométrique plus accessible à un large public, d’une part en multipliant les produits, et d’autre part en baissant les prix.

Illustration n°3 : Prix des produits de sécurité basés sur la technologie biométrique des empreintes digitales

Fournisseurs	Produits	Caractéristiques	Prix ht
GFI Prociels gfi.fr	Escale	Terminal/lecteur de badge haute sécurité capable de gérer une carte à puce ou sans contact et l’identification biométrique grâce à son capteur d’empreinte digitale. Celui-ci est basé sur les algorithmes de reconnaissance d’empreintes d’AST et le capteur de technologie d’Upek.	1700 €
APC apc.com/fr	Biometric Password Manager	Lecteur biométrique d’empreinte digitale, basé sur la technologie d’analyse des couches inférieures de l’épiderme TruePrint d’AuthenTec. Il est fourni avec un câble USB et un logiciel (compatible avec Windows XP, ME, 2000 et 98). Fonctionne pour 20 utilisateurs.	69,99 €
HP hp.com/fr	iPAQ hx 2750	PDA avec lecteur biométrique d’empreinte digitale HP ProtectTools sécurisé par Credant Technologies. Il est livré avec Microsoft Windows Mobile 2003 seconde édition et le processeur Intel PXA.270 à 624 MHz. Mémoire de 256 Mo.	542 €
Targus targus.com/fr	Defcon Fingerprint Authenticator	Capteur d’empreinte digitale intégrant la technologie TruePrint, comprenant un câble détachable et deux ports USB pour connecter une souris et un clavier. Il est compatible avec Windows 98, ME, 2000 et XP.	141,30 €
IBM ibm.fr	ThinkPad X41	Ordinateur ultraportable (268 x 211 x 21-27 mm pour 1,23 kg) avec Pentium M LV 758 (1,5 GhZ/2 Mo). Ce modèle est équipé du lecteur d’empreinte digitale intégré Fingerprint Reader.	2 000 €
Zalix zalix.fr	BioFlash	Disques flash USB avec accès protégé par empreinte digitale. Il est livré avec un logiciel contenant USB Secret pour crypter et décrypter les données, USB Zip pour compresser et décompresser les fichiers, Screen Saver Lock qui verrouille l’écran après déconnexion, et Recovery pour reformater le BioFlash.	98 €
Istec istec-europe.com	Fingdrive	Clé USB2 avec capteur biométrique d’empreinte digitale, d’une capacité de 128 Mo à 1 Go. Cette clé permet une partition variable entre les informations publiques et privées (protégées par le système biométrique) et gère 5 utilisateurs. Modèle proposé en plusieurs couleurs.	à partir de 80 €
Identix identix.com	Keytronic	Clavier équipé d’un lecteur biométrique d’empreinte digitale. Le logiciel Biologon fourni assure l’administration des informations de sécurité. Il est également possible d’adjoindre à ce modèle un lecteur de cartes à puces.	295 €

Source : Olivier WACHE, *Décision distribution*, 25 avril 2005 ; site 01net.com ; <http://www.01net.com/article/274782.html>

¹⁴⁵ Chiffres publiés sur internet : <http://www.01net.com/article/274782.html>

Les entreprises ne sont pas à court d'imagination pour développer des produits biométriques (empreintes digitales)

- La société Axess'In¹⁴⁶ a développé un attaché-case muni d'une serrure biométrique.
- De nombreux produits sont développés pour « sécuriser » l'usage de l'ordinateur, tels que des lecteurs biométriques branchés en USB et même des souris avec un lecteur biométrique (plus besoin de lâcher la souris). L'entreprise IBM a doté certains ordinateurs portables (ThinkPad T42) de lecteurs biométriques.
- La société Lexibook le Magic Computer Oui-Oui¹⁴⁷, jouet qui ressemble à un ordinateur portable et intègre un simulateur de « reconnaissance digitale » pour le démarrer.

A côté du développement de produits biométriques, les entreprises imaginent différentes applications. « La liste des applications pouvant utiliser la biométrie pour contrôler un accès (physique ou logique), peut être très longue. La taille de cette liste n'est limitée que par l'imagination de chacun »¹⁴⁸.

- **Contrôle d'accès aux locaux**
 - Salle informatique
 - Site sensible (service de recherche, site nucléaire)
- **Systèmes d'informations.**
 - Lancement du système d'exploitation
 - Accès au réseau
 - Commerce électronique
 - Transaction (financière pour les banques, données entre entreprises)
 - Signature de document (lot de fabrication de médicaments)
 - Tous les logiciels utilisant un mot de passe
- **Equipements de communication**
 - Terminaux d'accès à internet
 - Téléphones portables
- **Machines & Equipements divers**
 - Coffre fort avec serrure électronique
 - Distributeur automatique de billets
 - Casier sensible (club de tir, police)
 - Cantine d'entreprise (pour éviter l'utilisation d'un badge par une personne extérieure)
 - Casier de piscine (plus d'objet à porter sur soi)
 - Contrôle des adhérents dans un club, carte de fidélité
 - Contrôle des temps de présence
 - Voiture (anti-démarrage)
- **Etat / Administration**
 - Fichier judiciaire
 - Titres d'identité (carte nationale d'identité, passeport, permis de conduire, titre de séjour)
 - Services sociaux (sécurisation des règlements)
 - Services municipaux (sécurisation des accès aux écoles, contrôle de l'utilisation des services périscolaires)

¹⁴⁶ Site internet : <http://www.axessin.fr>

¹⁴⁷ Produit disponible sur internet :

http://www.lexibookjunior.com/product_list.aspx?nrref=668200&taf=12&tas=&id_lang=7

¹⁴⁸ Source : http://biometrie.online.fr/Marche_index.htm

- Système de vote électronique

Source : <http://biometrie.online.fr>

Une telle campagne marketing, visant à promouvoir l'usage de la biométrie, doit cependant nous inquiéter. Face à un tel développement, nous pouvons nous interroger sur la place que les entreprises se réservent dans la future société où l'empreinte digitale sera reine, malgré son lourd passé.

Paragraphe second : Le nouveau rôle des entreprises dans la nouvelle société

L'intérêt sécuritaire, cher aux Etats, des procédés biométriques d'identification ne passe-t-il pas au second plan, derrière l'intérêt économique des entreprises ?

Les propos de certains industriels peuvent faire froid dans le dos. Nous venons de voir que, malgré de possibles bienfaits de la biométrie, les dangers d'un développement non régulé de cette technologie sont bien supérieurs.

Le Groupement des industries de l'interconnexion, des composants et des sous-ensembles électroniques¹⁴⁹ a remis au gouvernement un « livre bleu » sur les grands programmes structurants, regroupant les propositions des industries électroniques et numériques¹⁵⁰.

Ce rapport débute par une menace au chômage. En cinq années, le nombre de personnes employées est passé de 300000 à 220000, alors que « cette filière est [...] stratégique pour le développement économique et pour la souveraineté nationale »¹⁵¹. L'Etat se doit donc de commander, de dépenser l'argent public pour le bénéfice d'entreprises privées, mais également d'édicter les mesures législatives nécessaires à la mise en place des innovations technologiques, ou des mesures fiscales aidant le secteur¹⁵².

Différents programmes doivent être mis en œuvre par l'Etat, dont celui sur la sécurité. Les programmes en eux-mêmes ne sont pas intéressants pour notre étude, seules les justifications sont pertinentes. Le GIXEL rappelle ainsi que nous vivons dans un monde dangereux, que ce soit avec la menace terroriste ou bien simplement dans les transports en commun. Cette insécurité pèse sur les échanges, et c'est à l'Etat de rétablir cette sécurité. Il va même jusqu'à comparer l'effort pour lutter contre le terrorisme à l'effort de guerre¹⁵³.

« 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.

¹⁴⁹ GIXEL, <http://www.gixel.fr>

¹⁵⁰ « Livre bleu », Grands programmes structurants, Propositions des industries électroniques et numériques ; juillet 2004 ; Disponible sur internet :

http://www.gixel.fr/Portal_Upload/Files/ASSISES%202004/LB300604.pdf

¹⁵¹ « Livre bleu », précité. Page 3

¹⁵² « Livre bleu », précité. Page 10

¹⁵³ « Livre bleu », précité. Page 34

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 représentants s'identifieront pour aller chercher les enfants.
- Introduction dans des biens de consommation, de confort ou des jeux : téléphone portable, ordinateur, voiture, domotique, jeux vidéo
- Développer les services « cardless » à la banque, au supermarché, dans les transports, pour l'accès Internet, ... »

Il est donc demandé à l'Etat de prendre en main la campagne publicitaire, pour le bénéfice des entreprises. Les termes employés trahissent une volonté d'imposer, de façon détournée avec des fonctionnalités attrayantes, une technologie à la population, sans lui demander son avis. Les citoyens sont donc réduits à de simples consommateurs de produits biométriques.

Le GIXEL va même plus loin en demandant à ce que la biométrie soit implantée dans les écoles, afin que les enfants s'habituent dès le plus jeune âge, peut-être au point de ne plus s'en passer après. C'est la population des enfants et des adolescents qui est clairement visée avec les téléphones portables, les ordinateurs, les jeux vidéo.

Le GIXEL termine en dénonçant la législation en vigueur¹⁵⁴, trop contraignante pour permettre l'application des innovations technologiques. « Cependant, le marché national ne soutient pas suffisamment les développements possibles de ces technologies à cause des faibles budgets qui ont été jusqu'alors consacrés par les pouvoirs publics et par une législation contraignante. L'objectif est d'augmenter la sécurité tout en évitant de nuire à la liberté de chacun, l'informatique et la biométrie devraient y parvenir. Le politique doit assouplir la législation afin de favoriser le développement des technologies de la sécurité électronique et informatique. »

L'informatique et la biométrie sont donc la solution pour augmenter la sécurité, alors que notre étude tend à démontrer que c'est justement cette combinaison qui est un danger pour la sécurité. Nous rejoignons ainsi l'Observatoire des Usages de l'Internet, qui mettait en garde contre la démarche consistant à partir d'innovations technologiques, développer sans but précis, et de se demander comment en forcer l'utilisation¹⁵⁵. Les entreprises vendent une technologie dans le but caché de faire du profit.

L'Etat doit lui-même mettre en place des procédés biométriques d'identification. Ainsi, l'Etat amorce un dispositif dont les véritables bénéficiaires sont les entreprises. Ainsi Monsieur CHOUKROUN¹⁵⁶, a déclaré lors d'une interview : « Nous recevons de nombreuses demandes de revendeurs et de SSII, qui souhaitent proposer des outils biométriques. Les récentes annonces de produits et les projets comme le projet INES ont un effet moteur sur le

¹⁵⁴ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 ; JORF du 7 août 2004 ; Disponible sur internet :

<http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm>

http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf

¹⁵⁵ Contribution de l'Observatoire des Usages de l'Internet au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnle.pdf>. Page 48 et suivantes.

¹⁵⁶ Directeur général de la société Zalix.

secteur. [...] Les revendeurs, sociétés de services, peuvent donc y trouver matière à développer des affaires, et nous les épaulons en proposant des formations gratuites. Dans leur démarche commerciale, l'important est de faire essayer le produit, pour lutter contre les quelques réticences qui subsistent ». ¹⁵⁷

L'entreprise qui obtiendra le marché dans le cadre du projet INES bénéficiera d'un impact publicitaire à peu de frais. Elle sera plus facilement reconnue du grand public, et disposera d'une carte de visite agréée par l'Etat pourra vendre ses solutions techniques.

La commercialisation des procédés biométriques d'identification peut faire passer au second rang non seulement la question de la protection des données mais aussi la question du niveau de sécurité obtenu. Les entreprises sont dans une logique économique, contrairement à l'Etat. Apparemment tous les moyens sont bons pour faire du profit, et il ne faut pas avoir peur d'enjoliver la réalité pour y arriver.

Qui possède effectivement le pouvoir de décision ? Au vu de ces éléments, l'Etat semble jouer le jeu des entreprises. Cette situation se rapproche du problème posé par la gouvernance de l'internet. C'est à l'ICANN¹⁵⁸ qui revient d'allouer l'espace des adresses de protocole internet, d'attribuer les identificateurs de protocole, de gérer le système de nom de domaine de premier niveau pour les codes génériques (gTLD) et les codes nationaux (ccTLD), et d'assurer les fonctions de gestion du système de serveurs racines. L'ICANN est une association de droit privé à but non lucratif, fondée suite à une directive du Département du Commerce américain, et qui fonctionne toujours sur la base d'un mémorandum avec ce ministère. Le lien n'est donc pas difficile à faire entre le développement de l'internet et l'action des entreprises.

Ce lien existe également en matière de biométrie. Les Etats-Unis jouent un rôle moteur dans le cadre du développement des procédés biométriques d'identification. Comme en matière d'internet, les Etats-Unis privilégient en premier lieu leurs entreprises.

¹⁵⁷ Cf. Olivier WACHE, *Décision distribution*, 25 avril 2005 ; site *01net.com* ; <http://www.01net.com/article/274782.html>

¹⁵⁸ Créée en 1998. Internet Corporation for Assigned Names and Numbers

Au terme de cette première partie de réflexion, nous pouvons nous apercevoir de toute la difficulté de la question de l'introduction des procédés d'identification biométriques. L'usage de ces technologies dépend avant tout de choix politiques (ou économiques) et d'une volonté, toute légitime soit-elle, d'éradiquer les actes déviants.

Le problème aujourd'hui résulte de l'application généralisée de ces procédés. Peu importe notre qualité, simple citoyen, voyageur, administré ou travailleur, le contrôle étatique sera possible à différents moments de notre vie que se soit dans le cadre d'un contrôle policier ou d'une relation de service avec l'administration. A ce contrôle étatique s'ajoutent les contrôles mis en œuvre par des entreprises.

Mais cette banalisation des procédés biométriques d'identification est la source d'effets néfastes. Hors quelques cas particuliers, les individus ne réagissent pas à la mise en place de ces dispositifs¹⁵⁹. Cette non-réaction s'explique justement par l'absence de connaissances sur les procédés biométriques d'identification. Or les données biométriques ne sont pas des données comme les autres. Elles sont liées de façon perpétuelle à une seule et unique personne.

Cette absence de réaction va même plus loin puisque l'individu n'exprime même pas son consentement à la mise en place des procédés biométriques d'identification, mise en place qui devient de ce fait unilatérale. La question est maintenant de savoir si l'individu, s'il n'a pas le choix de la technologie, peut au moins espérer un contrôle adéquat de ses données biométriques.

Face aux dangers inhérents à la technique biométrique d'identification, il est urgent et nécessaire d'élaborer une protection particulière, qui sera à même d'assurer ce contrôle adéquat des données biométriques (Titre second)

¹⁵⁹ Contribution de Monsieur DUBEY au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnief.pdf>. Page 30 et suivantes.

TITRE DEUXIEME. L'URGENCE ET LA NECESSITE D'UNE PROTECTION PARTICULIERE

Des intérêts autres que sécuritaires viennent fausser le débat sur les procédés biométriques d'identification. Ceux-ci sont pourtant très discrets, mais à nos yeux le débat actuel perd toute légitimité. Son unique rôle est d'obtenir l'aval de toute la population, en lui faisant miroiter un semblable de pouvoir de décision, alors que la solution est déjà acquise, tant au niveau international qu'au niveau national.

Il semble impossible aujourd'hui de revenir en arrière, mais pour autant ceci ne signifie pas que les autorités nationales puissent agir sans limite. Elles devront faire avec un corpus législatif, qui est aujourd'hui confronté à la délicate question du niveau de protection à accorder aux données personnelles (Chapitre premier).

Elles devront également faire avec les différents acteurs qui ont pour mission d'appliquer cette législation, bien qu'en l'état actuelle elle soit encore perfectible (Chapitre second).

Chapitre premier : L'adoption d'un corpus législatif : la délicate question du niveau de protection

L'enjeu du niveau de protection des données à caractère personnel est le suivant : une législation trop protectrice ruinerait les prétentions sécuritaires des autorités nationales. Elles doivent donc faire avec une législation élaborée en réponse à un projet de fichage de toute la population qu'elles voulaient mettre en place dans les années 70. Cette législation nationale a été un signal fort, et elle a été reprise au niveau international, toujours dans un souci de protection (Section première).

Les autorités nationales ne peuvent se permettre de revenir ouvertement sur les garanties accordées il y a presque trente ans. Néanmoins, il leur est indispensable de supprimer certaines garanties, et ce dans une logique sécuritaire. Loi après loi, ce sont quelques dispositions qui viennent élargir le champ d'application de textes sécuritaires, au détriment de la protection des données à caractère personnel. Aujourd'hui, l'armada de textes adoptés depuis le début de ce millénaire impose des limites à la législation applicable aux données biométriques, de sorte que la protection de ces données s'en retrouve diminuée (Section seconde).

Section première : Une lente construction dans un souci de protection

Aujourd'hui, la donnée biométrique relève de la loi du 6 janvier 1978, modifiée en 2004. Cette situation est acquise, mais il aura fallu près de 30 ans pour qu'une donnée biométrique soit qualifiée de « donnée personnelle » (Paragraphe premier).

A coté de cette protection générale, les données biométriques peuvent relever de l'application d'autres textes, plus particuliers (Paragraphe second).

Paragraphe premier : La qualification de « donnée personnelle »

En France, la notion de « donnée personnelle » a été introduite avec la loi du 6 janvier 1978¹⁶⁰. Le terme « donnée biométrique » n'apparaît pas expressément. Mais il a été avancé qu'une donnée biométrique peut, dans certains cas particuliers, renseigner sur l'état de santé de la personne concernée¹⁶¹, et doit donc être qualifiée de donnée personnelle.

L'impulsion majeure pour la reconnaissance de la qualification de « donnée personnelle » vient de l'Europe, d'abord du Conseil de l'Europe (A.), puis de l'Union

¹⁶⁰ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 ; JORF du 7 août 2004 ; Disponible sur internet :

<http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm>

http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf

¹⁶¹ Par exemple une maladie de l'œil.

Européenne (B.). Il faut attendre la loi du 6 août 2004¹⁶² (C.) pour que la France reconnaisse la qualification de « donnée à caractère personnel » à la donnée biométrique.

A. La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Cette convention a été signée le 28 janvier 1981, à Strasbourg, par tous les Etats membres du Conseil de l'Europe¹⁶³. Comme la loi française de 1978, la biométrie n'est pas envisagée explicitement.

Il faut donc attendre la publication d'un rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques¹⁶⁴ en 2005. Une des finalités de ce rapport était de démontrer que les principes énoncés dans la convention de 1981 s'appliquaient aux données biométriques.

L'intérêt de ce rapport réside dans le raisonnement juridique qui a amené à l'application de la convention 108.

L'article premier de la convention 108 est ainsi rédigé : « Le but de la présente Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant. » Dans la définition de l'article 2, lettre a, les données à caractère personnel désignent toute information concernant une personne physique identifiée ou identifiable.

Reste à savoir si une donnée biométrique est bien une donnée à caractère personnel. Le rapport reprend les différentes propositions, pour finalement les dépasser. Pour certains, ce n'est pas une donnée à caractère personnel pour deux raisons. D'une part parce qu'une empreinte incomplète est insuffisante pour identifier une personne, et d'autre part parce qu'une donnée biométrique ne comporte en elle-même aucune information sur la personne (excepté les informations sur la santé de la personne¹⁶⁵).

Une donnée biométrique peut être une donnée à caractère personnel. Elle permet par nature d'identifier une personne, dans la mesure où elle peut lui être rattachée de manière unique et permanente.

Plutôt que de trancher un tel débat, le rapport propose une solution beaucoup plus simple : « Le Comité est d'avis qu'il n'est pas nécessaire de décider si les données biométriques sont des données personnelles ou si c'est le cas seulement dans certaines

¹⁶² Loi n°2004-801 du 6 août 2004, modifiant la loi n° 78-17 du 6 janvier 1978 ; JORF du 7 août 2004.

¹⁶³ Convention STCE n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Disponible sur internet : <http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm> (Ci-après la convention n° 108)

¹⁶⁴ Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Rapport : « Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques ». Février 2005. Disponible sur internet : http://www.coe.int/T/F/Affaires_juridiques/Coop%20E9ration_juridique/Protection_des_donn%20es/Documents/Rapports/O-rapport%20biometrie%202005.asp

¹⁶⁵ Nous reprenons l'exemple des maladies de l'œil avec la reconnaissance rétinienne.

circonstances. Il pense que, dès que les données biométriques sont collectées en vue d'un traitement automatisé, la possibilité existe que ces données soient rattachées à une personne identifiable. Dans ce cas, la Convention s'applique ».

Cette protection a été adoptée dans un souci de protection d'une part des personnes (comme l'indique son titre), mais également dans un souci de protection des données¹⁶⁶.

Les principes de bases de la protection des données sont les suivants :

- Sur la qualité des données¹⁶⁷ : elles doivent être traitées loyalement et licitement, collectées pour des finalités déterminées, adéquates et non excessives au regard des finalités pour lesquelles elles ont été collectées, exactes et si nécessaire mises à jour, conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités.
- Sur les catégories particulières de données¹⁶⁸ : le traitement direct des données sensibles (origine raciale, opinions politiques, convictions religieuses, état de santé, vie sexuelle) est interdit, sauf si les Etats prévoient des garanties.
- Sur la sécurité des données¹⁶⁹ : le responsable de traitement se doit de prendre les « mesures de sécurité appropriées » pour empêcher toute modification ou destruction des données, ainsi que tout accès par un tiers non autorisé.
- Sur les garanties complémentaires pour la personne concernée¹⁷⁰ : elle doit être informée de l'existence du traitement. Elle doit disposer d'un droit d'accès et de modification.
- Sur les exceptions aux principes¹⁷¹ : elles sont possibles uniquement quand elles sont nécessaires à la protection de la sécurité de l'Etat, à la sûreté publique, aux intérêts monétaires de l'Etat ou à la répression des infractions pénales ou bien à la protection de la personne concernée.
- Sur les sanctions¹⁷² : les Etats membres sont libres de choisir les sanctions.

L'entrée en vigueur de cette convention était subordonnée au consentement de cinq Etats d'être liés par ce texte. Elle est entrée en vigueur le 10 janvier 1985. En France, la loi du 6 janvier 1978 énonçait déjà les principes de base. La transposition du texte européen s'est donc faite plus que rapidement.

B. La directive n° 95/46/CE 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

L'autre texte international de référence en matière de protection des données est la directive n° 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.

¹⁶⁶ Article 4-1 de la convention 108, précitée : « Chaque Partie prend, dans son droit interne, les mesures nécessaires pour donner effet aux principes de base pour la protection des données énoncés dans le présent chapitre »

¹⁶⁷ Article 5 de la convention 108, précitée

¹⁶⁸ Article 6 de la convention 108, précitée

¹⁶⁹ Article 7 de la convention 108, précitée

¹⁷⁰ Article 8 de la convention 108, précitée

¹⁷¹ Article 9 de la convention 108, précitée

¹⁷² Article 10 de la convention 108, précitée

Elle a été complétée par la directive n° 97/66/CE¹⁷³ 15 décembre 1997, qui sera abrogée et remplacée par la directive 2002/58/CE¹⁷⁴ du 12 juillet 2002, communément dénommée directive vie privée et communication électroniques.

Comme pour la convention 108 du Conseil de l'Europe, le terme biométrie n'apparaît pas expressément, que ce soit dans la directive n° 95/46/CE ou bien dans la directive n° 2002/58/CE. Mais cette absence n'empêche nullement l'application des textes communautaires, notamment en raison de leur effet direct vertical. Rappelons que les directives communautaires ont pour seuls destinataires les Etats membres qui sont tenus de les transposer dans leurs ordres juridiques internes. En principe, ce ne sont donc pas les dispositions des directives qui sont directement invoquées par les particuliers devant les juridictions nationales, mais les mesures nationales de transposition. Toutefois, les particuliers peuvent se prévaloir directement devant le juge national des droits que leur confèrent les dispositions d'une directive non transposée ou mal transposée à condition que le contenu des dispositions concernées soit inconditionnel et suffisamment clair et précis¹⁷⁵.

Si le droit national n'est pas conforme aux prescriptions de la directive invoquée, le juge interne écarte la disposition nationale non conforme et la remplace directement par la disposition de la directive (invocabilité d'exclusion) ; si aucune mesure de transposition n'a été prise, le juge interne applique directement les dispositions de la directive (invocabilité de substitution).

Néanmoins, l'effet direct reconnu aux directives par la Cour de justice est restreint : il ne peut être que vertical dans la mesure où les directives, en elles-mêmes, ne créent pas d'obligations vis à vis des particuliers. Elles ne peuvent donc être invoquées ni dans le cadre de litiges entre particuliers (absence d'effet horizontal¹⁷⁶ : arrêts du 26 février 1986, MARSHALL et du 14 juillet 1994, Paola Facini DORI) ni par les autorités nationales contre un particulier¹⁷⁷ (absence d'effet vertical inversé : arrêt du 5 avril 1979, RATTI, 148/78).

Dans la mesure où les applications biométriques permettent l'identification des personnes¹⁷⁸, les directives communautaires s'appliquent. L'article 2 a) de la directive de 1995 définit « les données à caractère personnel » comme toute information concernant une personne physique identifiée ou identifiable. La personne peut être identifiée par des éléments spécifiques propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

¹⁷³ Directive n° 97/66/CE du Parlement Européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Disponible sur internet : <http://europa.eu.int/ISPO/legal/fr/dataprot/protection.html>

¹⁷⁴ Directive 2002/58/CE du Parlement Européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Disponible sur internet : http://europa.eu.int/eur-lex/pri/fr/oj/dat/2002/l_201/l_20120020731fr00370047.pdf

¹⁷⁵ CJCE, 4 décembre 1974, Van Duyn, 41/74. Disponible sur internet : http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=fr&numdoc=61974J0041

¹⁷⁶ CJCE, 26 février 1986, Marshall, 152/84. Disponible sur internet : http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&numdoc=61984J0152&lg=fr

¹⁷⁷ CJCE, 5 avril 1979, Ratti, 148/78. Disponible sur internet : http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&lg=fr&numdoc=61978J0148

¹⁷⁸ GUERRIER, Claudine. « Protection des données personnelles et application biométriques en Europe ». *Communication - Commerce électronique*, juillet - août 2003 : pages 17 à 22.

Les données biométriques sont en relation étroite et constante avec l'identité physique et physiologique des individus. Ainsi elles doivent respectées les principes énoncés dans la directive.

- Sur la qualité des données¹⁷⁹ : la directive reprend la convention 108¹⁸⁰ du Conseil de l'Europe, en ajoutant des exceptions pour les traitements à des fins historiques, statistiques ou scientifiques.
- Sur les traitements portant sur des catégories particulières de données¹⁸¹ : les traitements de données dites sensibles¹⁸² sont en principe interdits. Des exceptions sont prévues, et les Etats membres peuvent apporter des dérogations supplémentaires pour un motif d'intérêt public important¹⁸³.
- Sur la sécurité des données¹⁸⁴ : la directive est plus précise que la convention n° 108 puisque que les mesures appropriées sont des mesures techniques et d'organisation.
- Sur les garanties complémentaires pour la personne concernée : la personne concernée doit être informée de l'existence du traitement¹⁸⁵, et disposer d'un droit d'accès et de rectification¹⁸⁶ et d'un droit d'opposition¹⁸⁷.
- Sur les exceptions et les limitations aux principes¹⁸⁸ : ce sont les mêmes que celles énoncées dans la convention n° 108.
- Sur les sanctions¹⁸⁹ : les Etats membres sont libres de choisir les sanctions, dans la mesure où elles assurent la pleine application de la directive.

C. La législation française

C'est avec la loi du 6 janvier 1978 que la France entre dans l'ère de la protection des données personnelles. Si nous reprenons le même raisonnement que nous avons eu pour la convention n° 108 et pour les directives communautaires, les données biométriques sont des données personnelles, et leur traitement doit respecter certains principes.

La donnée biométrique ne fera son entrée dans la loi « Informatique et Libertés » qu'avec la loi du 6 août 2004, qui modifiera le cadre juridique général (2/) afin de prendre en considération l'évolution de la société. Mais entre 1978 et 2004, plusieurs législations sectorielles seront adoptées (1/)

1/ D'un cadre juridique sectoriel

¹⁷⁹ Article 6 de la directive n° 95/46/CE, précitée

¹⁸⁰ « Les données doivent être traitées loyalement et licitement, collectées pour des finalités déterminées, adéquates et non excessives au regard des finalités pour lesquelles elles ont été collectées, exactes et si nécessaire mises à jour, conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités »

¹⁸¹ Article 8 de la directive n° 95/46/CE, précitée

¹⁸² Ce sont des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.

¹⁸³ Article 8-4 de la directive n° 95/46/CE, précitée

¹⁸⁴ Article 17 de la directive n° 95/46/CE, précitée

¹⁸⁵ Articles 10 et 11 de la directive n° 95/46/CE, précitée

¹⁸⁶ Article 12 de la directive n° 95/46/CE, précitée

¹⁸⁷ Article 14 de la directive n° 95/46/CE, précitée

¹⁸⁸ Article 13 de la directive n° 95/46/CE, précitée

¹⁸⁹ Article 10 de la directive n° 95/46/CE, précitée

Durant un peu plus de 25 années, le droit interne n'a proposé qu'un encadrement sectoriel de la biométrie. Il n'y avait pas de cadre juridique spécifique à la biométrie mais plutôt un encadrement de certains procédés biométriques. Néanmoins, les données acquises par le biais de la biométrie relèvent du cadre juridique relatif aux traitements informatisés des données personnelles tel que prévu par la loi « Informatique et Libertés » du 6 janvier 1978, comme nous l'avons vu précédemment.

Nous ne traiterons que de la législation relative au procédé biométrique des empreintes digitales. Différents textes ont été adoptés pour encadrer plusieurs traitements.

- Le décret du 8 avril 1987¹⁹⁰ relatif au Fichier Automatisé des Empreintes digitales¹⁹¹ (FAED), géré par le ministère de l'Intérieur, instaure un traitement automatisé des empreintes digitales et des traces prélevées dans le cadre d'une enquête (flagrance ou préliminaire) à des fins probatoires et/ou d'identification ainsi que des empreintes des détenus prélevées dans les établissements pénitenciers à des fins d'identification (et de preuve en cas de récidive).
- Par l'arrêté du 21 décembre 1989¹⁹², abrogé et remplacé par l'arrêté du 6 novembre 1995¹⁹³, le ministère des Affaires Etrangères a autorisé la création permanente d'un fichier informatisé des empreintes digitales des demandeurs du statut de réfugié sous l'autorité de l'OFPRA.
- Par l'arrêté du 21 décembre 2001¹⁹⁴, le ministère de l'Education Nationale a autorisé la création au rectorat de l'académie de Lille d'un traitement automatisé d'informations nominatives ayant pour finalité le contrôle de l'accès à certains locaux du rectorat par la reconnaissance des empreintes digitales de personnels spécialement habilités.

Ces textes sont spécifiques et encadrent des traitements particuliers. Ils ont néanmoins été élaborés dans le respect de la loi du 6 janvier 1978, qui crée un cadre général de protection des données personnelles.

2/ A un cadre juridique général

Avec la modification de la loi du 6 janvier 1978 par la loi du 6 août 2004, la donnée biométrique est expressément qualifiée de donnée à caractère personnel¹⁹⁵. Par conséquent la mise en œuvre d'un traitement automatisé¹⁹⁶ de données biométriques doit respecter quatre principes :

¹⁹⁰ Décret n° 87-249 du 8 avril 1987, relatif au fichier automatisé des empreintes digitales géré par le ministère de l'Intérieur. JORF du 9 avril 1987. <http://www.legifrance.gouv.fr/texteconsolide/PPHEP.htm>

¹⁹¹ Cf. Titre I, Chap I, Section I, §2, B

¹⁹² Disponible sur legifrance : <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=MAEF8910053A>

¹⁹³ Disponible sur legifrance : <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=MAEF9510027A>

¹⁹⁴ Disponible sur legifrance : <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=MEND0102798A>

¹⁹⁵ Article 2 : 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.

¹⁹⁶ Rappel : est un traitement de données à caractère personnel « toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou tout autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction » (article 2, alinéa 3 loi « informatique et libertés »).

- le principe de finalité (les données collectées doivent être recueillies pour une finalité précise) ;
- le principe de proportionnalité (la mise en œuvre du traitement ne doit pas être incompatible avec ses finalités) ;
- le caractère « adéquat, pertinent et non excessif » des données collectées eu égard aux finalités pour lesquelles ces données sont collectées ;
- le respect des obligations imposées au responsable du traitement (information des personnes concernées, informations sur les destinataires des données collectées, information, sur la durée raisonnable de conservation des données).

L'expression « donnée biométrique » apparaît :

- à l'article 25-I 8° : « Les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes. » ;
- à l'article 27-I 2° : « Les traitements de données à caractère personnel mis en œuvre pour le compte de l'Etat qui portent sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes. ».

Avec ces deux articles, le traitement de donnée biométrique est soumis au régime le plus contraignant prévu par la loi « Informatique et Libertés », celui de l'autorisation. Néanmoins, de tels traitements mis en œuvre pour le compte de l'Etat ne peuvent être créés que par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission Nationale de l'Informatique et des Libertés.

Le traitement de données biométriques doit respecter certains principes pour être licites. Ces principes n'ont pas changé depuis la loi de 1978, et ce sont les mêmes que ceux énoncés dans la convention n° 108 et les directives communautaires.

Paragraphe second : Les autres législations applicables aux données biométriques

Un traitement de données à caractère personnel, pour être mis en œuvre, ne doit pas seulement respecter les prescriptions de la loi « Informatique et Libertés ». A côté de cette législation générale, d'autres plus spécifiques trouvent matière à s'appliquer, soit parce que leurs principes sont repris, comme c'est le cas pour la protection de la vie privée (A.), soit parce qu'elles imposent plus de conditions de mise en œuvre, telle que la présomption d'innocence (B.) et l'information et la consultation des salariés (C.)

A. La protection de la vie privée

Le droit au respect de la vie privée est protégé sur le plan droit international¹⁹⁷ et par le droit interne français. L'apparition de la notion de vie privée est d'ailleurs récente puisqu'elle date d'une loi du 17 juillet 1970. Ce texte a inséré dans le Code civil un article 9 qui dispose : « Chacun a droit au respect de sa vie privée ».

La valeur constitutionnelle de ce droit de la personnalité a fait l'objet de vifs débats mais trois décisions du Conseil constitutionnel¹⁹⁸ ont donné à cet article toute sa force. Les

¹⁹⁷ Voir notamment : article 12 de la Déclaration universelle des droits de l'Homme (DUDH) ; article 17 du Pacte international des Nations Unies ; article 8 de la Convention Européenne des droits de l'Homme (CEDH).

¹⁹⁸ Décis. Cons. const. n° 94-352 DC du 18 janvier 1995 relative à la loi d'orientation et de programmation relative à la sécurité. <http://www.conseilconstitutionnel.fr/decision/1994/94352dc.htm>

sages ont ainsi déclaré en substance que le respect de la vie privée était rattaché au principe de la liberté individuelle au sens de l'article 66 de la Constitution et de la déclaration des droits de l'homme et du citoyen. La question de la liberté individuelle des individus est donc intimement liée à la protection de ce droit à la vie privé.

La vie privée est ce qui est « digne d'être protégée » par opposition à la vie publique. La vie privée est ce qui doit demeurer caché, à l'abri de la curiosité. L'analyse de la jurisprudence montre que les juges ont largement interprété les dispositions de l'article 9 du Code civil en l'occurrence en matière de photographies attentatoires au droits de la personnalité allant jusqu'à instituer une sorte de « responsabilité sans faute d'un hébergeur »¹⁹⁹.

La protection de la vie privée est soumise à dure épreuve avec l'explosion des technologies de l'information et de la communication. En raison du danger que l'informatique pouvait constituer vis-à-vis de la protection de la vie privée, le législateur a déclaré dans l'article premier de la loi relative « Informatique et Libertés » que « l'informatique ne doit porter atteinte ni à l'identité humaine (...) ni à leur vie privée ». La loi prévoit surtout que toute création de fichier doit être autorisée par la CNIL et que les fichiers doivent rester indépendants les uns par rapport aux autres. Le but est d'éviter que par un recoupement des informations contenues dans des fichiers, l'on parvienne à un fichage généralisé de tous les citoyens. La protection de la vie privée impose également que les informations ne soient pas collectées de manière frauduleuse déloyale ou illicite (d'où l'existence d'une procédure de déclaration des traitements).

Or le problème est tel que, à l'heure actuelle, différentes méthodes sont déjà utilisées pour recueillir des données personnelles. Le risque de profilage des personnes (déjà existant) serait d'autant plus attentatoire aux droits de l'Homme qu'il aurait un fondement biologique. Un portrait complet de ce que l'individu peut être au sens biologiques du terme.

B. La présomption d'innocence

La présomption d'innocence est un concept largement entendu et non une véritable présomption procédurale. Le concept de la présomption d'innocence est codifié par la loi n° 93-2 du 4 janvier 1993²⁰⁰ au sein du code civil et par la loi n° 2000-516 du 15 juin 2000²⁰¹ renforçant la présomption d'innocence et les droits des victimes.

Décis. Cons. const. n° 99-416 DC du 23 juillet 1999 relative à la loi portant création d'une couverture maladie universelle. <http://www.conseil-constitutionnel.fr/decision/1999/99416/99416dc.htm>

Décis. Cons. const. n° 99-419 DC du 9 novembre 1999 relative à la loi relative au pacte civil de solidarité. <http://www.conseil-constitutionnel.fr/decision/1999/99419/99419dc.htm>

¹⁹⁹ Cf. article de monsieur CHATILLON à propos de l'affaire Estelle Hallyday (CA Paris 10/02/99) ; site de la bibliothèque du DESS droit de l'internet administration et entreprises ; Rapport *Les données personnelles : enjeux juridiques et perspectives* ; IDT juin 1999 ; disponible sur la bibliothèque numérique du DESS droit de l'internet, Administration, Entreprises

http://dess-droit-internet.univ-paris1.fr/bibliotheque/article.php3?id_article=101&var_recherche=donn%C3%A9e+personnelles

²⁰⁰ Loi n° 93-2 du 4 janvier 1993 portant réforme de la procédure pénale. JORF du 5 janvier 1993. Disponible sur internet : <http://www.legifrance.gouv.fr/texteconsolide/PJEB0.htm>

²⁰¹ Loi n° 2000-516 du 15 juin 2006 renforçant la protection de la présomption d'innocence et les droits des victimes. JORF du 16 juin 2000. Disponible sur internet : <http://www.legifrance.gouv.fr/texteconsolide/PJEDG.htm>

Cependant, la notion pré-existait au sein de l'article 9 de la Déclaration des Droits de l'Homme et du Citoyen : « Tout homme étant présumé innocent jusqu'à ce qu'il ait été déclaré coupable, s'il est jugé indispensable de l'arrêter, toute rigueur qui ne serait pas nécessaire pour s'assurer de sa personne doit être sévèrement réprimée par la loi ». Le Conseil Constitutionnel a d'ailleurs proclamé que le droit au respect de la présomption d'innocence avait valeur constitutionnelle²⁰² et a expressément visé l'article 9 précité pour réaffirmer la valeur du principe²⁰³.

A l'instar de l'article 9 du code civil affirmant le droit au respect de la vie privée, l'article 9-1 instaure un droit à l'honneur et au respect de la réputation. Ce droit existe indépendamment d'une future reconnaissance de culpabilité ou d'innocence. La personne poursuivie pourra ainsi protéger son honneur et sa réputation contre les tiers, par exemple la presse.

C'est pourquoi, la biométrie, par sa nature même, appréhende les individus à des fins d'identification en-dehors de toute problématique quant à leur comportement, contraire à l'ordre public ou non. Dès lors, nous pouvons nous demander si la finalité du procédé ne risque pas d'être détournée pour des objectifs moins nobles au regard de l'innocence de chaque individu : à titre d'exemple, quid de la tentation des services de police de fichier les personnes recherchées mais aussi des personnes connues des services à des fins de prévention ?

La présomption d'innocence n'est-elle pas susceptible d'être remise en cause par le risque d'automatisation de la condamnation suite à la comparaison par les services de police entre l'empreinte prélevée et les autres fichiers de police ?

C'est pourquoi, une méthode biométrique renverse le principe de l'innocence à partir du moment où elle intervient en amont d'une procédure et qu'elle sert à elle seule à déterminer l'innocence ou la culpabilité de sa cible.

C. L'application du droit du travail

Une décision du Tribunal de Grande Instance de Paris²⁰⁴ est venue nous rappeler que le droit du travail s'appliquait également en matière de traitement des données personnelles des salariés.

Le comité d'entreprise et le syndicat Sud rail ont saisi le juge judiciaire pour obtenir l'interdiction d'installation d'une badgeuse biométrique mise en place par la société Effia Services. Cette décision est importante à plusieurs égards D'une part les demandeurs se sont fondés sur trois articles du Code du Travail (les articles L. 120-2, L. 121-8 et L. 432-2-1), et d'autre part il nous faut noter que le responsable du traitement avait réalisé les formalités préalables²⁰⁵ auprès de la CNIL.

²⁰² Décis. Cons. const. n° 80-127 du 19-20 janv. 1980

²⁰³ Décis. Cons. const. n° 89-258 DC du 8 juillet 1989 relative à la loi portant amnistie. <http://www.conseil-constitutionnel.fr/decision/1989/89258dc.htm>

²⁰⁴ TGI Paris, 1^{ère} chambre, section sociale, 19 avril 2005, CE d'Effia Services, Syndicat Sud Rail / Effia Services (RG n°05/00382) ; Disponible sur www.juriscom.net/documents/tgiparis20050419.pdf

²⁰⁵ Formalités imposées par la loi n° 78-17 du 6 janvier 1978 non modifiée (cf. infra Titre 2, Chapitre 2, Section 1, § 2, C.)

Aux termes de l'article L. 121-8 du Code du Travail, « aucune information concernant personnellement un salarié [...] ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié [...] ». L'obligation d'information préalable existe donc, dès lors que l'employeur collecte des informations sur un travailleur, quelque soit le procédé utilisé. L'information donnée aux salariés étant individuelle, elle peut prendre la forme d'une note distribuée à l'ensemble des salariés ou d'un courrier individuel, comme en l'espèce.

En application de l'article L. 432-2-1 du Code du Travail, le comité d'entreprise est obligatoirement informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel, mais également consulté avant toute installation de techniques permettant un contrôle de l'activité des salariés. Cet avis est purement consultatif et ne lie pas l'employeur. La saisine du comité doit avoir lieu dès lors que le dispositif rend possible la surveillance des salariés. L'absence de consultation du comité d'entreprise autorise ce dernier à saisir le tribunal correctionnel pour délit d'entrave, sanctionné d'un an d'emprisonnement et/ou 3 750 euros d'amende²⁰⁶. L'employeur avait respecté son obligation d'information et de consultation.

Mais le dispositif voulu par l'employeur sera condamné par les juges, en application de l'article L. 120-2, qui dispose que « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ». La biométrie, mettant en cause le corps humain et portant ainsi atteinte aux libertés individuelles, peut se justifier uniquement lorsqu'elle a « une finalité sécuritaire ou protectrice de l'activité exercée dans des locaux identifiés ».

Malheureusement, cette législation de protection souffre de quelques limites, de sorte que la protection accordée s'en trouve nettement diminuée.

Section seconde : Les limites de la législation actuelle : une protection amoindrie

Il aura donc fallu un peu plus de 25 années pour arriver à la protection que nous connaissons aujourd'hui. Nous pouvons dès maintenant affirmer que ce laps de temps est très long, comparé à l'évolution rapide des nouvelles technologies, à l'instantanéité permise par l'informatique.

Mais depuis peu, il semble que ce soit le processus inverse qui prenne le pas, à savoir une diminution de cette protection. La nouvelle mouture de la loi « Informatique et Libertés », bien qu'elle inclut aujourd'hui les traitements mis en œuvre par les personnes publiques, souffre de quelques faiblesses. D'une part, les pouvoirs publics ont la possibilité de sortir des sentiers battus avec la porte dérobée de la sécurité publique (Paragraphe premier), d'autre part la portée du droit d'accès est plus que limitée en matière de biométrie (Paragraphe deuxième).

Cette loi, qui instaure un climat juridique de protection des données, se retrouve également confrontée à des textes dits sécuritaires, dont la finalité est de permettre aux

²⁰⁶ Article L. 483-1 du Code du Travail

services de police d'accéder et d'exploiter des données. Il s'agit de la loi pour la sécurité intérieure (Paragraphe troisième).

Paragraphe premier : La sécurité publique comme une porte dérobée

La directive communautaire 95/46/CE²⁰⁷ a exclu, par son article 3, de son champ d'application les traitements de données à caractère personnel ayant pour objet la sécurité publique, la défense et la sûreté de l'Etat et son seizième considérant précise que les traitements des sons et images par vidéosurveillance n'entrent pas dans le champ d'application de la directive s'ils sont mis en œuvre « à des fins de sécurité publique, de défense, de sûreté de l'Etat ou de droit pénal ».

Les conditions juridiques d'utilisation des dispositifs biométriques nationaux utilisés à ces fins relèvent donc de la compétence de chaque Etat²⁰⁸. En France, ces conditions sont définies par la loi n° 78-17 du 6 janvier 1978, modifiée le 6 août 2004. La loi de 1978 comporte certaines dérogations en faveur des traitements mis en œuvre à des fins de sécurité.

D'une part, des dérogations sont prévues au principe de publicité lorsque les traitements concernent « la sûreté de l'Etat, la défense et la sécurité publique » ou ont pour finalité « la prévention, la recherche, la constatation ou la poursuites d'infractions pénales ». L'article 26-III dispose ainsi que certains de ces traitements peuvent être dispensés, par décret en Conseil d'Etat, de la publication de l'acte réglementaire qui les autorise. Ne sera oublié avec ce décret que le sens de l'avis de la CNIL²⁰⁹.

Néanmoins, les dispositions de l'article 30 restent pleinement applicables à de tels traitements. La demande d'avis doit toujours comporter les mentions obligatoires²¹⁰ qui visent notamment les finalités du traitement, les catégories de données à caractère personnel traitées, leur durée de conservation. Par ailleurs l'article 31 met à la charge de la CNIL l'obligation de tenir à la disposition du public la liste des traitements déclarés ou autorisés, à l'exception de ceux de l'article 26-III.

D'autre part, des dispositions dérogatoires limitent les droits des personnes dont les données font l'objet de traitements liés à la sécurité. L'article 38 qui pose le principe que toute personne a le droit de s'opposer pour des raisons légitimes à la collecte de données la

²⁰⁷ Directive n° 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. Disponible sur internet : <http://europa.eu.int/ISPO/legal/fr/dataprot/directiv/direct.html>

²⁰⁸ Certains principes ont été définis au niveau du Conseil de l'Europe en 1987 – Recommandation n° R (87) 15 du Comité des Ministres aux Etats membres visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police adoptée le 17 septembre 1987.

Les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel adoptées par l'OCDE le 23 septembre 1980 reconnaissent pour leur part la possibilité de déroger aux principes qu'elles définissent dans les domaines ressortissant de la souveraineté nationale, de la sécurité nationale et de l'ordre public, tout en précisant que ces exceptions devraient être aussi peu nombreuses que possible et portées à la connaissance du public

²⁰⁹ Une telle dérogation n'a été utilisée que pour les « services secrets ». Le décret du 7 mars 1986 dispose que « ne seront pas publiés les actes réglementaires relatifs aux fichiers gérés par la direction de la surveillance du territoire, la direction générale de la sécurité extérieure, et par la direction de la protection et de la sécurité de la défense ». Source : MARTIN, David. Les fichiers de police. Paris : Editions Presse Universitaire de France, 1999 » - Juin 1999.

²¹⁰ Mentions énumérées à l'article 30 de la loi n° 78-17 du 6 janvier 1978.

concernant exclut certains traitements limitativement désignés²¹¹. De même, l'article 32-V, qui définit le droit pour les personnes concernées à être informées, précise que ses dispositions ne s'appliquent pas à la collecte des données recueillies dans certaines conditions²¹² et «utilisées lors d'un traitement mis en œuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté [...] ». De plus, l'article 32-VI exclut de son champ d'application les traitements de données dont la finalité est « la prévention, la recherche, la constatation ou la poursuites d'infractions pénales ».

Enfin, l'article 41 définit une procédure particulière d'accès indirect et de rectification pour les traitements relatifs à « la sûreté de l'Etat, la défense et la sécurité publique ».

En résumé, la loi « Informatiques et libertés », dans sa rédaction après la modification du 6 août 2004, reprend en fait la rédaction retenue lors de l'adoption de la loi sur la sécurité intérieure.

Paragraphe deuxième : La portée d'un droit d'accès et de modification en matière de données biométriques.

S'il est un domaine où les données biométriques posent des problèmes techniques particuliers au regard de la protection des données personnelles, c'est bien celui des conditions d'exercice du droit d'accès ou de modification.

L'article 12 de la directive pose le principe de la « communication, sous forme intelligible, des données faisant l'objet des traitements ». Il reconnaît à la personne concernée le droit de prendre « connaissance de la logique qui sous-tend tout traitement automatique des données la concernant », au moins dans le cas où des décisions individuelles automatiques produisant des effets juridiques à son égard ou l'affectant de manière significative, sont prises sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, le quarante et unième considérant prenant soin de préciser que ce droit ne doit pas porter atteinte au secret des affaires, ni à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel mais que cela ne doit toutefois pas aboutir au refus de toute information de la personne concernée. La directive prévoit également la rectification, le verrouillage et l'effacement des données incomplètes ou inexactes.

La loi du 6 janvier 1978 reconnaissait à toute personne justifiant de son identité un droit d'interrogation et de communication « en langage clair » et posait le principe de la rectification, de la mise à jour et de l'effacement des informations inexactes, équivoques, périmées.

Avec la transposition de la directive par la loi du 6 août 2004, la communication des données à caractère personnel doit se faire « sous une forme accessible »²¹³. De ce point de vue, les techniques biométriques peuvent susciter quelques difficultés, dans la mesure où la

²¹¹ Article 38 al 3 de la loi n° 78-17, précitée : « [...] lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement. »

²¹² Article 32-III de la loi n° 78-1, précitée : « Lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée [...] »

²¹³ Article 39-I 4° de la loi n° 78-17, précitée

donnée n'est pas nécessairement conservée sous une forme visuellement reconnaissable. En effet, l'image numérisée de l'empreinte digitale n'est pas conservée telle quelle. Il serait alors très facile pour quelqu'un de fabriquer une fausse empreinte digitale à partir de cette image.

L'image le plus souvent est réduite à un gabarit, c'est-à-dire que seul un certain nombre de minuties est conservé. Mais cette compression se fait avec perte, de sorte qu'il est impossible de revenir à l'image de départ. Par conséquent, la communication de cette donnée biométrique ne peut plus se faire « sous une forme intelligible ».

La solution réside dans un droit d'accès direct, de façon à ce que la personne intéressée soit présente pour contrôler si les empreintes enregistrées sont bien les siennes. Dans l'hypothèse d'une inexactitude, la personne concernée pourra demander au responsable du traitement de mettre à jour son fichier.

Quid de certains fichiers, comportant des données biométriques, mais pour lesquels seul un accès indirect²¹⁴ a été reconnu ?

Paragraphe troisième : la loi sur la sécurité intérieure : l'ennemi du principe de finalité

La loi n° 2003-239 du 18 mars 2003²¹⁵, contient des dispositions qui réduisent la portée du principe de finalité énoncé dans la loi « Informatique et Libertés » du 6 janvier 1978. Le principe de finalité est un éléments cadre de la législation sur la protection des données. Si nous nous référons à l'article 6 de la loi « Informatique et Libertés », nous nous apercevons que le système est fondé sur les finalités du traitement. Ainsi :

- « [Les données] sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités. »
- « [Les données] sont adéquates, pertinentes et non excessives au regard des finalités... »
- « [Les données] sont exactes, complètes et, si nécessaires, mises à jour ; les mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées »
- « [Les données] sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités ... »

Les données doivent donc être collectées et utilisées dans des finalités précises. Il est normalement impossible d'utiliser des données pour des finalités différentes de celles pour lesquelles elles ont été collectées, mais la loi « Informatique et Libertés » contient quelques dérogations. Outre le cas du traitement ultérieur de données à des fins statistiques ou à des

²¹⁴ Article 41 de la loi n° 78-17, précitée : « Par dérogation aux articles 39 et 40, lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, le droit d'accès s'exerce dans les conditions prévues par le présent article pour l'ensemble des informations qu'il contient.

La demande est adressée à la commission qui désigne l'un de ses membres appartenant ou ayant appartenu au Conseil d'État, à la Cour de cassation ou à la Cour des comptes pour mener les investigations utiles et faire procéder aux modifications nécessaires. Celui-ci peut se faire assister d'un agent de la commission. Il est notifié au requérant qu'il a été procédé aux vérifications. »

²¹⁵ Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure ; JORF du 19 mars 2003 ; Disponible sur internet : <http://www.legifrance.gouv.fr/texteconsolide/PPED1.htm>

fins de recherche scientifique ou historique²¹⁶, la CNIL peut autoriser « les traitements ayant pour objet :

- l'interconnexion de fichiers relevant d'une ou plusieurs personnes morales gérant un service public et dont les finalités correspondent à des intérêts publics différents ;
- l'interconnexion de fichiers relevant d'autres personnes et dont les finalités principales sont différentes. »²¹⁷

Jusqu'à l'intervention de la loi sur la sécurité intérieure, seul l'article 78-3 du Code de Procédure Pénale et les articles consacrés au fichier national des empreintes génétiques faisaient clairement allusion au « prélèvement » de données biométriques sur les personnes.

L'article 78-3 relatif aux contrôles, vérifications et relevés d'identité dispose ainsi que « si la personne interpellée maintient son refus de justifier de son identité ou fournit des éléments d'identité manifestement inexacts, les opérations de vérification peuvent donner lieu, après autorisation du procureur de la République ou du juge d'instruction, à la prise d'empreintes digitales ou de photographies lorsque celle-ci constitue l'unique moyen d'établir l'identité de l'intéressé » et précise que « la prise d'empreintes ou de photographies doit être mentionné et spécialement motivée dans le procès verbal », l'article 78-5 édictant une peine à l'encontre des personnes refusant de se prêter aux prises d'empreintes digitales ou de photographies autorisées par le procureur de la République ou le juge d'instruction.

S'agissant des empreintes génétiques, jusqu'à l'intervention de la loi n° 2001-1062 du 15 novembre 2001 qui a défini une peine à l'encontre des personnes définitivement condamnées pour une des infractions visées qui refuseraient de se soumettre à un prélèvement biologique destiné à permettre l'analyse d'identification de leur empreinte génétique, un doute planait quant à la possibilité de procéder à un tel prélèvement sans le consentement de la personne, la CNIL ayant exposé les termes du problème dans son rapport d'activité de 1999.

La loi du 18 mars 2003 relative à la sécurité intérieure apporte sur ces questions une clarification importante en autorisant, dans le cadre des enquêtes de flagrance, des enquêtes préliminaires et au cours de l'information judiciaire les « opérations de prélèvements externes nécessaires à la réalisation d'examen techniques et scientifiques de comparaison avec les traces et indices prélevés pour les nécessités de l'enquête » ainsi que « les opérations de signalisation nécessaires à l'alimentation et à la consultation des fichiers de police selon les règles propres à chacun de ces fichiers », le refus de se soumettre aux opérations de prélèvement étant puni d'un an d'emprisonnement et de 15 000 euros d'amende.

S'agissant des personnes concernées, la loi vise celles susceptibles de fournir des renseignements sur les faits en cause, c'est-à-dire les témoins, ainsi que celles à l'encontre desquelles il existe une ou plusieurs raisons plausibles de soupçonner qu'elles ont commis ou tenté de commettre l'infraction.

Les dispositions législatives ou réglementaires afférentes aux fichiers particuliers définissent elles-mêmes des règles relatives notamment aux finalités et aux conditions d'accès de certaines personnes habilitées et des personnes concernées. Les finalités sont nécessairement déterminées de façon assez large.

²¹⁶ Article 6 2° de la loi n° 78-17, précitée

²¹⁷ Article 25-I 5° de la loi n° 78-17, précitée

Ainsi, le fichier d'empreintes digitales (FAED) a été constitué « en vue de faciliter la recherche et l'identification, par les services de la police nationale et de la gendarmerie nationale, des auteurs de crimes et de délits et de faciliter la poursuite, l'instruction et le jugement des affaires dont l'autorité judiciaire est saisie ».

Le fichier des empreintes génétiques (FNAEG) est ainsi « destiné à centraliser les empreintes génétiques issues des traces biologiques ainsi que les empreintes génétiques des personnes condamnées pour l'une des infractions mentionnées à l'article 706-55 (du code de procédure pénale) en vue de faciliter l'identification et la recherche des auteurs de ces infractions ».

Si nous nous référons à cet article, nous pouvons nous apercevoir qu'à la finalité prévue dès l'origine²¹⁸, différentes lois ont apporté quelques élargissements inquiétants. La loi du 15 novembre 2001²¹⁹ relative à la sécurité quotidienne a inclus dans le FNAEG les données génétiques des condamnés pour atteintes graves aux personnes. Puis la loi du 18 mars 2003²²⁰ sur la sécurité intérieure, a marqué une nouvelle étape dans l'extension du fichier. Il peut désormais être sollicité pour la quasi-totalité des crimes et délits d'atteintes aux personnes et aux biens (vols, destructions, coups et blessures volontaires, etc.) et pour les trafics (drogue, proxénétisme, exploitation de la mendicité). Les profils des condamnés sont gardés quarante ans. Le FNAEG peut également intégrer et conserver pendant vingt cinq années le profil génétique de personnes simplement "mises en cause" lors d'une enquête.

Selon le journal Le Monde²²¹, le ministère de l'Intérieur se serait fixé comme objectif pour 2006 de collecter 400 000 profils génétiques par an. De quoi aboutir rapidement au profilage de toute la population française.

Ces dispositions peuvent ainsi comporter des règles spécifiques. Ainsi par exemple, le décret du 8 avril 1987 relatif au fichier d'empreintes digitales énonce le principe selon lequel « aucune interconnexion, rapprochement ou aucune forme de mise en relation avec un autre traitement automatisé d'informations nominatives » n'est autorisé.

Mais la loi permet également aux services de police de saisir des données informatiques.

- L'article 60-1 du Code de Procédure Pénale permet à l'officier de police judiciaire de « requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des documents intéressant l'enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives [...] ».
- L'article 60-2 du Code de Procédure Pénale permet à l'officier de police judiciaire de demander aux organismes publics ou aux personnes morales de droit privé de mettre à sa disposition les informations utiles à la manifestation de la vérité, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent.

²¹⁸ A l'origine, le FNAEG ne concernait que les infractions de nature sexuelle.

²¹⁹ Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne. JORF du 16 novembre 2001. Disponible sur internet : <http://www.legifrance.gouv.fr/texteconsolide/PPEDZ.htm>

²²⁰ Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure ; JORF du 19 mars 2003 ; Disponible sur internet : <http://www.legifrance.gouv.fr/texteconsolide/PPED1.htm>

²²¹ Le Monde, 27 août 2006.

Ces deux articles sont applicables en matière d'enquête de flagrance. Les articles 77-1-1 et 77-1-2 du Code de Procédure Pénale reprennent le contenu de ces deux articles et l'applique en matière d'enquête préliminaire, à la différence majeure que cette réquisition ne peut être faite que par le procureur de la République, ou à défaut avec son autorisation.

Nous savons qu'aucune interconnexion entre le FAED et tout autre traitement de données à caractère personnel n'est possible. Mais nous pouvons imaginer l'hypothèse de la réquisition de la base de données biométriques des salariés de l'entreprise. Les services de police n'ont plus qu'à comparer l'empreinte digitale retrouvée sur les lieux d'un crime à cette base de données, plus ou moins importante selon la taille de l'entreprise. La CNIL a depuis longtemps²²² mis en lumière ce problème : « Quoiqu'il en soit, la connotation policière ne résulte pas uniquement de ce que la prise d'une empreinte digitale est, à l'origine, une technique policière. Elle est bien plus généralement liée à ce que dans la plupart des cas, si ce n'est tous, la constitution d'un fichier d'empreintes digitales, même à des fins qui ne sont pas illégitimes, va devenir un nouvel instrument de police, c'est-à-dire un outil de comparaison qui pourra être utilisé à des fins policières, nonobstant sa finalité initiale ».

Dès lors, une base de données d'empreintes digitales, quelle que soit la finalité initiale de sa constitution, est susceptible d'être utilisée à des fins de police.

La biométrie, utilisée pour sécuriser les accès, mais également contrôler le temps de travail des salariés, se généralise dans les entreprises. Et avec nous assistons à la création de centaines de bases de données, dont la finalité est très encadrée. Néanmoins, les services de police y auront accès.

Cette législation est le fruit d'un long travail émanant tant du législateur français que des organisations internationales. Malgré ses défauts, il reste à l'appliquer de la façon qui lui donnera la plus grande portée possible, et cette mission incombe à une pluralité d'acteurs (Chapitre second).

²²² CNIL. « 21^{ème} rapport d'activité : 2000 ». Paris : La Documentation française, 2001. 328 pages. Disponible sur internet : <http://lesrapports.ladocumentationfrancaise.fr/BRP/014000460/0000.pdf> .Page 107

Chapitre deuxième : Une législation perfectible appliquée par une pluralité d'acteurs

La législation, malgré ses défauts, doit être appliquée. Il ne tient qu'aux institutions qui sont chargées du contrôle de l'utilisation de la biométrie de faire en sorte que ces limites ne deviennent pas une faille réduisant considérablement la portée du système actuel (Section première).

Nous ne pouvons pas nous contenter de la situation actuelle, nous reposer sur le travail des autres. Il nous faut rester vigilants pour éviter les dérapages. Et la vigilance implique également de trouver des solutions assurant un meilleur encadrement des procédés biométriques d'identification (Section seconde).

Section première : Une utilisation de la biométrie sous le contrôle d'institutions nationales

Acteur incontournable de la protection des données à caractère personnel, la Commission Nationale de l'Informatique et des Libertés (Paragraphe premier) reste cependant peu connue de la population française.

Mais la Commission Nationale de l'Informatique et des Libertés n'est pas seule dans l'accomplissement de ses missions. Ainsi d'autres institutions, tant nationales qu'internationales, prennent position sur la biométrie (Paragraphe second).

Paragraphe premier : La Commission Nationale de l'Informatique et des Libertés

La Commission Nationale de l'Informatique et des Libertés (CNIL) a été créée par la loi n° 78-17 du 6 janvier 1978, relative à l'informatique, aux fichiers et aux libertés, sous la forme d'une autorité administrative indépendante. Elle a été confrontée à la biométrie alors qu'aucun régime juridique n'avait été adopté. Elle a tout de même réagi par une analyse au cas par cas, construisant progressivement sa doctrine pour aboutir finalement à un traitement général (A.).

La force de la CNIL tient également au fait qu'elle a rapidement affirmé son indépendance vis-à-vis de son créateur, l'Etat. Elle n'a pas hésité à pointer du doigt des fichiers gérés par les pouvoirs publics, et notamment les fichiers de police (B.).

A. D'une analyse au cas par cas à un traitement général

L'article 1 de la loi du 6 janvier 1978²²³ énonce solennellement que « l'informatique doit être au service de chaque citoyen [et] ne doit porter atteinte ni à l'identité humaine ni aux droits de l'Homme ni à la vie privée ni aux libertés individuelles ».

Malgré le manque de définition de l'identité humaine, l'informatique ne doit pas être une menace pour celle-ci. L'application de procédés informatisés d'identification doit alors par essence, et eu égard à l'article 1er de la loi susvisée, faire l'objet de toute l'attention de la CNIL.

Les premières applications de la biométrie²²⁴ sont apparues alors qu'aucun régime juridique général n'avait été mis sur pied. La CNIL a donc du procéder à une analyse au cas par cas. Néanmoins la CNIL avait émis son avis sur les procédés biométriques d'identification et anticipé la modification de loi « informatique et libertés » de 1978 en leur appliquant les principes de protection des données à caractère personnel²²⁵.

La CNIL a rappelé à plusieurs reprises que les données biométriques devaient non seulement être considérées comme des données à caractère personnel au sens de la loi « Informatiques et Libertés » mais qu'en outre elles n'étaient « pas des données comme les autres », et qu'ainsi elles « devaient faire l'objet d'une protection particulière »²²⁶.

Nous avons vu précédemment que la loi du 6 août 2004²²⁷ a apporté un véritable cadre juridique à la biométrie. La mise en œuvre d'un traitement automatisé doit dès lors respecter plusieurs principes²²⁸. A ces principes s'ajoutent les recommandations, les différents avis et les délibérations de la CNIL. desquels Au fil des décisions rendues sur les projets dont elle a été saisie, la CNIL a peu à peu dégagé une grille d'analyse reposant sur des critères permettant d'apprécier la conformité des dispositifs au regard des principes relatifs à la protection des données.

S'agissant du choix de la technique biométrique, la CNIL a établi une distinction selon que la technique biométrique envisagée porte ou non sur des éléments « laissant des traces »²²⁹. Cette expression désigne en premier lieu les technologies reposant sur la reconnaissance des empreintes digitales. Cette distinction repose sur la possibilité ou non de récupérer une donnée biométrique à l'insu de la personne. Ces données sont aussi dangereuses

²²³ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 ; JORF du 7 août 2004 ; Disponible sur internet :

<http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm>

http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf

²²⁴ Quelques exemples :

- Accès aux locaux : Délibération de la CNIL n° 97-044 du 10 juin 1997. Disponible sur internet :

<http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CNIL&nod=MCN97060044A>

- Accès aux cantines scolaires : CNIL. « 21^{ème} rapport d'activité : 2000 », précité. Pages 104 et suivantes.

²²⁵ CNIL. « 22^{ème} rapport d'activité : 2001 ». Paris : La Documentation française, 2002. 352 pages. Disponible sur internet : <http://lesrapports.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf>. Page 166 : « Par nature, un élément d'identification biométrique ou sa traduction informatique sous forme de gabarit constitue une donnée à caractère personnel entrant dans le champ d'application des lois « informatique et libertés » comme d'autres données personnelles (un nom, une adresse, un numéro de téléphone, etc.). »

²²⁶ CNIL. « 26^{ème} rapport d'activité : 2005 ». Paris : La Documentation française, 2006. 123 pages. Disponible sur internet : <http://lesrapports.ladocumentationfrancaise.fr/BRP/064000317/0000.pdf>. Page 49.

²²⁷ Loi n° 78-17 du 6 janvier 1978, précitée.

²²⁸ cf. supra Titre 2, Chapitre 2, Section 1, § 1, C., 1.

²²⁹ Expression utilisée dans la délibération de la CNIL n° 00-015 du 21 mars 2000. Disponible sur internet : <http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CNIL&nod=MCN97060044A>

que les empreintes génétiques par leur omniprésence²³⁰. Les risques de récupération et de réutilisation des empreintes digitales à d'autres fins sont très importants²³¹. D'autres techniques biométriques reposent sur des éléments « sans trace », comme c'est le cas pour le contour de la main, ou la reconnaissance vocale.

Dès lors, la CNIL est réticente vis-à-vis des technologies de reconnaissance des empreintes digitales, sans toutefois en rejeter catégoriquement les traitements ayant recours à des telles technologies. Tout dépend des justifications apportées pour la mise en œuvre du traitement, par exemple des nécessités particulières en terme de sécurité.

S'agissant d'une biométrie « à trace », la CNIL met en relation le système de stockage de ces données avec l'existence ou non d'un impératif particulier de sécurité. La constitution d'une base de données biométriques ne peut se faire qu'avec certains impératifs particuliers de sécurité, étant donné le risque accru de détournement de ces données²³². Une base de données biométriques centralisées ne sera toutefois pas indispensable dans la mesure où l'impératif de sécurité est moindre.

La finalité et la proportionnalité du traitement apparaissent donc comme les éléments déterminants, au regard de la technique et du système de stockage utilisés. La finalité du traitement doit être de nature à le justifier. Différentes finalités ont ainsi été retenues par la CNIL, comme l'impératif particulier de sécurité²³³, ou plus simplement le contrôle d'accès à certains locaux²³⁴.

La CNIL s'intéresse également à la proportionnalité du traitement. Celui-ci doit permettre de réaliser les objectifs pour lesquels il est mis en place, sans pour autant créer plus de problèmes qu'il n'est censé en résoudre. Nous citerons pour exemple la délibération autorisant la société TF1 à mettre en œuvre un traitement de données à caractère personnel (empreintes digitales)²³⁵ : ce traitement n'intéressait que certaines catégories précises de personnel devant accéder à certaines zones dites « sensibles ». De plus, les données n'étaient pas conservées dans une base de données centralisée, et elles faisaient l'objet d'un chiffrement.

Mais certaines finalités de traitements mettant en œuvre des données biométriques « à trace » ont été rejetées, peu importe les conditions de mise en œuvre :

- Accès restaurant scolaires

²³⁰ « Considérant cependant qu'à la différence d'autres données biométriques, les empreintes digitales laissent des traces qui peuvent être exploitées à des fins d'identification des personnes à partir des objets les plus divers que l'on a pu toucher ou avoir en main ». Délibération de la CNIL n° 00-015, précitée.

²³¹ Cf supra Titre 1, Chapitre 2, Section 1, § 1, B.

²³² « la constitution [d'une telle base de données] est dès lors susceptible d'être utilisée à des fins étrangères à la finalité recherchée par sa création ». Délibération de la CNIL n° 00-015, précitée.

« le traitement, sous une forme automatisée et centralisée, de données biométriques telles que les empreintes digitales ne peut être admis, compte tenu à la fois des caractéristiques de l'élément d'identification physique retenu, des usages possibles de ces traitements et des risques d'atteintes graves à la vie privée et aux libertés individuelles en résultant, que dans la mesure où des exigences impérieuses en matière de sécurité ou d'ordre public le justifient. » Délibération de la CNIL n° 2005-020 du 10 février 2005. Disponible sur internet : <http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CNIL&nod=MCP05020020A>

²³³ Nous citerons l'exemple de l'accès à certains locaux de la Banque de France, et également pour les examens scolaires et concours ...

²³⁴ Délibération de la CNIL n° 2005-001 du 13 janvier 2005. Disponible sur internet :

<http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CNIL&nod=MCP05010001A>

²³⁵ Délibération de la CNIL n° 2005-001 du 13 janvier 2005, précitée.

- Accès à un skate-parc
- Gestion des horaires du personnel

Néanmoins, un fait important jouait en défaveur de ces traitements. Avant la modification de la loi « Informatique et Libertés » en 2004, l'autorisation de la CNIL devait être obtenue quand le responsable du traitement était une personne publique²³⁶. Pour un traitement facilitant la gestion des horaires du personnel, la qualité du responsable du traitement avait donc son importance. Ainsi, dans la décision du Tribunal de Grande Instance du 19 avril 2004²³⁷, le responsable du traitement avait procédé à la déclaration préalable auprès de la CNIL du traitement de donnée biométrique.

Enfin, dans l'hypothèse d'un recours à une biométrie à traces avec stockage sur un support individuel mais en l'absence d'un impératif de sécurité, un dernier critère est pris en considération : le caractère facultatif du dispositif. Outre l'existence d'un stockage sur un support individuel, c'est le fait que seules les données des personnes volontaires fassent l'objet d'un traitement qui a décidé la CNIL à autoriser la chambre de commerce de Nice-Côte d'Azur à utiliser depuis 2005 une carte de fidélité comprenant un système de reconnaissance de l'empreinte digitale des voyageurs²³⁸.

De ces décisions au cas par cas, la CNIL a donc élaboré une véritable doctrine concernant la donnée biométrique. Mais depuis peu, la CNIL exerce un contrôle plus distant sur les demandes d'autorisation de tels traitements, et ce par l'édition d'autorisations uniques. La CNIL peut autoriser certains fichiers ou traitements de données personnelles sensibles ou à risques, qui visent une même finalité et des catégories de données et de destinataires identiques, au travers de décisions-cadre, appelées autorisations uniques. Si le traitement envisagé est conforme à l'une de ces autorisations, le responsable du traitement peut effectuer une simple déclaration de conformité.

De ces autorisations uniques, nous pouvons déduire un certain relâchement de l'activité de la CNIL. Au cours du premier semestre de l'année 2006, la CNIL a émis trois autorisations uniques concernant la biométrie.

- Délibération n°2006-101 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la gestion des horaires et de la restauration sur les lieux de travail (décision d'autorisation unique n° AU-007)²³⁹ ;
- Délibération 2006-102 du 27 avril 2006 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail (décision d'autorisation unique n° AU-008)²⁴⁰.

²³⁶ Voir le tableau récapitulatif des délibérations de la CNIL proposé par Madame LAFFAIRE. Source : LAFFAIRE, Marie-Laure et ELM, Thomas. « Biométrie, la première décision d'une longue série ». *Expertises*, août - septembre 2005 : pages 299 à 303.

²³⁷ TGI Paris, 1^{ère} chambre, section sociale, 19 avril 2005, CE d'Effia Services, Syndicat Sud Rail / Effia Services (RG n°05/00382) ; Disponible sur www.juriscom.net/documents/tgiparis20050419.pdf

²³⁸ Délibération de la CNIL n° 2005-115 du 7 juin 2005. Disponible sur internet :

<http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CNIL&nod=MCP05060115A>

²³⁹ Disponible sur legifrance :

<http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CNIL&nod=MCP06040101A>

²⁴⁰ Disponible sur legifrance :

<http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CNIL&nod=MCP06040102A>

- Délibération 2006-103 du 27 avril 2006 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 (décision d'autorisation unique n° AU-009)²⁴¹.

Deux de ces autorisations concernent une technologie utilisant le contour de la main, élément ne laissant pas de trace. Mais la troisième décision concerne une technologie utilisant les empreintes digitales. La CNIL, avec ces autorisations uniques, aura donc moins de demandes d'autorisation à traiter, mais il faut espérer que le temps gagné sera réinvesti dans des contrôles a posteriori, désormais seul moyen d'empêcher d'éventuelles dérives.

Durant l'année 2005, la CNIL aura adopté 316 délibérations²⁴², dont 36 concernaient la biométrie (un tiers pour les empreintes digitales, et deux tiers pour le contour de la main, une seule pour l'iris). La CNIL a ainsi autorisé 31 traitements de données biométriques, et refusé cinq projets de traitement. Ces cinq projets prévoyaient l'utilisation du contour de la main pour contrôler les horaires des salariés²⁴³, mais la CNIL a déclaré que « l'objectif d'une meilleure gestion des temps de travail, s'il est légitime, ne paraît pas, en lui-même, de nature à justifier l'enregistrement dans un lecteur biométrique des gabarits du contour de la main des employés. Ainsi, le recours à un élément propre à l'identité physique des employés aux seules fins de contrôler les temps de travail n'apparaît pas proportionné à la finalité poursuivie ». Puis la CNIL est revenue sur sa position en autorisant deux traitements 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 locaux²⁴⁴. Désormais, un tel traitement est adapté et proportionné à la finalité assignée au dispositif.

Durant l'année 2005, la CNIL a effectué 104 missions de contrôle²⁴⁵. Les trois autorisations uniques concernent 26 délibérations de l'année 2005, 31 si nous tenons compte des cinq projets refusés. Mais ce nombre va en augmentant. Pourtant, l'adoption de ces trois autorisations uniques n'aura pas, pour l'instant, de répercussions sur le nombre de contrôles effectués.

Le point le plus significatif est donc le revirement opéré par la CNIL sur la technologie de reconnaissance du contour de la main²⁴⁶. A ce stade de notre réflexion, nous pouvons nous demander si la CNIL n'a pas préféré céder face aux demandes d'autorisation, tout en espérant garder un contrôle. Plutôt que de s'opposer, la CNIL semble accompagner le développement de la biométrie, et ainsi jouer le jeu des acteurs économiques. N'est-ce pas là une tentative « d'endormissement » de la CNIL ? La banalisation de cette technologie est la porte ouverte à d'autres technologies plus dangereuses.

De nombreux projets sont mis en oeuvre par des entreprises privées, quelques fois par des organismes publics. A coté de ces projets, il ne faut pas oublier que la CNIL exerce également un contrôle sur les pouvoirs publics et leurs fichiers de police.

²⁴¹ Disponible sur legifrance :

<http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CNIL&nod=MCP06040103A>

²⁴² Liste en annexe rapport 2005

²⁴³ Délibérations de la CNIL du 17 février 2005 n° 2005-031, n° 2005-034, n° 2005-035, n° 2005-036 et n° 2005-037

²⁴⁴ Délibérations de la CNIL du 21 juin 2005 (n° 2005-163) et du 3 novembre 2005 (n° 2005-247)

²⁴⁵ Source : <http://www.itrnews.com/article.php?oid=53150&usermail>

²⁴⁶ Cinq refus d'autorisation et 17 autorisations

B. Le contrôle de la CNIL sur les pouvoirs publics

La CNIL est liée à l'évolution des fichiers de police. En effet, tous ces fichiers de police représentent précisément ce pour quoi la loi du 6 janvier 1978 a été adoptée et ce pour quoi la CNIL a été créée.

Monsieur TRUDEL s'étonne du fait que les risques de dérives de procédés d'identification dominant les débats²⁴⁷, et notamment les risques d'abus de la part des services de police. Mais selon lui, « n'est-ce pas via un contrôle des pouvoirs de police conséquent qu'il serait adéquat de prévenir les possibles dérives ? ».

Le recours à l'informatique peut faire craindre que l'utilisation des fichiers de police automatisés constitue un risque grave pour les libertés. En effet, des risques existent dès lors que des informations inexactes ou incomplètes peuvent être introduites dans l'ordinateur et que ces informations vont être conservées pendant très longtemps²⁴⁸. La situation peut devenir catastrophique pour une personne dès lors qu'il est procédé à des interconnexions ou à des échanges de données avec ces fichiers. Aux faiblesses technologiques s'ajoutent les défaillances humaines toujours possibles.

Selon l'article 5 du décret du 14 octobre 1991²⁴⁹ : « Les fonctionnaires des renseignements généraux dûment habilités et dans la limite du besoin d'en connaître sont seuls autorisés à accéder aux informations (*dont les signes physiques particuliers, objectifs et inaltérables, comme éléments de signalement*). Ces informations ne peuvent être communiquées aux services de police et de gendarmerie que si elles ont été collectées dans les cas [strictement prévus par le présent décret]. La communication est subordonnée à une demande écrite qui précise l'identité du consultant, l'objet et les motifs de la consultation. Cette demande ne peut être agréée que par le directeur central ou le responsable du service départemental des renseignements généraux et dans la seule mesure où elle se rattache aux finalités exposées [dans le décret]. Lorsque la communication a été autorisée, la fiche de consultation est conservée pendant un délai de deux ans, à la disposition des autorités de contrôle. Elle est détruite au terme de ce délai. Le décret relatif au fichier informatisé du terrorisme fixe les cas et les conditions dans lesquels d'autres fonctionnaires ou militaires relevant du ministère de la défense peuvent, pour l'exercice de leur mission, avoir accès aux informations de ce fichier ».

Avant l'intervention du législateur à partir de 1978, le Conseil d'Etat a été saisi du problème. Le 13 février 1976, un arrêt précise : « s'il appartient à l'autorité de police de recueillir et, le cas échéant, de réunir sous forme de fichier toutes les informations utiles sur les personnes dont l'état mental risque de menacer l'ordre public, elle a, en même temps, le devoir de veiller à ce que l'accès aux renseignements rassemblés soit strictement réservé aux seuls fonctionnaires placés sous son autorité, qui ont la charge d'exécuter la mission de service public ainsi définie ».²⁵⁰

²⁴⁷ Contribution de Monsieur TRUDEL au débat sur la CNIE, disponible sur le site internet du FDI :

<http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnle.pdf> ; page 66 et suivantes.

²⁴⁸ Données conservées pendant très longtemps pour le FAED et le FNAEG

²⁴⁹ Décret n° 91-1051 du 14 octobre 1991 portant application aux fichiers informatisés, manuels ou mécanographiques gérés par les services des renseignements généraux des dispositions de l'article 31, alinéa 3, de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ; JORF du 15 octobre 1991 ; <http://www.legifrance.gouv.fr/texteconsolide/PPHTK.htm>

²⁵⁰ Cf. Conseil d'Etat, Assemblée, du 13/02/76, *Deberon* ; Recueil page 100.

Avec l'utilisation des procédés biométriques d'identification, il devient prioritaire de s'assurer que les policiers ayant accès à ce type de données respectent l'usage exclusif auquel ils sont tenus et qu'ils ne puissent pas en faire un usage à des fins personnelles par exemple²⁵¹. Ces nouvelles questions d'éthique policière doivent d'ores et déjà faire partie du quotidien de tous les policiers, quelque soit leur rang, leur fonction. Une formation rénovée des policiers s'impose prenant en compte ce genre de question... Encore est-il indispensable que les pratiques non éthiques soient dénoncées.

La dénomination et la finalité du traitement, le service auprès duquel s'exerce le droit d'accès, les catégories d'informations nominatives enregistrées, les destinataires habilités à recevoir communication des informations, tous ces éléments doivent être précisés par l'acte réglementaire qui concerne des traitements automatisés d'informations nominatives opérés pour le compte de l'Etat ou d'un établissement public ; acte qui est soumis à l'avis de la CNIL²⁵².

La « mémoire » de la police devrait donc être limitée à certaines catégories de personnes ou de faits, spécialisée par objet, surveillée et contrôlée dans sa constitution et son utilisation, et dont la finalité ne peut être que l'ordre public. La CNIL joue à cet égard un rôle important puisqu'elle a la possibilité de contrôler les fichiers de police. Une prérogative qui se présente comme une garantie de la préservation de l'Etat de droit, l'Etat devant être lui même soumis au droit commun.

Mais cette surveillance des fichiers de la police par la CNIL est semble-t-il remise en question. La loi « informatique et libertés » modifiée prévoit en effet que la création des fichiers de sécurité (police, gendarmerie, renseignements généraux) sont désormais soumis à un avis consultatif de la CNIL (et non plus une autorisation). L'avis favorable de la CNIL ne serait donc plus de rigueur (l'on ne pouvait passer outre un avis négatif qu'à l'issue d'un décret pris sur avis conforme du Conseil d'Etat).

Il faut cependant noter que les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes, mis en œuvre pour le compte de l'Etat, sont expressément soumis au régime de l'autorisation de la CNIL à l'article 27- I, 2° de la loi « Informatique et Libertés ».

La question reste de savoir jusqu'où peut aller la préservation de l'ordre public érigée en « raison d'Etat ». Que faut-il penser et comment interpréter l'article 1er de la loi sur la sécurité quotidienne²⁵³ adoptée en urgence le 15 novembre 2001 selon lequel : « La sécurité est un droit fondamental. Elle est une condition de l'exercice des libertés et de la réduction des inégalités » ? Il a également été inséré à ce texte un chapitre sur la lutte contre le terrorisme.

Si à temps exceptionnel, mesure exceptionnelle, la généralisation des procédés d'identification basés sur la biométrie ne présage rien de bon pour les libertés individuelles.

Paragraphe second : Les autres intervenants

²⁵¹ Cf. Contribution de Monsieur DAMASIO au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnle.pdf> ; page 23 et suivantes

²⁵² Article 26 de la loi n° 78-17 du 6 janvier 1978, précitée.

²⁵³ Loi n° 2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne ; JORF du 16 novembre 2001. Disponible sur internet : <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=INTX0100032L>.

Deux institutions internationales, l'une européenne et l'autre communautaire, sont venues apporter leur pierre à l'édifice en précisant que les textes qu'elles ont adopté en matière de protection des données à caractère personnel s'appliquent bien en présence de données biométriques (A.)

Les autorités nationales ne restent pas inactives puisqu'elles ont sous leur autorité des organismes de nature diverses, acteurs principaux dans le domaine de la sécurité (B.). Mais récemment, les juridictions judiciaires se sont révélées comme des intervenants en matière de protection des données à caractère personnel (C.).

A. Les institutions européennes et communautaires

Dans le cadre du Conseil de l'Europe, le rapport d'étape²⁵⁴ sur l'application des principes de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel²⁵⁵ (STE No 108, ci-après la Convention 108), à la collecte et au traitement de données biométriques représente l'aboutissement de travaux entrepris en 2003 par le Groupe de Projet sur la Protection des Données (CJ-PD) sous l'égide du Comité européen de Coopération Juridique (CDCJ) et, suite à la restructuration des comités de protection des données, poursuivis en 2004 et 2005 par le Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (T-PD).

Le CJ-PD a reçu mandat du Comité des Ministres pour élaborer en priorité à l'attention du CDCJ ou son bureau, un rapport sur l'incidence des principes de protection des données sur l'utilisation des données biométriques (empreintes digitales, identification par l'iris, identification du visage, géométrie de la main, etc.) dans différents domaines.

Dans le cadre communautaire, nous ne pouvons pas passer à côté du groupe de protection des personnes, plus connu sous le nom de « groupe de l'article 29 » (en référence à l'article 29 de la directive 95/46/CE). Il s'agit de l'organe consultatif indépendant de l'UE sur la protection des données et de la vie privée.

L'article 30 définit les missions et les pouvoirs de ce groupe : « 1. Le groupe a pour mission :

- a) d'examiner toute question portant sur la mise en oeuvre des dispositions nationales prises en application de la présente directive, en vue de contribuer à leur mise en oeuvre homogène;
- b) de donner à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers;
- c) de conseiller la Commission sur tout projet de modification de la présente directive, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les

²⁵⁴ Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Rapport : « Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques ». Février 2005. Disponible sur internet : http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Rapports/O-rapport%20biometrie%202005.asp

²⁵⁵ Convention STCE n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Disponible sur internet : <http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm>

droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures communautaires ayant une incidence sur ces droits et libertés.

[...]

3. Le groupe peut émettre de sa propre initiative des recommandations sur toute question concernant la protection des personnes à l'égard du traitement de données à caractère personnel dans la Communauté. [...]

Dans le cadre de ses fonctions, le groupe de l'article 29 a adopté un document de travail sur la biométrie²⁵⁶ et émis un avis²⁵⁷. A travers l'élaboration de ces documents, le groupe tend à préciser l'application des principes édictés dans la directive 95/46/CE à la biométrie.

B. Les acteurs de la sécurité

Les opinions divergent dans les débats sociaux organisés autour de la mise en œuvre des procédés biométriques d'identification. Entre ceux qui sont hantés par les récits de Georges ORWELL qui présente une société sous le contrôle du « Big Brother »²⁵⁸, et ceux qui ont une confiance aveugle dans les nouvelles technologies, ravis d'être libérés de toutes les contraintes pratiques, il n'est pas facile de se faire une opinion libérée de la passion.

En matière de développement des procédés biométriques d'identification différents intérêts entrent en jeu, individuels, économiques, stratégiques, politiques. La question étant de savoir quelle est la place laissée à la protection des droits et des libertés.

Un ensemble d'organismes directement sous le contrôle étatique gère les questions de sécurité des systèmes d'information. La sécurité des systèmes d'information et des réseaux fait aujourd'hui l'objet d'un traitement particulier. De nombreux organismes en charge de ces questions ont progressivement été créés.

Parmi toutes les structures gouvernementales existantes, nous citerons la Direction Centrale de la Sécurité des Systèmes d'Information mise en place par un décret de 2001.²⁵⁹ Elle a remplacé le service central de la sécurité des systèmes d'information. Créée au sein du Secrétariat Général de la Défense Nationale (SGDN), la DCSSI s'est vue confier six missions²⁶⁰ :

« - Contribuer à la définition interministérielle et à l'expression de la politique gouvernementale en matière de sécurité des systèmes d'information

²⁵⁶ Document de travail sur la biométrie adopté le 1^{er} août 2003 - Disponible sur internet :

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_fr.pdf

²⁵⁷ 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), adopté le 11 août 2004 - Disponible sur internet :

http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp96_fr.pdf

²⁵⁸ Lire également LEVIN, Ira. Un bonheur insoutenable. Paris : Editions J'ai lu, 1972.

²⁵⁹ Décret n° 2001-693 du 31 juillet 2001 créant au secrétariat général de la défense nationale une direction centrale de la sécurité des systèmes d'information. JORF du 2 août 2001. Disponible sur internet :

<http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=PRMX0100093D>

²⁶⁰ Cf. site de la DCSSI : <http://www.ssi.gouv.fr/fr/dcssi/>

- Assurer la fonction d'autorité nationale de régulation pour la SSI (sécurité des systèmes d'information) en délivrant les agréments, cautions ou certificats pour les systèmes d'information de l'État, les procédés et les produits cryptologiques employés par l'administration et les services publics, et en contrôlant les centres d'évaluation de la sécurité des technologies de l'information (CESTI)
- Évaluer les menaces pesant sur les systèmes d'information, donner l'alerte, développer les capacités à les contrer et à les prévenir
- Assister les services publics en matière de SSI (sécurité des systèmes d'information)
- Développer l'expertise scientifique et technique dans le domaine de la SSI (sécurité des systèmes d'information), au bénéfice de l'administration et des services publics
- Former et sensibiliser à la SSI (sécurité des systèmes d'information - Centre de formation à la sécurité des systèmes d'information) ».

Mais nous pouvons nous poser la question de l'indépendance d'organismes comme la DCSSI qui est placée sous l'autorité du SGDN lequel est directement placé sous l'autorité du Premier ministre. Nous pouvons cependant remarquer que Monsieur WOLF, auteur de l'article très critique sur l'authentification biométrique²⁶¹, est responsable du centre de formation de la DCSSI.

Or en matière de sécurité des systèmes d'information les intérêts en présence sont différents selon que l'on se place du point de vue des scientifiques (dont l'objectif est de faire avancer la recherche et donc de partager au maximum l'information), des industriels (dont l'objectif est de vendre leurs produits de sécurité),²⁶² des individus (soucieux de la protection de leur vie privée) ou de l'Etat (dont l'un des devoirs essentiel est d'assurer la sécurité intérieure et extérieure du pays).

C. L'implication récente des juridictions de l'ordre judiciaire

A ce stade de notre étude, nous ne pouvons ne pas faire référence à la décision du Tribunal de Grande Instance de Paris, rendu le 19 avril 2005²⁶³, car c'est une des premières décisions de jurisprudence en la matière²⁶⁴.

Les faits sont les suivants : la société Effia Services, société intervenant dans le secteur du portage de bagages et d'accompagnement aux usagers, avait mis en place un système biométrique utilisant la technologies des empreintes digitales pour mieux gérer et contrôler le temps de présence des salariés sur l'ensemble de ses sites. L'empreinte digitale était mémorisée sur une carte à puce, que le salarié devait introduire dans une badgeuse. Le salarié devait ensuite apposer son doigt sur le lecteur afin que soit procédé à la comparaison entre l'empreinte stockée et celle lue par le lecteur.

Ce traitement a été mis en œuvre sous la législation de la loi du 6 janvier 1978 non modifiée. Ainsi, le régime des formalités applicables dépendait d'un critère organique. La

²⁶¹ WOLF, Philippe. « De l'authentification biométrique ». *Sécurité des systèmes d'information*, n° 46, octobre 2003 : 6 pages. Egalement disponible sur internet : <http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num46.pdf>

²⁶² Cf Titre 1, Chapitre 2, Section 2.

²⁶³ TGI Paris, 1^{ère} chambre, section sociale, 19 avril 2005, CE d'Effia Services, Syndicat Sud Rail / Effia Services (RG n°05/00382) ; Disponible sur www.juriscom.net/documents/tgiparis20050419.pdf

²⁶⁴ Voir LAFFAIRE, Marie-Laure et ELM, Thomas. « Biométrie, la première décision d'une longue série ». *Expertises*, août - septembre 2005 : pages 299 à 303

société Effia Services étant une entreprise privée, sa seule obligation envers la CNIL était, en application de l'ancien article 16 de la loi, de déclarer le traitement de données à caractère personnel envisagé. Mais les traitements automatisés opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité publique, ou d'une personne morale de droit privé gérant un service public, devaient être créés par un acte réglementaire pris après avis motivé de la CNIL²⁶⁵. La société Effia services s'était conformée à la législation en vigueur.

Le comité d'entreprise et le syndicat Sud Rail ont contesté la validité juridique de ce système de pointage par badge biométrique et ont donc porté l'affaire en justice. Il en ressort une décision qui cherche à s'inspirer de la doctrine de la CNIL, mais qui reste toutefois mal rédigée.

Le 8 avril 2004, la CNIL avait adopté un avis défavorable²⁶⁶ à la mise en œuvre d'un système biométrique ayant pour finalité la gestion du temps du personnel d'un centre hospitalier. En se fondant sur les principes d'adaptation et de proportionnalité par rapport aux buts visés, la CNIL avait estimé que « l'objectif d'une meilleure gestion du temps de travail, s'il est légitime, ne paraît pas de nature à justifier l'enregistrement dans un lecteur biométrique des empreintes digitales des personnels du centre hospitalier ». Elle précisait toutefois que le seul impératif de sécurité pouvait justifier la centralisation des données biométrique dans une base de données.

Le Tribunal retient que la mise en place d'un système biométrique pour contrôler le temps de présence des salariés dans l'entreprise n'est ni justifié ni proportionné au but recherché. Mais la rédaction de la conclusion à laquelle arrivent les juges est plus gênante. Dans la décision, il est écrit que : « Il s'ensuit que l'objectif poursuivi n'est pas de nature à justifier la constitution d'une base de données d'empreintes digitales des personnels travaillant dans les espaces publics des gares de la SNCF, le traitement pris dans son ensemble n'apparaissant ni adapté ni proportionné au but recherché. » Cette rédaction est gênante dans la mesure où la décision décrit elle-même la technique de stockage de la donnée biométrique, à savoir sur un badge individuel.

Madame LAFFAIRE²⁶⁷ tire les conséquences de cette maladresse dans la rédaction. Il semblerait que le Tribunal n'est finalement pas compris le dispositif technique qu'il devait jugé alors que la distinction entre la constitution d'une base de données et stockage des données sur un support remis à la personne est fondamentale²⁶⁸. Mais nous pouvons également mettre cette maladresse sur le compte de la nouveauté et de la technicité du domaine abordé.

Cette décision est donc une étape importante dans la protection des données biométriques, dans la mesure où le juge judiciaire pourrait devenir un garde-fou, surtout avec les autorisations uniques de la CNIL.

²⁶⁵ Ancien article 15 de la loi n° 78-17 du 6 janvier 1978, précitée.

²⁶⁶ Délibération de la CNIL n° 04-018 du 8 avril 2004. Disponible sur internet :

<http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CNIL&nod=MCP04040018A>

²⁶⁷ Voir à ce propos LAFFAIRE, Marie-Laure et ELM, Thomas. « Biométrie, la première décision d'une longue série ». *Expertises*, août - septembre 2005 : pages 299 à 303

²⁶⁸ cf Titre 2, Chapitre 2, Section 1, § 1, A.

Et comme toute étape importante, elle a été accompagnée de son lot de commentaires, dont certains étaient plutôt très critiques, à l'instar de Monsieur BARBRY²⁶⁹. Selon lui, cette décision sera un stable majeur dans le développement des technologies biométriques, « dont les objectifs ne sont pas uniquement sécuritaires mais peuvent tout aussi bien s'appliquer en matière de confort des salariés ou de celui des employeurs ». Ce confort pour les salariés tient par exemple dans la substitution de la donnée biométriques aux mots de passe, or nous avons vu précédemment les risques d'une telle substitution. Pour Monsieur BARBRY, « l'encadrement du développement de la biométrie, s'il doit être respectueux de la dignité humaine et des libertés individuelles, doit également donner une chance à l'innovation et faire confiance en cela aux industriels [...] ». C'est sans compter sur les propos du GIXEL²⁷⁰.

La pluralité d'intervenants pose problème dès lors que ceux-ci ne parlent pas d'une seule et même voix, à tout le moins du moment qu'ils n'essaient pas de se gêner les uns les autres. Néanmoins, leurs actions ne sont pas suffisantes pour assurer un niveau adéquat de protection aux données biométriques. D'autres solutions pour un meilleur encadrement de la biométrie existe.

Section seconde. Les solutions pour un meilleur encadrement de la biométrie

La sanction juridique est inefficace face à des pirates informatiques qui tentent de récupérer des données à caractère personnel. Il est nécessaire que cette protection juridique s'accompagne d'une protection technique (Paragraphe premier).

En plus de cette protection technique, nous pensons qu'une meilleure implication de la population dans ces projets de procédés d'identification biométriques permettrait d'empêcher les dérives tant redoutées. La population se doit d'être « éduquée » afin qu'elle prenne conscience du rôle qui lui revient de droit (Paragraphe second).

Paragraphe premier : Une protection juridique inefficace sans protection technique

L'informatique prend une place de plus en plus importante dans notre société, et le droit tente de suivre cette évolution. L'exemple le plus récent que nous citerons est la loi sur les droits d'auteur et les droits voisins dans la société de l'information²⁷¹, qui vient renforcer juridiquement les mesures techniques de protection des œuvres. En matière de protection des données à caractère personnel, il faut sécuriser la donnée, mais cette sécurisation doit nécessairement s'accompagner de mesures destinées à restreindre l'accès à cette donnée.

En matière de sécurité des données l'article 34 de la loi « Informatique et Libertés » prévoit que « 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

²⁶⁹ BARBRY, Eric et ROUILLE-MIRZA, Ségolène. « La biométrie dans l'entreprise : quand l'innovation se heurte à la culture de l'interdit ». *Gazette du Palais*, 20 juillet 2005 : pages 7 à 8.

²⁷⁰ GIXEL. « Livre bleu , Grands programmes structurants, Propositions des industries électroniques et numériques » ; juillet 2004 ; Disponible sur internet :

<http://www.gixel.fr/Portal Upload/Files/ASSISES%202004/LB300604.pdf>

²⁷¹ Loi n° 2006-961 du 1er août 2006 dite loi DADVSI. JORF 3 août 2006. Disponible sur internet : <http://www.legifrance.gouv.fr/WAspad/UnTexteDeJorf?numjo=MCCX0300082L>

sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Cette obligation d'assurer la sécurité et la confidentialité des traitements et des données est transcrite à l'article 226-17 du Code pénal.²⁷² Remarquons au passage que cet article a conservé l'ancienne dénomination des données à caractère personnel (information nominative), une ancienne dénomination plus restrictive que cette dernière.

La question de la confidentialité des traitements nécessite dès lors la sécurisation des procédés biométriques. En effet, les données biométriques vont circuler sur un réseau informatique, et il faut s'assurer qu'aucun pirate ne puisse accéder aux données. Au-delà de cette intrusion, la loi « Informatique et Libertés » impose que l'accès aux données biométrique ne soit autorisé qu'à certaines personnes habilitées.

Si nous confrontons le projet INES, qui regroupera les données biométriques toute la population française, avec l'obligation de confidentialité, nous apercevons déjà l'ampleur des difficultés que l'Etat rencontrera. La nécessité de mettre en place des procédures d'accès aux données identifiantes qui soient sécurisées a, à plusieurs reprises, été évoquée par monsieur de VILLEPIN lorsqu'il occupait le poste de ministre de l'Intérieur. Il a précisé à ce propos qu'il s'agissait d'un « enjeu majeur pour la sécurité [du] territoire, la lutte contre le détournement de droits et l'escroquerie à l'identité ».

Dans cette optique, sécuriser la biométrie consiste donc non seulement à protéger les données biométriques mais aussi à contrôler l'accès à ces données.

La question est d'autant plus importante que les données sont susceptibles de circuler sur un réseau informatisé si elles sont regroupées dans un fichier centralisé à des fins de comparaison, comme pour le projet INES. Pour ce qui est de la protection des données biométriques, la question de leur sécurité dépend des choix technologiques qui sont faits. Des alternatives à un fichier centralisé ont été proposées. Le ministère de l'Intérieur considère dans les débats sur la carte d'identité électronique que cela ne permettrait pas d'assurer une bonne lutte contre la fraude.

Néanmoins, les alternatives proposées démontrent bien que les risques sont différents entre les biométrie « à trace » (comme les empreintes digitale) et les biométries « sans traces » (comme l'iris de l'œil).

En ce qui concerne la sécurité de l'accès aux données, il conviendrait de s'assurer que les personnes ayant accès aux données soient effectivement habilitées à cela. C'est donc à une habilitation sécurisée qu'il convient de parvenir. Ce problème a été abordé lors des débats sur la CNIE. Le ministère de l'Intérieur aurait ainsi envisagé de permettre aux personnes de vérifier l'habilitation de celles ayant accès aux données. Mais cette « habilitation sécurisée » n'est pas pour le moment intégrée au projet INES.

Enfin, une solution originale et efficace permettrait de prévenir tout éventuel usage policier de base de données d'empreintes digitales constituées à d'autres fins. Ainsi, lors de la

²⁷² « Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers est puni de cinq années d'emprisonnement et de 300000 euros d'amende ».

18e conférence internationale des autorités de protection des données qui a eu lieu à Ottawa en septembre 1996, un consultant américain préconisait que le gabarit de l'empreinte digitale soit utilisé pour chiffrer l'élément contenu dans la base de données, de sorte que chaque gabarit d'une empreinte ne pourrait être déchiffré qu'en présence de l'intéressé auquel l'information biométrique se rapporte²⁷³.

En définitive nous nous apercevons que la mise en œuvre de procédés biométriques à des fins d'identification impose l'établissement de tout un arsenal technique qui augmente encore le coût de l'utilisation de cette identité informatisée. La mise en œuvre de ces procédés dans les entreprises reste à leur charge. Mais ceux mis en œuvre par l'Etat pèseront sur le budget public, sur les contribuables. En plus d'être assimilés à des criminels²⁷⁴, les contribuables financeront la lutte contre la fraude à l'identité, contre le terrorisme.

Paragraphe deuxième : La nécessité d'une prise de conscience de la population

Dans le cadre du projet INES, c'est toute la population²⁷⁵ qui aura ses données biométriques centralisées dans une base de données, sous le contrôle de l'Etat. Mais le développement des procédés biométriques d'identification dans les entreprises, pour accéder aux restaurants scolaires, dans la vie quotidienne, nous amène à nous poser la question sur la propriété des données (A.). Néanmoins, à défaut de reconnaissance d'un droit de propriété, il est indispensable que la population soit associée à la mise en œuvre des procédés biométriques (B.).

A. La question de la propriété des données à caractère personnel

Notre droit est construit autour de la propriété. Ainsi la Déclaration des Droits de l'Homme et du Citoyen déclare que « le but de toute association politique est la conservation des droits naturels et imprescriptibles de l'homme. Ces droits sont la liberté, la propriété, la sûreté et la résistance à l'oppression »²⁷⁶ et que « la propriété étant un droit inviolable et sacré, nul ne peut en être privé, si ce n'est lorsque la nécessité publique, légalement constatée, l'exige évidemment, et sous la condition d'une juste et préalable indemnité »²⁷⁷.

Combinée à l'informatique, la biométrie permet de transformer une donnée brute (caractéristiques biologiques, physiques ou comportementales) en une empreinte numérique, en une donnée numérique. Une donnée numérique est la représentation d'une information sous une forme conventionnelle (codage en système binaire) destinée à faciliter son traitement²⁷⁸. L'information est définie quant à elle comme tout « élément de connaissance susceptible d'être représenté à l'aide de conventions pour être conservé, traité ou communiqué »²⁷⁹.

²⁷³ CNIL. « 22^{ème} rapport d'activité : 2001 ». Paris : La Documentation française, 2002. 352 pages. Page 168. Disponible sur internet : <http://lesrapports.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf>

²⁷⁴ Cf. Titre 1er

²⁷⁵ A l'heure actuelle, la CNIE n'est pas obligatoire, ce qui limiterait ses avantages.

²⁷⁶ Article 2 de la Déclaration des Droits de l'Homme et du Citoyen

²⁷⁷ Article 17 de la Déclaration des Droits de l'Homme et du Citoyen

²⁷⁸ Définition sur le site internet de Celog : <http://www.celog.fr/silex/tome1/termino1.htm#def43>

²⁷⁹ LUCAS, André, DEVEZE, Jean, et FRAYSSINET, Jean. *Droit de l'informatique et de l'Internet*. Paris : Editions Presses Universitaires de France, 2001 ; 748 pages.

Pour certains auteurs, il ne fait aucun doute que l'information doit être reconnue comme un bien juridique, étant donnée sa valeur marchande de l'information²⁸⁰. Si l'information est un bien, et qu'un bien est « toute chose matérielle susceptible d'appropriation »²⁸¹, alors l'information peut être appropriée. Autrement dit, pourrait-on inclure dans le patrimoine²⁸² des personnes les informations à caractère personnel qui les concernent ? Il faut en effet remarquer que l'information sur l'identité des personnes est devenue une source de profit importante pour les entreprises et même un enjeu marketing.

D'autres auteurs ont également montré que le recours à la thèse de la propriété donnerait un appui à la loi dite « informatique et libertés »²⁸³ qui confère aux personnes physiques des droits sur les informations à caractère personnel les concernant.²⁸⁴ Les personnes physiques ont en effet divers droits sur les données personnelles qui font l'objet d'un traitement automatisé (droit d'accès, d'information, de rectification, d'opposition).

D'autres enfin pensent que cette patrimonialisation de l'information permettrait de reconnaître aux Etats un « droit de souveraineté » sur les informations recueillies sur son sol.²⁸⁵

Mais à l'instar de messieurs FRAYSSINET, DEVEZE et LUCAS, la patrimonialisation de l'information ne nous paraît pas applicable en matière de protection des données à caractère personnel.

Ces auteurs font ainsi valoir que « si la personne concernée revendique une certaine maîtrise sur des informations la concernant, ce n'est pas en invoquant leur valeur patrimoniale mais en faisant valoir un droit de la personnalité »²⁸⁶.

B. La participation de la population à la mise en œuvre des procédés biométriques d'identification

Afin d'impliquer la population dans la mise en œuvre des procédés biométriques, il était indispensable que celle-ci en comprenne les enjeux et les risques. Il est impossible pour une personne lambda de participer à un projet, de donner son avis, sans connaître la matière

²⁸⁰ Voir thèse de P. CATALA, *Ebauche d'une théorie juridique de l'information* ; D. 1984 chronique page 97. Repris dans LUCAS, André, DEVEZE, Jean, et FRAYSSINET, Jean. *Droit de l'informatique et de l'Internet*. Paris : Editions Presses Universitaires de France, 2001 ; 748 pages. Page 269, note 4.

²⁸¹ CORNU, Gérard. *Vocabulaire juridique*. Paris : Editions Presse Universitaire de France, 2005 (7^{ème} édition). 970 pages. Page 111.

²⁸² Patrimoine : « Ensemble des biens et des obligations d'une même personne, envisagé comme formant une universalité de droit, un tout comprenant non seulement ses biens présents mais aussi ses biens à venir ». Définition reprise dans le Vocabulaire juridique de CORNU, Gérard, précité. Page 654

²⁸³ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 ; JORF du 7 août 2004 ; Disponible sur internet :

<http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm>

http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf

²⁸⁴ Herbert MAISL ; *La maîtrise d'une interdépendance* ; JCP G. 1978 I, 2891, n°26. Repris dans *Droit de l'informatique et de l'Internet* de André LUCAS, Jean DEVEZE, Jean FRAYSSINET. Paris : Editions Presses Universitaires de France, 2001. 748 pages. Page 270, note 7.

²⁸⁵ GARZON, G. *Biens immatériels et flux transfrontalier*. Paris : Litec, 1986. Pages 94-98. Repris dans *Droit de l'informatique et de l'Internet* de André LUCAS, Jean DEVEZE, Jean FRAYSSINET. Paris : Editions Presses Universitaires de France, 2001. 748 pages. Page 270, note 8.

²⁸⁶ POULLET, Y. « Le fondement du droit de la protection des données nominatives : propriétés ou libertés ». Repris dans *Droit de l'informatique et de l'Internet* de André LUCAS, Jean DEVEZE, Jean FRAYSSINET. Paris : Editions Presses Universitaires de France, 2001. 748 pages. Page 271.

de ce projet. Dès lors, il nous faut revenir à la condition essentielle de leur participation : les Français ont-ils les moyens de s'informer sur les procédés biométriques d'identification ?

Il faut reconnaître que les sources d'informations relatives à la biométrie ne manquent pas. Le débat s'est en effet largement organisé autour de l'identité biométrique, et de nombreux sites internet reprennent cette question²⁸⁷. Mais beaucoup sont le fait d'internautes « amateurs », dans la mesure où seule un aspect particulier de la biométrie est traité, le plus souvent d'une façon très critique. A côté de ses sites « amateurs », de nombreux organismes contribuent à l'information des citoyens sur ce sujet. La CNIL et le Forum des Droits sur l'Internet (FDI) participent largement à l'information des citoyens sur ce thème.

Le site internet de la CNIL²⁸⁸ est une interface qui concoure largement à l'information du public sur la question de la biométrie. Un dossier complet sur la technique mais aussi sur l'application de la biométrie aux titres d'identité est accessible en ligne.²⁸⁹

Le Forum des Droits sur l'Internet a également largement participé à l'information des citoyens notamment quant à la mise en œuvre du projet INES. En effet, le FDI a été chargé d'organiser, en accord avec le ministère de l'Intérieur, un débat public sur ce projet. Ainsi ont été organisés des débats en ligne sur le forum, des manifestations et des débats en régions et des échanges de messages électroniques venus d'internautes et d'experts mais aussi des sondages réalisés avec l'institut IPSOS.

Le ministère de l'Intérieur est également intervenu lors des débats sur le projet INES d'une manière qui se voulait pédagogique, claire et rassurante²⁹⁰. Néanmoins, cette intervention s'est traduite par une augmentation significative des messages postés sur le forum.

Les principaux sujets abordés dans les débats ont été repris et synthétisés par le FDI dans un rapport sur la carte d'identité électronique²⁹¹. Les avis des internautes ont été publiés dans un autre document²⁹². Mais nous ne pouvons que regretter le mode d'identification des internautes. En effet, ceux-ci se sont exprimés sous couvert de pseudonymes, de sorte qu'il est impossible de vérifier leurs compétences, leurs qualités en la matière. Pourtant, le rapport final n'hésite pas à les qualifier de « citoyens-experts »²⁹³.

L'information, plus ou moins objective (tout dépend de la source même de l'information donc), sur la biométrie ne manque donc pas.

Mais différents facteurs mettent en cause l'implication réelle des individus à propos de la sauvegarde de leurs libertés individuelles. Le Forum des droits sur l'internet s'est également interrogé sur l'efficacité des débats organisés autour de la Carte nationale

²⁸⁷ <http://ecolesdifferentes.free.fr/JEUDES1000BORNES.htm>,

http://yonne.lautre.net/article.php3?id_article=1520.

²⁸⁸ <http://www.cnil.fr>

²⁸⁹ http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/LA_BIOMETRIEmai2005.pdf

²⁹⁰ Présentation du projet INES publié sur le site du FDI :

<http://www.foruminternet.org/telechargement/forum/pres-prog-ines-20050301.pdf>

²⁹¹ Forum sur les Droits de l'Internet. Rapport : « Projet de carte nationale d'identité électronique ». Paris, 16 juin 2005. 45 pages. Disponible sur internet : <http://www.foruminternet.org/telechargement/documents/rapp-cnie-20050616.pdf>

²⁹² Synthèse des débats en ligne : http://www.foruminternet.org/telechargement/forum/syntheses_cnie.pdf

²⁹³ FDI. Rapport : « Projet de carte nationale d'identité électronique », précité. Page 30

d'identité électronique. La question étant effectivement de savoir si l'opinion de la population peut influencer sur un projet dans lequel le ministère de l'Intérieur est déjà bien engagé.

Si le FDI regrette le manque de moyens dont il a disposé pour « faire connaître le débat auprès du grand public », ²⁹⁴ il précise que les débats organisés autour de la CNIE auraient eu un impact sur l'avancé du projet et les orientations prises. Ainsi, l'avis des citoyens aurait été pris en compte par le ministère de l'Intérieur sur différents points et notamment quant à la question d'assurer une plus grande sécurité.

Derrière l'organisation de ces débats, nous voyons l'importance du facteur humain dans le processus biométrique d'identification ²⁹⁵. Le rapport du député CABAL insiste sur la phase « d'enrôlement » des individus ²⁹⁶ et dispose à cet égard qu'il « convient de gérer la relation homme/machine ». Cette relation est primordiale, et les professionnels de la biométrie l'ont bien compris. Ainsi l'argument développé par ces derniers est « simplicité et efficacité » ²⁹⁷. Mais cette publicité dangereuse, nous l'avons vu, de la biométrie nous semble réduire le consentement des individus dans le processus légal qui s'organise autour de la biométrie.

La population doit dès lors comprendre qu'elle est un régulateur nécessaire de la biométrie.

²⁹⁴ FDI. Rapport : « Projet de carte nationale d'identité électronique », précité. Page 29

²⁹⁵ CABAL, Christian. Rapport « Méthodes scientifiques d'identification des personnes à partir des données biométriques ». Rapport n° 958, déposé à l'Assemblée Nationale le 16 juin 2006. Disponible sur le site internet de l'Assemblée Nationale : <http://www.assemblee-nationale.fr/12/rap-ocgst/i0938.asp>

²⁹⁶ Rapport CABAL, précité. Page 28

²⁹⁷ Cf. Titre 1, Chapitre 2, Section 2.

CONCLUSION

Au terme de ce mémoire, nous nous sommes demandés si les données biométriques bénéficient-elles de la protection qui leur revient, eu égard à leur nature. Mais ce raisonnement ne doit pas se limiter au seul cas français. Les données à caractère personnel sont susceptibles de circuler entre les pays²⁹⁸, dès lors une protection élaborée au niveau communautaire et international semble plus adéquate.

Le projet de Traité établissant une Constitution pour l'Europe²⁹⁹, rejeté en juin 2005 en France, va dans le sens d'une protection adéquate pour la donnée biométrique. Il dispose en effet dans son article II-68, relatif à la protection des données à caractère personnel :

« 1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ses règles est soumis au contrôle d'une autorité indépendante ».

Nous remarquons au passage que le consentement de la personne concernée est mentionné avant la possibilité de collecter les données sur la base d'un autre fondement légitime prévu par la loi.

Par ailleurs, du 14 au 16 septembre 2005, lors de la 27^{ème} conférence internationale des Commissaires à la protection des données et à la vie privée, une déclaration finale intéressant la protection des données personnelles a été adoptée. Cette déclaration vise en effet à reconnaître solennellement un droit universel à la protection des données.³⁰⁰

De surcroît, nous devons nous demander si certaines données biométriques, et nous pensons plus particulièrement aux empreintes génétiques, ne pouvaient être intégrées aux dites « données sensibles » au sens de la loi « informatique et libertés ». ³⁰¹ Les données génétiques fournissent, ou sont susceptibles de fournir dans l'avenir, une information scientifique, médicale et personnelle pertinente tout au long de la vie d'un individu. Cette

²⁹⁸ Mais la carte du monde interactive disponible sur le site de la CNIL montre combien le niveau de protection diverge selon les Etats. Cf. site internet de la CNIL <http://www.cnil.fr/index.php?id=1100#>

²⁹⁹ Disponible sur internet : <http://constitution-europeenne.info/texte.htm>

³⁰⁰ Déclaration disponible sur internet :

http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_f.pdf

³⁰¹ Cf. article 8- I de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004. JORF du 7 août 2004. Disponible sur internet :

<http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm>

http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf

information peut également avoir une incidence significative sur la famille de l'intéressé, et dans certains cas sur l'ensemble du groupe auquel il appartient.

De surcroît, les données génétiques sont susceptibles de révéler des informations sur plusieurs personnes tout en ne permettant de n'en identifier qu'une seule. En conséquence, ces données doivent être traitées avec une attention particulière.

Dès lors, ne faudrait-il pas procéder rapidement à cette requalification des données génétiques en données « sensibles » ? Certains industriels vont même jusqu'à envisager l'enregistrement de l'empreinte génétique dans la future carte d'identité électronique³⁰².

Avec l'ADN, les procédés biométriques d'identification touchent à ce que les hommes ont de plus personnel : leur identité génétique. Le droit est insuffisant pour éviter toute dérive, toute utilisation immorale de telles données.

Le droit et la morale sont parfois opposés, en soulignant que la morale tend à la perfection de l'Homme sur un plan personnel idéal, tandis que le droit, positiviste par essence, doit tenir compte des contingences de la vie en communauté dans un souci de paix sociale. Il va de soi, toutefois, que le sens de ce qui est bien et juste ne peut être absent des préoccupations du législateur et que tout système juridique comporte des préoccupations morales.

Ces préoccupations morales ne doivent pas être effacées au bénéfice d'une logique sécuritaire. Le droit se doit de les prendre en compte, pour une meilleure utilisation de la biométrie à des fins d'identification.

³⁰² Contribution de Monsieur WEIZS au débat sur la CNIE, disponible sur le site internet du FDI : <http://www.foruminternet.org/telechargement/forum/avis-specialistes-cnle.pdf> ; contribution page 27 et s.

BIBLIOGRAPHIE

➤ **Manuels et Traités de droit**

BORRICAND, Jacques *et alii*. *Problèmes actuels de sciences criminelles*. Volume XVII. Aix-en-Provence : Presses universitaires d'Aix-Marseille, 2001. 171 pages.

CARBONNIER, Jean. *Droit civil Tome 1*. Paris : Editions Presse Universitaire de France, 2004 (1^{ère} édition). 1496 pages.

CONTE, Philippe et MAISTRE DE CHAMBON, Patrick. *Procédure pénale*. Paris : Editions Armand Colin, 2001 (3^{ème} édition). 426 pages.

CORNU, Gérard. *Vocabulaire juridique*. Paris : Editions Presse Universitaire de France, 2005 (7^{ème} édition). 970 pages.

LAFFAIRE, Marie-Laure. *Protection des données à caractère personnel*. Paris : Editions d'Organisation, 2005. 542 pages

LUCAS, André, DEVEZE, Jean, et FRAYSSINET, Jean. *Droit de l'informatique et de l'Internet*. Paris : Editions Presses Universitaires de France, 2001 ; 748 pages.

➤ **Autres manuels**

BUQUET, Alain. *Manuel de criminalistique moderne*. Paris : Editions Presse Universitaire de France, 2003 (2^{ème} édition). 262 pages.

DIAZ, Charles. *La police technique et scientifique*. Paris : Editions Presse Universitaire de France, 2000. 127 pages.

➤ **Lois**

Convention STCE n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Disponible sur internet :

<http://conventions.coe.int/Treaty/fr/Treaties/Html/108.htm>

Directive n° 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. Disponible sur internet :

<http://europa.eu.int/ISPO/legal/fr/dataprot/directiv/direct.html>

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 ; JORF du 7 août 2004 ; Disponible sur internet :
<http://www.legifrance.gouv.fr/texteconsolide/PPEAU.htm>
http://www.cnil.fr/fileadmin/documents/approfondir/textes/CNIL-78-17_definitive-annotee.pdf

Loi n° 2003-239 du 18 mars 2003 pour la sécurité intérieure ; JORF du 19 mars 2003 ; Disponible sur internet :
<http://www.legifrance.gouv.fr/texteconsolide/PPED1.htm>

Décret n° 2005-1309 du 20 octobre 2005 pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004 ; JORF du 22 octobre 2005 ; Disponible sur internet :
<http://www.legifrance.gouv.fr/texteconsolide/PRHWE.htm>
<http://www.cnil.fr/index.php?id=1880>

Code Civil, Code de Procédure Pénale, Code de la Propriété Intellectuelle, Code du Travail : disponible sur internet <http://legifrance.gouv.fr/WAspad/ListeCodes>

➤ **Essais et études**

GEORGET Pierre ; « Traiter, échanger, partager les données » ; *Ethique et société de l'information* ; La documentation Française ; Paris 2000 ; 194 pages ; pages 69 à 77.

POUSSON Didier ; « L'identité informatisée » ; Sous la direction de J. POUSSON-PETIT ; *L'identité de la personne humaine* ; Editions Bruylant ; 2002 ; 1001 pages.

➤ **Rapports**

CABAL, Christian. Rapport « Méthodes scientifiques d'identification des personnes à partir des données biométriques ». Rapport n° 958, déposé à l'Assemblée Nationale le 16 juin 2006. Disponible sur le site internet de l'Assemblée Nationale : <http://www.assemblee-nationale.fr/12/rap-ocst/i0938.asp>

Commission Nationale de l'Informatique et des Libertés. Rapport d'activité.

- « 20^{ème} rapport d'activité : 1999 ». Paris : La Documentation française, 2000. 360 pages. Disponible sur internet :
<http://lesrapports.ladocumentationfrancaise.fr/BRP/004001043/0000.pdf>
- « 21^{ème} rapport d'activité : 2000 ». Paris : La Documentation française, 2001. 328 pages. Disponible sur internet :
<http://lesrapports.ladocumentationfrancaise.fr/BRP/014000460/0000.pdf>
- « 22^{ème} rapport d'activité : 2001 ». Paris : La Documentation française, 2002. 352 pages. Disponible sur internet :
<http://lesrapports.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf>
- « 23^{ème} rapport d'activité : 2002 ». Paris : La Documentation française, 2003. 414 pages. Disponible sur internet :
<http://lesrapports.ladocumentationfrancaise.fr/BRP/034000366/0000.pdf>
- « 24^{ème} rapport d'activité : 2003 ». Paris : La Documentation française, 2004. 538 pages. Disponible sur internet :
<http://lesrapports.ladocumentationfrancaise.fr/BRP/044000252/0000.pdf>

- « 25^{ème} rapport d'activité : 2004 ». Paris : La Documentation française, 2005. 112 pages. Disponible sur internet : <http://lesrapports.ladocumentationfrancaise.fr/BRP/054000256/0000.pdf>
- « 26^{ème} rapport d'activité : 2005 ». Paris : La Documentation française, 2006. 123 pages. Disponible sur internet : <http://lesrapports.ladocumentationfrancaise.fr/BRP/064000317/0000.pdf>

Comité Consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Rapport : « Rapport d'étape sur l'application des principes de la Convention 108 à la collecte et au traitement des données biométriques ». Février 2005. Disponible sur internet :

http://www.coe.int/T/F/Affaires_juridiques/Coop%E9ration_juridique/Protection_des_donn%E9es/Documents/Rapports/O-rapport%20biometrie%202005.asp

CHATILLON, Georges. Rapport « Les données personnelles : enjeux juridiques et perspectives ». IDT juin. 1999.

Disponible sur internet :

http://dess-droit-internet.univ-paris1.fr/bibliotheque/article.php3?id_article=101&var_recherche=donn%C3%A9e+personnelles

Forum sur les Droits de l'Internet. Rapport : « Projet de carte nationale d'identité électronique ». Paris, 16 juin 2005. 45 pages. Disponible sur internet :

<http://www.foruminternet.org/telechargement/documents/rapp-cnle-20050616.pdf>

LECERF, Jean-René. « Rapport d'information sur la nouvelle génération de documents d'identité et la fraude documentaire ». Rapport d'information n° 239, déposé au Sénat le 29 juin 2005. Disponible sur le site internet du Sénat : <http://www.senat.fr/rap/r04-439/r04-4391.pdf>

Vie privée, droit de l'homme : actes de la 23e conférence internationale des commissaires à la protection des données ; La Documentation Française ; Paris, 2002 ; 557 pages

GIXEL. « Livre bleu , Grands programmes structurants, Propositions des industries électroniques et numériques » ; juillet 2004 ; Disponible sur internet :

<http://www.gixel.fr/Portal Upload/Files/ASSISES%202004/LB300604.pdf>

➤ Travaux universitaires

BŒUFS Géraldine sous la direction de KOSTIC Gaël ; *Le recul de la vie privée au nom de la croisade anti-terroriste* ; Mémoire rédigé dans le cadre du DESS Droit du Multimédia et de l'informatique, Université Paris 2 ; Paris, année universitaire 2003-2004 ; 68 pages ; http://www.u-paris2.fr/dess-dmi/rep_travaux/77_G.Boeufs.pdf

AUGER Delphine sous la direction de CHATILLON George ; *Biométrie : l'équilibre entre « liberté individuelle » et promesse sécuritaire serait-elle impossible ?* ; Mémoire rédigé dans le cadre du DESS Droit de l'internet - Administration - Entreprises, Université Paris 1, année universitaire 2004-2005 - 88 pages

➤ **Reuves juridiques**

BARBRY, Eric et ROUILLE-MIRZA, Ségolène. « La biométrie dans l'entreprise : quand l'innovation se heurte à la culture de l'interdit ». *Gazette du Palais*, 20 juillet 2005 : pages 7 à 8

GUERRIER, Claudine. « Protection des données personnelles et application biométriques en Europe ». *Communication - Commerce électronique*, juillet - août 2003 : pages 17 à 22

GUERRIER, Claudine. « Les cartes d'identité et la biométrie : l'enjeu sécuritaire ». *Communication - Commerce électronique*, mai 2004 : pages 19 à 23

GUINIER, Daniel. « Biométrie : classification au vu des nouveaux motifs » ; *Expertises* ; février 2005 : pages 62 à 68.

LAFFAIRE, Marie-Laure et ELM, Thomas. « Biométrie, la première décision d'une longue série ». *Expertises*, août - septembre 2005 : pages 299 à 303

BARBRY, Eric, et GRASSTER, Marie-Charlotte. « La biométrie est permise dans les entreprises sous réserves de certaines précautions ». *Gazette du Palais*, n°293, 20 octobre 2005 : pages 14 à 16.

LECLERCQ, Pierre ; « A propos de la biométrie (Quelques réflexions après visite de l'exposition « Biométrie, le corps identité » à la Cité des sciences) ». *Communication - Commerce électronique*, mars 2006 : pages 14 à 18

HADJALI, Sonia. « Droit du travail et nouvelles technologies : de la cybersurveillance à la cyberconfiance ». *Gazette du Palais*, n°110, 20 avril 2006 : pages 30 à 33

➤ **Autres revues**

WOLF, Philippe. « De l'authentification biométrique ». *Sécurité des systèmes d'information*, n° 46, octobre 2003 : 6 pages.

Egalement disponible sur internet : <http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num46.pdf>

➤ **Articles en ligne**

Sous la direction de madame PREUSS-LAUSSINOTE ; « Encadrement et risques de la biométrie » ; 27 février 2004 ;

http://www.e-juristes.org/article.php3?id_article=161&var_recherche=biometrie

CRAIPEAU Sylvie, DUBEY Gérard, GUCHET Xavier ; « La biométrie : usages et représentations » ; Rapport final, projet incitatif GET 2003 ; février 2004 ; www.foruminternet.org/telechargement/forum/biometrieint.pdf

GUCHET Xavier ; « Manger sous surveillance : l'usage d'une technique biométrique pour le contrôle d'accès à la cantine scolaire » ; 2004 ;
<http://www.creis.sgdg.org/colloques%20creis/2004/IS04programme%20et%20actes.htm>

LEMOINE Philippe ; Communication relative aux « enjeux technologiques et la protection des données personnelles » ; 4 mars 2004.
http://dess-droit-internet.univ-paris1.fr/bibliotheque/article.php3?id_article=415&var_recherche=biometrie

➤ **Site internet**

Site internet de la Commission Nationale de l'Informatique et des Libertés :
<http://www.cnil.fr/>

Site internet du Forum sur les Droits de l'Internet : <http://www.foruminternet.org/>

Portail français destiné à faire le lien entre tous les acteurs de la biométrie et les utilisateurs :
<http://biometrie.online.fr/>

Portail européen sur la biométrie :
<http://www.europeanbiometrics.info/activities/index.php>