N° 938

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DOUZIÈME LÉGISLATURE

Enregistré à la présidence de l'Assemblée nationale
Le 16 juin 2003

N° 355

SÉNAT

SESSION ORDINAIRE DE 2002 - 2003

Annexe au procès-verbal
de la séance du 12 juin 2003

**OFFICE PARLEMENTAIRE D'ÉVALUATION
DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES**

RAPPORT (1ère partie)

sur

LES MÉTHODES SCIENTIFIQUES D'IDENTIFICATION DES PERSONNES À PARTIR DE DONNÉES BIOMÉTRIQUES ET LES TECHNIQUES DE MISE EN OEUVRE

Par M. Christian CABAL,
Député

Déposé sur le Bureau de l'Assemblée nationale
par M. Claude BIRRAUX,
Président de l'Office

Déposé sur le Bureau du Sénat
par M. Henri REVOL,
Premier Vice-Président de l'Office

Recherche

SAISINE

RÉPUBLIQUE FRANÇAISE
LIBERTÉ • ÉGALITÉ • FRATERNITÉ

ASSEMBLÉE NATIONALE

Paris, le 17 octobre 2002

LE PRÉSIDENT

Monsieur le Président et cher Collègue,

En application de l'article 6*ter* de l'ordonnance n° 58-1100 du 17 novembre 1958 relative au fonctionnement des assemblées parlementaires, le Bureau de l'Assemblée nationale a décidé, à son initiative, de saisir l'Office parlementaire d'évaluation des choix scientifiques et technologiques d'une étude sur « *les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre* »

Je vous prie, Monsieur le Président et cher Collègue, de croire à l'assurance de mes meilleurs sentiments.

Jean-Louis DEBRÉ

Monsieur Claude BIRRAUX
Président de l'Office parlementaire d'évaluation
des choix scientifiques et technologiques

TABLE DES MATIERES

PREMIERE PARTIE DU RAPPORT

DEUXIEME PARTIE DU RAPPORT

ANNEXES

INTRODUCTION

« La biométrie a la renommée d'une science aride. Son armature technique est incompatible avec les découvertes qui frappent l'imagination ».

Tel était le constat établi par Eugène SCHREIDER[1] en 1960, alors qu'une dizaine d'années plus tard la « révolution biométrique » était annoncée sans véritablement prendre corps[2] et qu'à l'aube du vingt-et-unième siècle, un commissaire à la protection des données personnelles a pu observer que la biométrie suscite aujourd'hui « fascination et inquiétude »[3].

Pour expliquer ces différences d'appréciation, plusieurs facteurs peuvent être évoqués qui permettront de mieux circonscrire le champ et la portée de l'étude confiée par le Bureau de l'Assemblée nationale à l'Office parlementaire d'évaluation des choix scientifiques et technologiques et qui porte sur ***« les méthodes scientifiques d'identification des personnes à partir des données biométriques et les techniques de mise en œuvre »[4].***

Il y a tout d'abord certainement un glissement sémantique.

Le terme « biométrie » est de plus en plus utilisé pour définir des techniques permettant d'identifier une personne à partir de l'un ou plusieurs de ses caractères biologiques ou comportementaux alors même que la biométrie recouvre un champ scientifique beaucoup plus vaste[5]. Même dans le seul domaine de l'identification humaine, l'utilisation du mot biométrie est, dans le langage courant, de plus en plus limitée à l'identification de personnes vivantes, excluant ainsi les travaux conduits en matière d'identification *post mortem*. Réduite à cette acception, la notion d'identification s'est par ailleurs appauvrie puisqu'elle ne

---

[1] « La biométrie » - Eugène SCHREIDER (Directeur adjoint du laboratoire d'anthropologie physique de l'Ecole Pratique des Hautes Etudes, Professeur de l'Institut de Démographie de l'Université de Paris) - PUF - Collection « Que sais-je » - 1960.

[2] « Technologies internationales » n°69, novembre 2000.

[3] Jennifer STODDART, Présidente de la Commission d'accès à l'information du Québec, septembre 2001.

[4] Saisine transmise par le Bureau de l'Assemblée nationale le 17 octobre 2002.

[5] Le terme « biométrie » a été introduit dans le vocabulaire scientifique à la fin du dix-neuvième siècle et correspond aux mots anglais « *biometry* » ou « *biometrics* » employés parfois par les auteurs américains comme des synonymes du mot « statistiques ». Dans la langue française, plusieurs acceptions sont données : « étude mathématique, surtout statistique, des phénomènes biologiques » (dictionnaire Hachette), « science qui étudie à l'aide des mathématiques (statistiques et probabilités) les variations biologiques à l'intérieur d'un groupe déterminé » (dictionnaire Robert), « science des variations biologiques, des phénomènes qui s'y rattachent et des problèmes qui en découlent » (Eugène SCHREIDER dans son article consacré à la biométrie paru dans l'*Encyclopaedia Universalis*).

tient pas compte des éléments constitutifs de l'identité d'un individu tels que l'âge par exemple, alors que divers travaux permettent désormais à partir d'examens radiologiques des os ou maxillo-dentaires d'établir à peu près de manière certaine l'âge d'une personne.

Les méthodes scientifiques utilisées reposent-elles cependant sur les mêmes principes? Selon Eugène SCHREIDER, la biométrie se fonde sur la mensuration et le dénombrement et utilise les statistiques et les probabilités afin de donner aux phénomènes biologiques une *« expression quantitative plausible »*, ce qui le conduisait à affirmer que si la biométrie apporte un peu de précision, elle le fait au détriment de la certitude.

Or, les techniques se sont nettement perfectionnées et modifient à la fois les méthodes d'observation et de traitement.

Grâce à elles, les données biométriques susceptibles de servir à une identification se diversifient. En 1960, Eugène SCHREIDER considérait ainsi que la topographie du système pileux, la couleur des cheveux, la pigmentation des yeux ne constituait pas des caractères « mesurables ». Aujourd'hui, aucun caractère ne semble *a priori* exclu. Les données biométriques ne sont plus nécessairement anatomiques, la voix, le geste, l'odeur, la chaleur sont désormais aussi pris en compte et les photographies numérisées sont maintenant utilisées pour la reconnaissance faciale.

L'automatisation permet par ailleurs d'effectuer des traitements de masse rapidement, voire presque instantanément, dans des domaines où le patient et minutieux travail d'expertise semblait réservé à « l'homme de l'art ». Si les technologies biométriques sont définies comme des systèmes de reconnaissance « automatiques »[6], le degré d'automaticité est lui-même devenu un critère de distinction. Ainsi, par exemple, l'analyse d'ADN sera tantôt classée dans la catégorie des techniques biométriques[7], tantôt elle en sera exclue[8] en raison des conditions dans lesquelles la comparaison d'ADN est habituellement pratiquée.

---

[6] Ainsi par exemple, dans ses deux derniers rapports d'activité, la Commission nationale de l'informatique et des libertés (CNIL) considère que les systèmes biométriques sont « des applications permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main…), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche) ». Le *Parliamentary Office of Science and Technology* britannique a donné une définition voisine : la biométrie est la mesure de caractéristiques biologiques telles que les empreintes digitales, le dessin de l'iris, l'image de la rétine, la forme du visage ou de la main ou de caractères comportementaux comme la voix, la démarche ou la signature et les techniques biométriques utilisent ces caractéristiques pour identifier les individus automatiquement.

[7] Telle est la position de la CNIL, de la commission d'accès à l'information du Québec ou de l'organisme allemand *Biotrust*.

[8] Telle est la position du *Parliamentary Office of Science and Technology* britannique, du *General Accounting Office* américain ou de l'*Electronic Warfare Associates* canadien.

Le troisième facteur est lié à l'élargissement des domaines d'application des systèmes biométriques d'identification.

L'utilisation des procédés d'identification humaine a été longtemps cantonnée aux applications militaires et policières : *« l'identification humaine, celle des récidivistes d'abord, celle des malfaiteurs ensuite grâce aux traces abandonnées par eux sur les lieux d'infraction, a été dès l'origine la préoccupation majeure des services de police technique ou scientifique »*[9]. Dans ce domaine d'ailleurs, les besoins d'identification ne se limitent plus à la seule répression des atteintes à la sécurité publique, mais s'étendent à leur prévention.

En marge de l'état civil et de la signature manuscrite, pour répondre aux autres besoins d'identification et d'authentification dans le monde physique comme électronique, divers moyens ont été mis en œuvre (codes, mots de passe, numéros d'identification, cartes, signature numérique…) que des procédés biométriques sont susceptibles de remplacer ou de « sécuriser ».

Ces besoins d'identification s'inscrivent dans un cadre spatial plus ou moins large ; ils peuvent être circonscrits à un bâtiment ou un réseau restreint comme prendre une dimension internationale par l'effet de l'intensification de la circulation transfrontalière des hommes et la mondialisation des échanges de biens et de services. Ils doivent, par ailleurs, se concilier avec d'autres besoins, tels que le respect de la vie privée, la protection des données personnelles, les libertés individuelles au premier rang desquelles celle d'aller et venir.

Parce qu'aujourd'hui les systèmes biométriques d'identification des personnes suscitent un intérêt certain et des craintes multiples, il y a débat.

Ce débat est tout d'abord de nature technique. Les systèmes biométriques d'identification sont-ils fiables ? Sont-ils plus performants que les méthodes d'identification habituellement pratiquées ? Parmi les différentes techniques, quelles sont celles qui semblent les plus sûres et les plus pratiques au regard de l'usage que l'on veut en faire ?

Il est aussi politique et le Parlement français a déjà eu l'occasion de délibérer à plusieurs reprises, en premier lieu lors de la création du fichier national d'empreintes génétiques, l'Office parlementaire d'évaluation des choix scientifiques et technologiques ayant publié un rapport sur *« la valeur scientifique de l'utilisation des empreintes génétiques dans le domaine judiciaire »*[10] et, plus récemment, lors de l'adoption de la loi du 29 août 2002 d'orientation et de

---

[9] « La police technique et scientifique » - Charles Diaz - PUF – Collection « Que sais-je ? » - 2000.

[10] « La valeur scientifique de l'utilisation des empreintes génétiques dans le domaine judiciaire » par Christian Cabal, député, n°3121 Assemblée Nationale (11ème législature) et Sénat n°94 (2001-2002)

programmation pour la sécurité intérieure[11] et de la loi du 18 mars 2003 sur la sécurité intérieure. Cette évolution n'est pas propre à la France. Dans beaucoup d'autres pays européens, au sein du G8, de l'Union européenne, aux Etats-Unis, au Canada et ailleurs ce débat a lieu.

Dans les instances scientifiques, techniques, administratives et politiques un consensus est actuellement recherché. Aussi est-il normal que le Parlement soit lui-même associé à ce débat, même si les décisions qui seront finalement prises débordent le cadre de ses compétences strictement législatives.

Votre rapporteur, face aux excès d'enthousiasme ou de défiance à l'égard des techniques biométriques d'identification, a jugé opportun, tout d'abord, de dresser une sorte d'état des lieux des opinions exprimées à ce sujet, en ce qui concerne les performances des systèmes, mais aussi les risques liés à un développement incontrôlé de ces derniers.

Dans une large mesure ces excès et l'absence de consensus expliquent les blocages que l'on a pu constater, les applications biométriques restant de fait relativement limitées. Il convient dès lors de s'interroger sur les conditions dans lesquelles il paraît possible d'assurer un développement maîtrisé des techniques biométriques, eu égard au cadre juridique actuel et aux rapports de force existants en particulier au plan international.

[11] L'annexe 3, dans son paragraphe intitulé « Moderniser les services et mieux utiliser les technologies de traitement de l'information », énonce que « les nouvelles technologies devront (…) être développées dans le domaine de la maîtrise du flux migratoire et de la lutte contre la fraude documentaire (lecture automatique des passeports et des cartes nationales d'identité, mise en œuvre des technologies de biométrie aux contrôles transfrontières…) »

PREMIERE PARTIE :

Eviter les excès de confiance ou de défiance : pour une analyse raisonnée des techniques d'identification des personnes à partir des données biométriques

L'analyse des différents documents consacrés aux systèmes biométriques d'identification des personnes révèle l'existence de fortes oppositions tant en ce qui concerne l'évaluation de leurs performances respectives que l'appréciation des effets de leur utilisation.

I - Certitudes et doutes sur les performances des techniques biométriques d'identification

Il existe incontestablement une mode des systèmes biométriques d'identification qui sont souvent perçus comme une panacée : les utilisateurs en attendent une fiabilité à toute épreuve permettant de supprimer l'intervention humaine des opérations de contrôle. Certes, ces systèmes ont réalisé beaucoup de progrès, mais ils ne correspondent pas toujours aux besoins et les utilisateurs potentiels ont beaucoup de mal à analyser leurs performances faute de critères de certification. En outre, ces techniques sont pour certaines en cours de développement et les résultats parfois prometteurs obtenus en laboratoire ne doivent pas être confondus avec les performances de systèmes opérationnels, pour lesquels les paramètres de réussite sont très divers.

1- Analyse des progrès techniques enregistrés et à venir.

Reconnaissance faciale ou vocale, identification d'empreintes, numérisation de l'iris, analyse comportementale... Les technologies d'identification n'ont pas attendu les attentats du 11 septembre 2001 aux Etats-Unis pour émerger. Depuis cette date, le marché se développe de manière considérable, notamment dans les aéroports où, pour des raisons évidentes de sécurité, il est indispensable d'identifier rapidement les personnes et de s'assurer de la validité des titres présentés.

L'analyse de certaines données du corps humain pour identifier un individu n'est pas récente : l'empreinte digitale n'est pas une technique neuve à proprement parler. ***Ce qui constitue une évolution majeure est le couplage de ces techniques avec l'informatique***.

a) Les caractéristiques communes aux divers systèmes de biométrie

La biométrie est un système d'identification des individus utilisant des caractéristiques mesurables comme les empreintes digitales, l'iris, la rétine, la forme du visage, de la main, la voix voire la démarche ou le système veineux . Lors de la mission qu'il a conduite au Japon, votre Rapporteur a été impressionné par la variété des systèmes qu'il a pu voir fonctionner. Quasiment tout, dans l'anatomie ou le comportement d'un individu, peut être transformé en un code informatique permettant de l'identifier.

A partir d'un élément biométrique propre à un individu on détermine un ***gabarit***, c'est-à-dire ***une suite numérique qui caractérise l'élément biométrique*** et c'est le gabarit qui est conservé et non l'image de l'élément biométrique à proprement parler. La technique d'élaboration du gabarit est propre à chaque éditeur de logiciel biométrique.

Pour reconnaître un individu, on extrait des paramètres de l'image photographiée (empreinte, face, iris…) puis on compare le gabarit obtenu avec tous les paramètres précédemment extraits et sauvegardés.

La novation de ce système de reconnaissance à partir d'éléments de biométrie est son caractère automatisé par le recours à l'informatique.

Jusqu'à présent l'identification se faisait à partir de trois moyens principaux :

✓ Sur la reconnaissance visuelle des individus. Mais il existe deux problèmes principaux ; le coût de l'immobilisation d'une personne (gardien), qui limite les points de contrôle et souvent impose des horaires d'ouverture et de fermeture ; en outre, ce type de contrôle est lié au sérieux du contrôleur qui peut se laisser abuser par des ressemblances et être sensible à des éléments tels que la fatigue.

✓ Sur une possession : clé, carte à puce… mais il y a un risque de perte.

✓ Sur une connaissance : code carte bleue, code pin, mot de passe… mais il y a un risque d'oubli.

Avec la biométrie, nous disposons de systèmes automatisés permettant de reconnaître les personnes avec une grande précision sans avoir besoin de carte ni de mot de passe. Sa palette d'utilisation est très large :

- elle peut être utilisée dans des documents d'identification tels que par exemple une carte d'identité, un passeport, un permis de conduire, etc…

- pour le contrôle de prestations sociales, votre Rapporteur ayant pu constater que cet usage était particulièrement important aux Etats-Unis.

- pour restreindre l'accès à des appareils privés : PC, téléphones portables.…

- pour restreindre l'accès à des pièces sécurisées : coffres, salles de produits dangereux…

- pour permettre l'identification d'une personne sur un réseau : e-commerce.

Si aujourd'hui la biométrie peut se développer, elle le doit d'abord à un confort d'utilisation accru.

La vitesse d'acquisition constitue un autre facteur très important. Une vitesse de 6 à 10 secondes par personne est en général considérée comme acceptable, et ce n'est que récemment que les systèmes biométriques ont pu atteindre ces vitesses.

La combinaison de l'optronique et de l'informatique permet aujourd'hui de développer des systèmes qui présentent un grand confort d'utilisation qui à terme pourra être accru par de nouvelles puces qui ont fait leur apparition sur le marché. Elles peuvent intégrer les données biométriques et être interrogées par des ondes radio cryptées ce qui autorise un passage sans avoir à sortir un document de sa poche.

Ce mouvement n'est d'ailleurs pas achevé. Des constructeurs développent des outils numériques d'identification biométrique destinés aux ordinateurs de demain, ceux qui auront assez de puissance pour faire tourner des applications complexes de calculs géométriques en 3D en temps réel.

Ces fonctions réclament une puissance de calcul que les processeurs actuels ont du mal à fournir pour peu que les besoins en reconnaissance soient un peu élevés.

La reconnaissance faciale a encore de gros progrès à faire avant d'être fiable dans les aéroports ; l'arrivée de nouveaux processeurs, la baisse des tarifs des caméras et d'autres technologies permettront de traiter mieux et plus vite les algorithmes temps réels.

La mise sur le marché de systèmes automatisés et fiables n'exclut pourtant pas toute présence humaine. Celle-ci demeure nécessaire pour contrôler l'enregistrement des données, du moins pour l'accès aux zones sécurisées et surtout pour gérer les résultats erronés.

b) Une vaste palette d'outils

Au cours de ses visites et missions, votre Rapporteur a pu tester la quasi-totalité de la palette des produits existants sur le marché ou en cours de

développement dans des laboratoires. Certains industriels ont tendance à présenter leur système comme le meilleur, car le plus sûr et le plus facile d'emploi, mais il est essentiel de considérer que les différents outils obéissent à des finalités variées et à des objectifs différents.

Aussi passerons-nous en revue les différents produits disponibles à l'aide d'une grille d'analyse relativement simple prenant en compte le confort d'utilisation, la précision, puis le rapport qualité-prix et, enfin, le degré de sécurité, point fondamental même s'il est plus difficile à appréhender, comme nous le verrons dans la partie suivante.

Certains systèmes tels que la reconnaissance à partir de la démarche, que votre Rapporteur a pu voir fonctionner en laboratoire, sont encore loin d'être opérationnels et les recherches effectuées dans ce domaine sont extrêmement diverses et fragmentées.

Un recensement exhaustif s'avère ainsi irréaliste.

L'analyse des systèmes commercialisés ou en voie de l'être permet toutefois de prendre la mesure de la variété des solutions proposées et de « diagnostiquer » une diversification croissante des produits qui seront mis sur le marché dans les prochaines années.

Les outils de reconnaissance anatomique

- *L'empreinte digitale : Un système éprouvé d'un bon rapport qualité prix*

Il s'agit de ***la technique la plus ancienne[12] et la plus répandue***, car très nettement dominante parmi les « grands systèmes » traitant plusieurs millions de données biométriques.

Dès 1901 cette méthode d'identification a été adoptée par Scotland Yard et dès 1903 par la Préfecture de police, ce qui explique sa très forte connotation policière.

Le fonctionnement repose sur les principes suivants : un capteur prend une image du doigt, un logiciel repère les emplacements remarquables sillons avec crêtes et vallées, minuties (arche, boucle et tourbillon) et les transforme en un code informatique. Les systèmes haut de gamme ayant un grand nombre de points sont très précis et sont aussi capables de vérifier que l'empreinte appartient bien à un doigt et non à un moulage.

[12] En effet, dès 1892, il a été démontré que l'empreinte digitale est unique pour chaque individu et ne change pas au cours de la vie.

Suivant le niveau de sécurité recherché, les logiciels examineront entre une dizaine de minuties pour des systèmes peu discriminants et plus de quatre-vingts pour des systèmes de haute sécurité.

Le dispositif d'authentification de l'empreinte digitale est composé de trois éléments:

- un lecteur (prise d'image des empreintes digitales);

- un logiciel de traitement (algorithmes d'extraction des minuties de comparaison) ;

- une électronique de traitement (en général un ordinateur).

Des progrès très marquants ont été réalisés ces dernières années en matière de capture d'images.

Il existe, en effet, diverses méthodes pour l'acquisition de l'empreinte :

- Optique : un appareil photo numérique peut être utilisé pour prendre une image de l'empreinte digitale. Le doigt est placé sur une vitre suffisamment éclairée avec une lentille en dessous. Deux inconvénients sont cependant à regretter : une image reste sur le verre qui peut être réutilisée et il est très difficile de distinguer les vrais doigts et les bonnes imitations.

- Capacitive : Le doigt est placé sur un maillage de pixels sensibles aux différences de charges, qui captent la variation locale de capacitance entre les crêtes (majoritairement constituées d'eau) et les vallées (air). Une image peut alors être construite à partir de la forme des crêtes et des vallées. Même si cette méthode est très sensible aux décharges électrostatiques (ESD) et aux champs électriques parasites et même si elle peut être facilement trompée par une empreinte digitale artificielle, elle est le plus largement utilisée pour la prise d'empreintes digitales.

- Radio : Une onde radio de faible intensité est transmise au doigt, et agit comme un transmetteur, la variation de distance introduite par les crêtes et les vallées pouvant être détectée par des pixels agissant comme des antennes. Cela nécessite que le doigt soit en contact avec la région émettrice du détecteur (souvent en périphérie). Cette technologie reposant sur une propriété de la peau, il est difficile de tromper un détecteur radio avec une empreinte artificielle. Le seul point faible de cette technique est la nécessité d'une bonne qualité de contact entre le doigt et l'anneau transmetteur et le risque de surchauffe désagréable.

- Pression : Avec des piézo-électriques, une surface sensible à la pression peut être élaborée qui détermine l'empreinte digitale quand l'utilisateur appuie un doigt dessus. Certaines entreprises développent des produits avec cette technologie, malgré les nombreux inconvénients qu'elle comporte : peu de

sensibilité, incapacité à distinguer un faux moulage d'empreinte et risque de dommage si une pression trop forte est appliquée.

- MEMS : un ensemble de détecteurs type MEMS (micro-electro-mechanical systems) a été construit en laboratoire. Il permet de repérer les crêtes et les vallées d'une empreinte digitale. Toutefois, ce composant n'est pas très robuste et il ne permet pas de distinguer un vrai doigt d'un faux.

- Thermique : des pyro-électriques qui convertissent une différence de température en une différence de tension sont utilisés. La différence de température entre les crêtes en contact avec le détecteur et les vallées donne un dessin de l'empreinte. Cette méthode présente de nombreux avantages : pas de signal transmis au doigt, bonne immunité aux décharges électrostatiques, fonctionnement à des températures extrêmes comme à température ambiante et, enfin, impossibilité de berner le système avec un moulage. Il y a néanmoins un désavantage de taille : l'image thermique disparaît très vite. Au début il y a une grosse différence de température entre le doigt et le détecteur, mais en $1/10^{ème}$ de seconde les deux atteignent la même température et l'image disparaît.

Enfin, il existe d'autres technologies telles que les **ultrasons** pour capturer l'image d'une empreinte digitale. Toutefois, elles sont moins adaptées aux applications impliquant des productions importantes.

Lors de la prise de ces images, par l'une ou l'autre de ces techniques, deux procédés peuvent être utilisés : soit le doigt est statique et posé sur une surface qui englobe toute l'empreinte à photographier pendant tout le temps nécessaire, soit le doigt glisse sur un petit rectangle suffisamment large, mais long seulement de quelques pixels. Avec la première méthode, l'image est obtenue d'un seul coup, mais cela nécessite une grande surface active et une image rémanente reste sur la surface. Pour la seconde méthode, l'empreinte est scannée et reconstituée après informatiquement et, dans ce cas, il n'existe pas de risque d'image résiduelle, et la fabrication s'effectue à un moindre coût, car la surface active est plus petite.

Une fois l'empreinte digitale de l'utilisateur stockée dans un fichier, il faut vérifier la concordance entre la personne contrôlée et celle dont l'identité est stockée.

Le demandeur d'accès est invité à placer son doigt sur le lecteur. L'image est digitalisée et analysée afin d'en extraire les éléments caractéristiques.

La *"signature"* de l'empreinte est comparée avec le fichier préalablement enregistré sous la même identité.

Le système autorise ou refuse l'accès, en fonction du résultat de la comparaison des deux fichiers *"signature"*.

Une fois l'image saisie, elle est comparée à l'image de référence stockée ou, plus exactement, aux points remarquables transformés en code informatique.

Le système calcule un facteur de qualité qui permet d'établir un critère automatique de fiabilité de la "signature" de l'empreinte.

Le système de vérification d'identité est basé sur la comparaison de deux ensembles de minuties (fichier "signature"), correspondants respectivement à deux doigts à comparer. Pour déterminer si deux ensembles de minuties extraits de deux images correspondent à des empreintes du même doigt, il est nécessaire d'adopter un système de comparaison qui soit insensible à d'éventuelles interprétations, rotations et déformations qui affectent systématiquement les empreintes digitales.

A partir de deux ensembles de minuties extraites, le système est capable de donner un indice de similitude ou de correspondance qui vaut :

0 % si les empreintes sont totalement différentes ;

100 % si les empreintes viennent de la même image.

Deux fichiers "signature" calculés à partir de la même empreinte ne donneront jamais 100 % de ressemblance du fait des différences qui existent lors de l'acquisition de deux images (petites déformations ou déplacements), ils donneront cependant toujours un niveau élevé de similitude.

Déterminer, à partir de cet indice de similitude, si deux empreintes sont issues du même doigt est une ***question purement statistique***. ***Pour décider d'accepter la similitude entre deux "signatures", il faut établir un seuil d'acceptation.***

Avec un petit nombre de minuties (15 ou 20) correctement localisées, il est possible d'identifier une empreinte parmi plusieurs millions d'exemplaires.

Généralement, chaque minutie occupe environ un espace de 16 octets sans compactage ni compression. Ceci explique la taille de chaque fichier *signature,* 240 octets pour 15 minuties et 1600 octets pour 100 minuties.

En matière d'empreintes digitales, des progrès significatifs sont enregistrés dans le domaine de la miniaturisation et autorisent aujourd'hui le recours aux empreintes digitales par l'intégration des capteurs dans la majorité des applications (téléphones, récepteur FSE).

Aujourd'hui, les matériels retenus présentent un certain nombre d'avantages tels que le faible coût des lecteurs grâce aux nouveaux capteurs de type "Chip silicium", et la rapidité des traitements.

- L'authentification par la géométrie de la main

Cette technique de reconnaissance, bien que basée sur la même partie du corps, est moins contraignante que la reconnaissance d'empreintes digitales, la saleté et les petites coupures n'empêchant pas l'identification.

La forme de la main est acquise par un scanner spécialisé, généralement à infrarouge. Des paramètres tels que la longueur des doigts, leur épaisseur et leur position relative sont extraits de l'image et comparés à la base de donnée. Cette biométrie est toutefois sujette aux modifications de la forme de la main liées notamment au vieillissement.

Le système prend une photographie de la main et examine 90 caractéristiques, y compris la forme tridimensionnelle de la main, de la longueur et de la largeur des doigts et de la forme des articulations.

Pour utiliser la géométrie de la main, l'utilisateur place sa main sur une platine possédant des guides pour positionner les doigts.

Les lecteurs de géométrie de la main sont de grande taille.

Très simple à utiliser, cette technologie rencontre cependant des limites : elle est trop encombrante pour un usage sur un bureau (par exemple pour ouvrir un ordinateur). De plus, le coût des lecteurs est sensiblement plus élevé que pour l'empreinte digitale.

- La reconnaissance par l'iris : un système sûr mais « fermé »

L'utilisation de l'iris pour l'identification remonte aux années 50, mais ce n'est qu'à partir des années 80 que J. Daugman conçoit une méthode basée sur les ondes de Gabor. L'identification par l'iris utilise plus de paramètres que la plupart des autres méthodes d'identification et la fiabilité qui en résulte permet le passage de l'identification à l'authentification. Par contre, cette méthode est protégée par des brevets qui limitent son développement.

L'iris est la zone colorée visible entre le blanc de l'oeil et la pupille. Les stries qui forment la base des muscles ciliaires du cristallin sont stables durant toute la vie de l'individu. La forme de l'iris, c'est-à-dire l'enchevêtrement des tubes, est fixe et ne varie que très peu durant la vie de l'individu.

Par contre, la couleur (des tubes) varie un peu avec le temps (5 à 10 ans) et sous l'impact de certaines maladies.

L'iris n'est pas lié à l'ADN : les deux iris d'un individu ont a peu près la même couleur mais leur forme (enchevêtrement des tubes) est aussi différente que celle de l'iris d'une autre personne. Ainsi, deux vrais jumeaux ont quatre iris autant différenciés que ceux de deux personnes aléatoirement sélectionnées.

L'iris contient une quantité d'informations particulièrement importante, que certains n'hésitent pas à comparer à la quantité d'informations contenues dans l'ADN. Cela est probablement exagéré, mais la crainte que des informations relatives à la santé puissent être obtenues à partir de l'iris est réelle. L'iris n'occupe qu'une surface très faible. L'observation pratique à travers un système optique ne permet de déceler que des contours macroscopiques et non de descendre au niveau des tubes élémentaires. Toutefois, ceci évolue avec la précision des capteurs. Les iris sont néanmoins suffisamment variés pour qu'une approximation de l'information totale suffise à certifier l'identité d'un individu.

Les systèmes performants, en contrôlant que l'iris change de taille avec l'intensité de la lumière, ne sont même pas bernés par une image ou une lentille reproduisant le dessin de l'iris d'une personne. Cette technique **couvre seulement 6% du marché** de la biométrie car elle reste chère à mettre en œuvre et elle oblige à scanner l'œil, ce qui rebute beaucoup les utilisateurs. Cependant, votre Rapporteur a testé ces systèmes au Japon et il a pu constater leur facilité d'usage et leur absence de caractère intrusif, car il suffit de fixer à distance une caméra qui est moins exposée qu'un capteur avec contact comme pour le capteur d'empreintes.

Toutefois, l'éclairage de l'iris pose un problème de reflets car le nombre de questions à résoudre augmente presque proportionnellement avec la distance Oeil-Caméra, ce que votre Rapporteur a pu constater à l'aéroport de Tokyo-Narita.

- La rétine :

La lecture des caractéristiques de la rétine est une technologie plus ancienne que la lecture de l'iris. L'image rétinienne est capturée à l'aide d'un éclairage infra-rouge non visible et en intensité inoffensive entrant et ressortant de la pupille.

La rétine est la couche sensorielle de l'œil qui permet la vision. Cette zone est parcourue par des vaisseaux sanguins qui émergent au niveau de la papille optique, où l'on distingue l'artère et la veine centrale de la rétine qui se divisent elles-mêmes en artères et veines de diamètre plus faible pour vasculariser les cellules qui permettent la vision. La grande variété de configuration des vaisseaux sanguins présenterait la même diversité que les empreintes digitales. L'aspect des vaisseaux peut être modifié par l'âge ou la maladie, mais la position respective des vaisseaux reste inchangée durant toute la vie de l'individu et cette carte vasculaire est propre à chaque individu, elle diffère entre 2 jumeaux.

Une caméra est utilisée pour capturer la cartographie des vaisseaux, pour cela il est nécessaire d'illuminer le fond de l'œil.

Aussi, cette technologie, très précise, s'avère-t-elle bien contraignante puisqu'il faut scanner la rétine avec une lumière infrarouge intense. Une fois que les yeux sont illuminés, un balayage est réalisé pour capturer les caractéristiques de la rétine. Le procédé est donc non seulement invasif, mais aussi difficile à mettre en œuvre. De ce fait, cette technique n'a pas reçu une bonne acceptation par le grand public en raison de la nécessité de placer ses yeux à proximité de la tête de lecture du système (à moins de 4 centimètres).

Réputé comme étant l'un des plus fiables moyens biométriques, car les lecteurs de rétine identifient jusqu'à 192 points de repères, ce système souffre d'une réticence psychologique de l'usager.

- La reconnaissance faciale

Les premières études théoriques remontent au début des années 1970 et les premiers systèmes industriels ont vu le jour au milieu des années 1990.

Cette technologie a de plus en plus d'adeptes avec 15% de parts de marché. Elle s'appuie sur deux méthodes :

- la recherche des caractéristiques principales du visage comme l'écart entre les deux yeux, l'écartement des narines ou encore la largeur de la bouche, ce qui permet de construire une carte du faciès ;

- l'analyse globale de l'image du visage par des techniques statistiques.

Il existe deux moyens d'investigation. Soit le sujet est fixe et bien éclairé et la technologie est alors très au point. Soit le visage est reconnu en mouvement, sur une vidéo mais avec un fort taux d'échec.

La plupart des systèmes d'identification du visage utilisent du matériel standard, un ordinateur et une caméra pour capturer l'image.

L'image est enregistrée dans une base de données exigeant approximativement 100 à 200 octets de mémoire par image. Ces systèmes utilisent des mesures de distances entre divers éléments du visage comme moyen de vérification. Très simple à utiliser, le lecteur (caméra) est cependant coûteux.

L'authentification faciale est une biométrie relativement peu sûre. En effet, le signal acquis est sujet à des variations beaucoup plus élevées que d'autres caractéristiques. Celles-ci peuvent être causées, entre autres, par le maquillage, la pilosité, la présence ou l'absence de lunettes, le vieillissement et l'expression d'une émotion. La méthode d'authentification du visage est sensible à la variation de l'éclairage et au changement de la position du visage lors de l'acquisition de l'image. Ces variables (lunettes de soleil, moustaches et barbes,

expressions faciales anormales, inclinaison importante de la tête) peuvent causer des anomalies avec des systèmes d'identification du visage.

- Le réseau veineux

Cette technique récente semble prometteuse. Elle sonde par infrarouge le dessin du réseau veineux, soit du doigt, soit de la main. Les premiers produits viennent d'être mis sur le marché.

Des espoirs peuvent être fondés sur cette technologie qui présente de nombreux avantages, car elle permet de prendre une empreinte sans contact et sans laisser de trace, elle est en outre très difficile à déjouer par un imposteur.

- La thermographie du visage

Cette technique, proche de la précédente, avec les mêmes avantages et inconvénients, utilise une caméra infra rouge pour faire apparaître une répartition de chaleur du visage unique à chaque individu.

Cette technique est encore trop expérimentale pour susciter de longs développements. Il en va de même pour le recours à la dentition, l'odeur, la pression sanguine, la forme de l'oreille….

Les outils de reconnaissance dynamique

Il s'agit des techniques d'authentification à partir de la capacité à reproduire un geste. On emploie en général le terme de technique par apprentissage. Actuellement les recherches portent principalement sur trois techniques : la reconnaissance vocale, la reconnaissance dynamique des signatures et l'authentification par la frappe sur un clavier Ces techniques paraissent aujourd'hui plus adaptées à la sécurisation d'outils personnels (de type ordinateur ou au commerce électronique) qu'à l'accès à des zones sécurisées.

- La reconnaissance vocale :

Les recherches remontent à l'apparition du téléphone, mais l'explosion du téléphone mobile et d'internet ont fait progresser les recherches.

La vérification vocale consiste à reconnaître automatiquement l'identité d'une personne prononçant une ou plusieurs phrases en déterminant si un locuteur est bien celui qu'il prétend être, comme un auditeur humain identifie son interlocuteur au cours d'une conversation. Pour cela, le système dispose, en entrée, d'un échantillon de parole et d'une identité proclamée. Une mesure de ressemblance est calculée entre l'échantillon et la référence du locuteur correspondant à l'identité proclamée. Si cette mesure est en-dessous d'un certain seuil, le système accepte le locuteur ; dans le cas contraire, le locuteur est considéré comme un imposteur et rejeté.

Il existe plusieurs types d'applications :

- les applications «sur site» : serrures vocales pour contrôle d'accès, cabines bancaires en libre service,

- les applications liées aux télécommunications : ces applications concernent l'identification du locuteur à travers le réseau téléphonique pour accéder à un service ou pour identifier un interlocuteur ,

- les applications judiciaires : recherche de suspects, orientations d'enquêtes, preuves lors d'un jugement.

Dans le cas des applications « sur site », l'environnement de prononciation de la phrase ou du mot de passe est plus facilement contrôlé que dans le cas des applications via le réseau téléphonique (distorsions dues au canal, différences entre les combinés téléphoniques, bande passante limitée). A cela s'ajoute le fait que le locuteur peut être non-coopératif.

Le principal avantage de cette technique est d'autoriser une reconnaissance à distance. Cette technique a une bonne acceptabilité, mais présente, à l'évidence, un niveau de sécurité inférieur aux autres techniques. Il est relativement facile d'enregistrer et de reproduire une voix. Il est possible de s'affranchir de ce problème en faisant varier la phrase à prononcer, ou en couplant cette technique avec la prononciation d'un mot de passe. Mais la reconnaissance vocale nécessite aussi une excellente qualité audio, il est impossible de l'installer dans un lieu avec des bruits de fond. Enfin la technique reste assez peu fiable : deux voix ne diffèrent que d'assez peu et une même voix est sujette à variation du fait de maladies…

De fait, ces systèmes peuvent présenter un intérêt pour l'accès d'un petit nombre de personnes à une pièce peu sécurisée ou dans des applications grand public pour utiliser, par exemple, un téléphone portable.

L'identification de la voix est considérée par les utilisateurs comme une des formes les plus normales de la technologie biométrique, car elle n'est pas intrusive et n'exige aucun contact physique avec le lecteur du système.

Les systèmes d'identification de la voix se concentrent sur les seules caractéristiques de voix qui sont uniques à la configuration de la parole d'un individu. Ces configurations de la parole sont constituées par une combinaison des facteurs comportementaux et physiologiques.

La plupart des systèmes d'identification de la voix utilisent l'affichage d'un texte : des mots spécifiques doivent être lus puis parlés afin de vérifier que la personne à authentifier est bien présente et qu'il ne s'agit pas d'un enregistrement.

Il n'est pas possible d'imiter la voix d'une personne inscrite dans la base de données. La variabilité d'une personne à une autre démontre les différences du signal de parole en fonction du locuteur. Cette variabilité, utile pour différencier les locuteurs, est également mélangée à d'autres types de variabilité - variabilité due au contenu linguistique, variabilité intra-locuteur (qui fait que la voix dépend aussi de l'état physique et émotionnel d'un individu), variabilité due aux conditions d'enregistrement du signal de parole (bruit ambiant, microphone utilisé, lignes de transmission) - qui peuvent rendre l'identification du locuteur plus difficile.

Malgré toutes ces difficultés apparentes, la voix reste un moyen biométrique intéressant à exploiter, car pratique et disponible via le réseau téléphonique pour un bon niveau de fiabilité, contrairement à ses concurrents.

Toutefois, la fatigue, le stress ou un rhume peuvent provoquer des variations de la voix et générer des perturbations. La fraude est également possible avec certains dispositifs en enregistrant, à son insu, la voix d'une personne autorisée.

Une dégradation croissante des performances a été observée au fur et à mesure que le temps qui sépare la session d'enregistrement de la session de test augmente. De plus, le comportement des locuteurs se modifie lorsque ceux-ci s'habituent au système. Les modèles des locuteurs doivent donc être régulièrement mis à jour avec les nouvelles données d'exploitation du système. Les altérations de la voix dues à l'état physique (fatigue, rhume) ou émotionnel (stress), lorsqu'ils sont importants, peuvent mettre aussi en échec l'efficacité de certains systèmes.

La plupart des problèmes rencontrés en vérification vocale sont dus à une inégalité entre les conditions d'apprentissage et les conditions de test : variabilité due au locuteur, au canal de transmission ou aux conditions d'enregistrement.

Pour des raisons pratiques, les modèles doivent être mis à jour en utilisant les données d'exploitation. On peut soit ré-estimer les modèles des locuteurs en utilisant les données d'apprentissage initiales et les nouvelles données d'exploitation, soit adapter le modèle initial du locuteur avec les données d'exploitation. Cette deuxième alternative ne nécessite aucun stockage des données de sessions précédentes puisque l'adaptation se fait « en ligne ». L'adaptation des modèles est particulièrement nécessaire sur de la parole téléphonique pour prendre en compte les différentes conditions d'appel (combiné, canal, ...). Une première solution consiste à créer le modèle d'un locuteur à partir de différents environnements d'appel.

- La signature dynamique

Cette solution peut présenter un intérêt en particulier dans le commerce électronique, mais il s'agit plus d'une méthode d'authentification que d'identification et, malgré les progrès techniques, le risque de contre-façon est loin d'être négligeable.

- La frappe sur un clavier

Cette technique repose sur les particularités de chaque individu lorsqu'il frappe sur un clavier, en particulier, la force avec laquelle il frappe. En l'état actuel des techniques, cette méthode peut difficilement être regardée comme une technique de haute sécurité, mais plus comme une technique de substitution à un code pour ouvrir un appareil électronique.

2 - Analyse des défaillances techniques des systèmes biométriques.

Une analyse objective des performances techniques des systèmes biométriques et de leurs faiblesses éventuelles se heurte à diverses difficultés.

D'une part, il est malaisé d'isoler dans les systèmes biométriques les défaillances imputables aux dispositifs eux-mêmes de celles liées à l'environnement technique, physique, voire juridique dans lequel ils sont implantés. C'est ainsi que beaucoup d'études se proposant d'analyser les performances des systèmes biométriques reposent sur une confusion irréductible entre les critères permettant d'apprécier la fiabilité des produits et les contraintes devant être prises en compte lorsqu'il est envisagé de les implanter et qui déterminent largement l'opportunité d'une telle implantation eu égard aux finalités recherchées[13].

D'autre part, la diversité des techniques biométriques, dont certaines sont éprouvées dans des domaines d'application plus ou moins spécialisés et d'autres sont encore « émergentes », rend les analyses plus compliquées encore. Celles-ci privilégient en effet tantôt les résultats empiriques d'applications opérationnelles, tantôt les résultats de tests effectués dans des laboratoires, voire parfois mêlent les uns et les autres. Or ces résultats diffèrent sensiblement selon la nature de l'application, la taille des bases utilisées et l'environnement. Les

[13] Le succès ou l'échec d'un système biométrique, pour une application déterminée ne dépend pas uniquement de la fiabilité du produit lui-même ; il existe de nombreux autres facteurs qui contribuent au succès ou à l'échec final du dispositif mis en œuvre ("*The success or failure of a biometric system in a particular application is not dependant upon the reliability of the biometric product alone (...). There are many other factors that contribute to the overall success or failure of the implementation*") UK Biometrics Working Group – Use of Biometrics for Identification and Authentification – Advice on Product Selection – Issue 2.0 – 21 janvier 2003 p.4.

conclusions peuvent ainsi diverger selon que sont retenues les performances « réelles » ou les performances « virtuelles » d'un système déterminé.

Enfin, les mesures de performance issues des tests sont elles-mêmes controversées. La qualité technique des tests effectués est souvent débattue et l'impartialité des organismes généralement mise en doute.

En dépit de ces difficultés, il est possible d'identifier deux faiblesses essentielles habituellement évoquées pour mettre en doute la fiabilité des systèmes biométriques. L'une découle de la composante humaine des systèmes biométriques, l'autre provient de leur assise statistique.

a) La composante humaine des systèmes biométriques.

Schématiquement, les systèmes biométriques se proposent de comparer deux (vérification /« *one to one comparison* ») ou plusieurs (identification / « *one to many comparison* ») échantillons et de déterminer automatiquement s'il y a ou pas ressemblance des échantillons. A partir de cette ressemblance (« *match* ») ou de cette différence (« *non-match* »), on conclut que les deux échantillons apparentés proviennent de la même personne ou, au contraire, en cas de non apparentement que les échantillons ne proviennent pas de la même personne.

L'individu est ainsi sollicité à deux reprises, lors du prélèvement du premier échantillon qui servira de référence et lors du prélèvement du second échantillon qui sera comparé au précédent.

Il est, en effet, communément admis que le processus des systèmes biométriques comporte deux phases : l'enrôlement au cours duquel l'information biométrique d'une personne est ajoutée au système et la vérification / identification au cours de laquelle une nouvelle information biométrique (« *live biometric* ») est comparée à celle(s) déjà enregistrée(s), cette comparaison, automatisée, devant en principe avoir lieu dès la saisie de la seconde information (en temps réel).

Un certain nombre de procédures utilisant des données biométriques ne répondent pas à ces prescriptions. Les enquêtes menées dans le domaine de la médecine légale ou dans le cadre d'investigations policières sont, par exemple, plus sophistiquées et il revient à l'expert de prendre en compte un ensemble de données relatives notamment aux circonstances dans lesquelles les échantillons ont été collectés et d'analyser les résultats observés[14]. De même, le processus précédemment décrit se distingue de celui, également automatisé, qui consisterait à comparer deux enregistrements identiques d'un même échantillon, mais issus d'une duplication, situation qui pourrait se produire dans le cas où la même image

[14] *Cf.* Annexe 3

biométrique serait stockée sur deux supports différents (carte et base de données par exemple), le contrôle ne portant pas alors sur le détenteur de la carte, mais seulement sur l'identité des données biométriques contenues sur chacun des supports.

Toutes les études insistent sur le caractère crucial de la phase de prélèvement des échantillons (« enrôlement »). Lors de la capture des échantillons (« *samples* »), certaines caractéristiques (« *features* ») sont en effet extraites pour former le gabarit (« *template* ») qui sera utilisé pour la comparaison et la qualité du gabarit détermine largement la performance du système.

Les critiques formulées à l'encontre des systèmes biométriques portent ainsi souvent sur la difficulté à gérer la relation homme-machine[15] .

La **contrainte psychologique** est ainsi fréquemment analysée : les systèmes biométriques seraient d'autant plus efficaces que la personne coopérerait au processus. Cette notion de coopération recouvre deux caractères comportementaux, l'un relatif à ***l'acceptabilité*** du processus mis en œuvre, l'autre afférent à ***l'apprentissage*** du processus par la personne qui s'y soumet.

Sur le premier point (l'acceptabilité), les études prennent généralement en compte les réticences telles que la peur de la technique, la crainte d'une atteinte à la vie privée, l'aversion du contact physique avec un objet[16] (certaines techniques telles que la reconnaissance rétinienne sont ainsi jugées trop « intrusives ») ou l'image négative que peut avoir telle technique dans l'opinion publique (l'empreinte digitale est à cet égard souvent mentionnée).

Les difficultés d'adaptation des personnes aux exigences techniques des procédés utilisés sont aussi mises en évidence. Certaines techniques sont plus faciles à mettre en œuvre que d'autres. On a pu aussi constater[17] que l'âge, le sexe ou l'origine ethnique voire sociale (les hommes d'affaires présenteraient ainsi une meilleure aptitude pour se soumettre à un contrôle de l'iris) pouvaient affecter la performance de certaines techniques et les « faux rejets » seraient plus nombreux chez les jeunes et les personnes âgées. Le *Face Recognition Vendor Test 2002* (FRVT 2002) a ainsi révélé que, pour la reconnaissance faciale, les hommes sont plus facilement identifiables que les femmes et qu'il est plus aisé de reconnaître une personne âgée qu'un jeune individu.

---

[15] Farzin DERAVI, chercheur à l'université de Kent à Canterbury « *Audio-visual Person Recognition for Security and Access Control »*; de même le groupe de travail britannique sur la biométrie a insisté sur la relation réciproque qui s'établit entre l'homme et la technique : « *Biometric systems may be thought as a marriage between technology and human beings* » BWG *op.cit.* p.7.

[16] Ce qui peut être très important dans certaines cultures, par exemple au Japon.

[17] BWG p.18 ; *National Security Agency* « *Guidelines for placing biometrics in smartcards* » version 1.0 – 15 septembre 1998.

Cependant, si ce genre de considérations méritent d'être prises en compte pour étudier l'opportunité de l'implantation d'un système donné, elles ne paraissent pas devoir constituer un critère de performance technique. On peut remarquer d'ailleurs que, d'une part, les analyses psychologiques n'aboutissent pas toujours à des conclusions identiques[18], en raison notamment de l'imprécision des notions utilisées[19] et, d'autre part, que les appréciations formulées sur un plan général ne se trouvent pas nécessairement vérifiées *in concreto*, lorsqu'une application particulière est implantée[20].

Sur le plan technique – mais nous verrons ultérieurement que la dimension humaine de la biométrie ne doit pas être prise en compte exclusivement sur ce plan -, deux observations peuvent être formulées.

En premier lieu, le caractère contraignant de la technique utilisée qui oblige la personne à se plier aux exigences techniques du procédé constitue généralement, à l'heure actuelle, un gage d'efficacité[21]. Les techniques de reconnaissance vocale ou faciale sont plus performantes dans un environnement contraint isolant la personne des effets perturbateurs du bruit ambiant ou des différences de luminosité. Le balayage rétinien est « invasif » mais d'une grande sécurité. En général d'ailleurs, une gamme de produits plus ou moins sophistiqués permet de tenir compte de la variété des situations et des populations concernées. Ainsi dans le domaine de l'empreinte digitale, le système peut fonctionner avec un seul doigt posé (applications civiles) ou exiger l'empreinte roulée des dix

---

[18] L'appréciation de « l'acceptabilité » est ainsi variable. L'empreinte digitale est considérée comme faiblement (F. DERAVI) ou moyennement (JAIN) acceptée ; l'iris est jugée faiblement (JAIN) ou moyennement (F. DERAVI) acceptée. Il peut en aller de même pour l'appréciation des facilités d'utilisation : la voix est tantôt considérée comme très facilement utilisable (F. DERAVI) tantôt moyennement (JAIN).

[19] Tel est le cas de la notion d'acceptabilité qui est distincte de la notion de consentement. Certaines typologies de systèmes biométriques distinguent ainsi les systèmes coopératifs/non coopératifs selon que la personne a intérêt à se faire reconnaître ou au contraire qu'elle espère que le système échoue, ou encore les systèmes déclarés/non déclarés, selon qu'ils exigent une collaboration de la personne ou qui peuvent s'en passer, le « prélèvement » pouvant avoir lieu à l'insu de la personne. Si les personnes donnent facilement leurs photographies d'identité, on ne peut en conclure que la reconnaissance faciale soit fortement acceptée. En tout état de cause, il ne semble pas que les conclusions sur l'acceptabilité de tel ou tel procédé reposent sur des études statistiques sérieuses (combien de personnes interrogées ? quelles questions posées ? les personnes interrogées ont-elles préalablement été informées sur les caractères et les finalités des dispositifs analysés ?).

[20] Tel est le cas en particulier de l'empreinte digitale. Si la plupart des études font état d'une forte réticence psychologique à l'égard de l'utilisation de cette technique, on doit néanmoins constater que l'implantation, dans le domaine civil, d'applications utilisant cette technique, a été parfois bien acceptée par les usagers. Les rapports de la CNIL analysant différents projets d'implantation de tels systèmes en France révèlent ainsi que les usagers consultés les avaient préalablement acceptés ; de même, divers sondages organisés aux Etats-Unis ont montré que l'utilisation des empreintes digitales était de mieux en mieux acceptée depuis que cette technique est employée dans des domaines civils et non plus uniquement dans le domaine judiciaire.

[21] Ce n'est cependant pas toujours le cas. Ainsi au cours des auditions organisées par votre rapporteur, le procédé de la « main guidée » utilisé pour la reconnaissance de la géométrie de la main a été jugé pertinent par certains et inopportun par d'autres.

doigts (applications policières). Cette diversité de produits vise à couvrir la multiplicité des finalités des systèmes mis en place et donc des contextes d'utilisation.

En second lieu, afin de réduire les incertitudes inhérentes à la phase de capture, des paramètres de correction peuvent être intégrés. La reconnaissance faciale à partir d'images prises par des caméras de vidéosurveillance montre que la coopération des personnes n'est pas toujours nécessaire et certaines techniques contrôlent les effets de nombreux problèmes susceptibles d'affecter la qualité de l'échantillon. Les techniques de traitement d'images de plus en plus sophistiquées facilitent ainsi la lecture d'images distordues.

Plus convaincantes sont apparemment les **considérations démographiques** portant sur la ***généralité*** et la ***permanence*** d'une donnée biométrique déterminée et mettant l'accent sur la diversité, notamment dans le temps, de la personne humaine, sur les changements inévitables qui l'affectent et qui sont liés à l'âge, la maladie ou l'accident.

S'agissant de la généralité, le GAO[22] a ainsi fortement insisté sur le fait que 1 à 3% des personnes ne présentent pas la donnée biométrique souhaitée (doigts coupés, mains amputées, borgnes, muets…) et en a conclu que la reconnaissance faciale constituait de ce point de vue la technique la plus sûre[23] !

En ce qui concerne la permanence, le BWG britannique a pour sa part pris soin de préciser que cette notion couvrait une période indéfinie, mais non pas infinie. Même la technique de l'empreinte digitale dont le caractère permanent a pourtant été démontré peut se trouver altérée : le vieillissement qui rend les doigts plus secs, le travail manuel et l'usage de détergents, une blessure peuvent compromettre sa fiabilité. Le BWG a ainsi recensé divers maux affectant la performance de systèmes biométriques et aucun système n'est épargné.

Ces remarques sont certainement pertinentes. Elles révèlent qu'aucun système n'est à l'abri d'impondérables. Mais ces difficultés ne semblent pas insurmontables ; tout au plus créent-elles des sujétions techniques supplémentaires lorsqu'une application est mise en œuvre (contrôle des enrôlements, mise en place de solutions alternatives ou « multimodales » pour les personnes insusceptibles de se faire enrôler, mise à jour des données biométriques enregistrées en procédant à un nouvel enrôlement).

La composante statistique des systèmes biométriques constitue une autre limite souvent évoquée pour contester la fiabilité des systèmes biométriques.

---

[22] *General Accounting Office* (Etats-Unis) « *Biometrics for Border Security* » - Evaluation technique de l'utilisation de la biométrie pour la sécurité des frontières – novembre 2002 – GAO-03-174.

[23] Le GAO avait exclu l'ADN de son champ d'investigation.

b) La composante statistique des systèmes biométriques : les taux d'erreurs.

Il est courant de trouver dans la « littérature » consacrée aux systèmes biométriques l'assertion suivante : les systèmes biométriques ne sont pas sûrs à 100% et il est irréaliste d'espérer de tels systèmes un taux nul d'erreur.

Une telle affirmation exprime une vérité, une réalité que l'on ne saurait contester. Néanmoins, l'insistance avec laquelle cette vérité est assénée mérite d'être analysée.

Quelle technique peut en effet se prétendre infaillible et apporter la preuve d'une performance à 100% en toutes circonstances ? Pourtant, on reproche communément aux systèmes biométriques de ne pas pouvoir atteindre la perfection. L'enjeu d'un tel débat n'est pas exclusivement technique et, en fait, derrière l'argument technique, se cachent souvent des intérêts politiques et économiques visant soit à empêcher l'application des techniques biométriques, soit à en retarder le développement. En effet, le déploiement des techniques biométriques non seulement effraie pour des raisons qui seront examinées ultérieurement, mais est aussi susceptible de remettre en cause des positions économiques acquises ou en voie d'être consolidées (producteurs de cartes, sécurité informatique notamment). La concurrence qui s'exerce sur le marché des techniques biométriques lui-même a fait de la performance un critère d'arbitrage, de choix entre les différentes techniques proposées. Alors que certains produits sont depuis plusieurs années opérationnels, la plupart des technologies en sont encore aux stades de la recherche et de l'expérimentation et plus les techniques seront testées, plus elles seront performantes.

Si la question des taux d'erreurs est essentielle, on assiste actuellement à une véritable « guerre des taux » qui ne peut que nuire à un examen serein des enjeux en présence.

Trois approches peuvent être identifiées dans ce domaine, l'une mettant en doute l'unicité d'une donnée biométrique déterminée, l'autre insistant sur le caractère approximatif des systèmes de vérification ou d'identification fondés sur une donnée biométrique, la troisième visant à comparer les taux d'erreurs des différents systèmes.

La question de l'***unicité*** est importante puisque les systèmes biométriques prétendent relier une donnée à une personne. Elle recouvre en fait deux problèmes : l'unicité du caractère biométrique choisi et l'unicité de la mesure ou de la représentation graphique de ce caractère, l'un comme l'autre devant être propres à une seule personne.

Parce que l'unicité d'une donnée biométrique n'a jamais été scientifiquement démontrée, la biométrie repose sur des méthodes statistiques destinées à déterminer la probabilité que deux personnes présentent la même donnée.

Le GAO[24], dans l'annexe consacrée à l'empreinte digitale qui pourtant avec la rétine constitue l'une des données biométriques ayant fait l'objet de travaux scientifiques les plus sérieux depuis longtemps[25], a émis de nombreuses réserves. Après avoir noté que l'inspection manuelle de millions d'empreintes digitales avait conduit à reconnaître le principe de leur unicité, le GAO a rappelé que cette unicité n'avait jamais été formellement établie par des procédés scientifiques. Après avoir indiqué que le fichier du FBI était le plus étendu au monde avec 400 millions d'empreintes digitales et que le FBI n'avait jamais constaté deux empreintes digitales identiques provenant de deux personnes distinctes, le GAO a observé qu'aucun test n'avait été mené pour vérifier si les empreintes digitales enregistrées dans ce fichier étaient véritablement uniques, remarquant de surcroît qu'en mars 2000 le *National Institute of Justice* avait lancé une étude scientifique pour démontrer rigoureusement l'unicité des empreintes digitales.

Sur un plan pratique, la pertinence des interrogations portant sur l'unicité peut être considérée comme relative. Tout dépend en effet du taux de probabilité qu'une personne ait la même donnée qu'une autre. Cette probabilité varie selon la technique utilisée. Ainsi, pour dix points de comparaison, la probabilité de trouver les mêmes points disposés de façon identique sur les empreintes digitales de deux personnes différentes serait d'une chance sur un million et, pour 14 à 17 points, d'une chance sur 17 milliards[26] . En revanche aucun test n'aurait été réalisé pour déterminer la probabilité que deux personnes puissent avoir la même voix ou le même visage[27]

Par ailleurs, la performance technique d'un système biométrique est mesurée sur la base de différents ***taux d'erreurs***, la tolérance zéro étant irréaliste[28]. Comme l'a souligné une étude émanant du gouvernement canadien, les techniques biométriques ne sont pas exactes à 100% ; elles restent approximatives, même si les caractéristiques humaines prises en compte étaient uniques. Cette approximation résulte des imprécisions des techniques appliquées

---

[24] p.101.

[25] Il est vrai que ces travaux sont anciens. La commission d'accès à l'information du Québec précise ainsi que, pour les empreintes digitales, dès le XIXème siècle Galton, physiologiste, anthropologue et psychologue avait établi l'unicité et la permanence des 24 régions qu'il avait identifiées, avec une probabilité de $1{,}45 \times 10^{-11}$. En 1936, le Dr Carleton Simon et le Dr Isadora Golstein menèrent des travaux sur les vaisseaux sanguins de la rétine et 20 ans plus tard, le Dr Paul Tower, dans une étude sur les jumeaux, confirma cette unicité. Pour la voix, en 1962, Laurence Kersta, un ingénieur aux Bell Laboratories, établit que la voix de chaque personne était unique.

[26] Criminalistique et criminologie – http://www.ifrance.com. En 1911, devant l'Académie française des sciences, le Pr Balthazard a démontré que le risque de trouver deux personnes ayant 17 points identiques était de 1 sur 17 milliards. Il en va de même en matière d'empreintes génétiques : lorsqu'il y a une similitude entre deux profils génétiques, une étude préalable de populations permet de définir la fréquence de ce profil dans la population concernée.

[27] P. Jonathon Philipps, Alvin Martin, C.L. Wilson, Mark Przybocki (NIST) – "*An introduction to evaluating biometric systems*" – IEEE – 2000.

[28] BWG " *Tolerance of zero errors is inachievable*".

et des différentes circonstances dans lesquelles les caractéristiques humaines sont présentées et mesurées[29].

Une étude consacrée à l'analyse statistique des performances des systèmes utilisant l'empreinte digitale[30] notait ainsi que la probabilité que quelqu'un d'autre ait une configuration identique était suffisamment faible pour écarter une fausse acceptation, mais que celle-ci demeurait, car l'utilisation de systèmes automatiques comportant des paramètres destinés à introduire une plus grande flexibilité pour détecter les caractères distordus et donc réduire le nombre de faux rejets, conduisait à augmenter la probabilité de fausses acceptations.

- FMR (" *False Match Rate*") et FAR ("*False Acceptation Rate*")

Ces taux déterminent la probabilité pour un système de « reconnaître » une personne qui normalement n'aurait pas dû être reconnue.

Le FMR, parfois appelé « false positive rate », indique la probabilité pour un système d'apparenter de façon erronée une personne à une donnée biométrique enregistrée.

Dans un système d'authentification ou d'identification positive, un apparentement erroné revient à autoriser l'accès à une personne qui n'était pas autorisée à y accéder. Dans un système d'identification négative où il s'agit de vérifier que la personne n'est pas déjà référencée dans le système pour lui accorder l'accès, l'apparentement erroné conduira à lui refuser l'accès alors qu'elle remplit les conditions pour y accéder.

Le taux de fausses acceptations est, quant à lui, le ratio entre le nombre de personnes qui ont été acceptées alors qu'elles n'auraient pas dû l'être et le nombre total de personnes non autorisées qui ont tenté de se faire accepter. Il se réfère généralement à la notion d'imposteur (rapport entre le nombre d'imposteurs qui sont de façon erronée acceptés et le nombre total d'imposteurs s'étant présentés)[31].

- FNMR (« *False Non-match Rate* ») et FRR (« *False Rejection Rate*")

Ces taux déterminent la probabilité pour un système donné de ne pas « reconnaître » une personne qui normalement aurait dû être reconnue.

---

[29] "*Biometrics are implicitly not 100% unambiguous ; they are close. Even though human characteristics may be unique, the technology and techniques used for measuring these characteristics have a built-in tolerance. This is due to inaccuracies of the applied techniques and the different circumstances under whitch the characteristics are presented and measured*" EWA-Electronic Walfare Associates – Canada – "*Biometric technology security evaluation under the common criteria*" – Version 1.2 – Septembre 2001 p.18.

[30] RODDY et STOSZ – "*Fingerprint Features – Statistical analysis and system performance estimates*" – 10/02/1999.

[31] *National Security Agency* op.cit. Ainsi, si le FAR est de 1 %, cela signifie qu'une personne sur 100 ayant essayé de pénétrer dans le système est susceptible de réussir.

Le FNMR, parfois appelé « *false negative rate* » mesure la probabilité pour un système de ne pas apparenter une personne à sa donnée biométrique enregistrée. Dans un système d'authentification ou d'identification positive, un faux apparentement conduit à refuser l'accès à une personne pourtant autorisée à y accéder et dans un système d'identification négative, à permettre l'accès à une personne qui aurait dû être rejetée.

Le taux de faux rejets (FRR) est le ratio entre le nombre de personnes autorisées dont l'accès a été refusé et le nombre total de personnes autorisées s'étant présentées.

Les deux types de taux (FMR et FNMR ou FAR et FRR) sont reliés de façon inverse. A l'extrême, un FMR nul aboutit à ce que le FNMR soit égal à 1 et inversement un FNMR nul aboutit à porter le FMR à 1. Cela signifie que l'excès de rigueur dans la comparaison, en exigeant une similitude totale des éléments comparés, conduit à rejeter tout le monde ou, ce qui revient au même à n'accepter personne (aucun apparentement) et qu'à l'inverse un laxisme excessif dans la comparaison aboutit à accepter tout le monde ou, ce qui revient au même, à ne rejeter personne (aucun non apparentement).

Il existe, en effet, forcément une zone d'incertitude où il est difficile d'arbitrer parce que les éléments que l'on compare sont très ressemblants bien que provenant de deux personnes différentes ou qu'ils présentent des différences bien qu'issus de la même personne. Les systèmes définissent donc un seuil permettant de gérer les écarts entre le gabarit enregistré et l'échantillon réel et généralement les producteurs fournissent les moyens de contrôler ce seuil pour leur système. Par exemple, pour une application visant à contrôler l'accès de personnes autorisées à une zone hautement sécurisée, le FAR devra être le plus bas possible au risque d'augmenter le taux des rejets erronés.

D'autres taux sont utilisés, tels que l'EER (« *Equal Error Rate* ») qui définit un compromis généralement retenu pour les applications civiles consistant à obtenir une égalité entre le FFR et le FAR ou entre le FMR et le FNMR ou encore le FTER (« *Failure To Enrol Rate* ») qui mesure la probabilité qu'une personne ne puisse être enrôlée pour des raisons physiques tenant à la personne ou techniques liées au dispositif de capture. Mais l'augmentation du taux d'échec à l'enrôlement, lorsqu'elle est délibérée et destinée à éliminer les images de mauvaise qualité ne pouvant servir de référence pour les comparaisons futures peut permettre une diminution des taux d'erreurs (FM ou FNM).

Si ces différents taux permettent de donner une mesure objective de la performance d'un système donné, ils ne peuvent à l'heure actuelle servir de ***critères de comparaison***.

D'une part en effet, actuellement, seuls certains systèmes, dans un nombre limité d'environnements par application, ont été testés[32] et les méthodes de test en sont elles-mêmes à un stade d'essai. Des paramètres de performance ont été définis en laboratoire mais n'ont pas été vérifiés dans un environnement réel.

Les résultats théoriques paraissent prometteurs puisque des FMR de 1 sur 100 000, 1 sur 1 000 000 000, voire 1 sur 10^{78} et des FNMR de 1%, 0,1% ou 0,01% sont affichés.

Mais une certaine suspicion demeure. On assiste en effet aujourd'hui à une véritable « guerre des taux » qui reflète la concurrence s'exerçant sur le marché, voire des segments de celui-ci, et les comparaisons ne paraissent pas toujours impartiales, ni très sérieuses[33], faute d'organisme agréé de certification.

Néanmoins plusieurs bases de données biométriques ont été constituées pour les tests (NIST, NBTC *National Biometrics Test Center* de San José en Californie, Programme AFIS *Automated Fingerprint Identification System*, le projet ESPRIT dans le cadre du *National Physical Laboratory* au Royaume Uni ou encore le projet BIOTEST engagé dans le cadre européen).

A titre d'exemple, le *National Physical Laboratory* britannique a publié récemment [34] un test comparatif de huit techniques réalisé sur la base de 200 volontaires s'étant soumis trois fois, à trois occasions, à la procédure de test, lequel a ainsi porté sur 1 800 gabarits pour chaque technique et 2 millions de combinaisons. Les résultats sont présentés dans le tableau suivant qui révèle, pour le FAR, un écart de 1 à 10 entre le deuxième algorithme et le premier algorithme utilisés pour la reconnaissance des empreintes digitales :

---

[32] Dans un article publié en 2000, des chercheurs américains du NIST (*National Institute of Standards and Technology*) rappelaient que la voix, les empreintes digitale et la face avaient fait l'objet des plus nombreux tests et études et que pour l'iris, les évaluations indépendantes avaient été plus tardives et plus rares. La reconnaissance faciale a été évaluée en 1996/1997 dans le cadre du programme FERET (*Face recognition technology*) et les résultats ont montré que les taux FAR-FRR variaient sensiblement en fonction des changements d'illumination, de position et des caméras utilisées. Pour la voix, testée par le NIST, les résultats variaient aussi de façon importante, comme d'ailleurs pour l'empreinte digitale. En conclusion, les auteurs observaient que les buts recherchés étaient déterminants lors du choix d'un système. *« An introduction to evaluating biometric Systems* » – IEEE – 2000. D'après une étude récente du Center for Mathematics and Scientific Computing du National Physics Laboratory (Royaume Uni) intitulée « *Biometric Product Testing Final Report* » du 19 mars 2001, la reconnaissance par l'iris garantit un taux de fausse acceptation nul pour 2 millions comparaisons – *http://www.iriadiantech.com*

[33] Le GAO n'a pas échappé à la critique du Département de la Justice sur ce point qui lui a reproché de comparer en quelque sorte des « carottes et des navets ». Le fichier IAFIS (*Integrated Automated Fingerprint Identification System*) du FBI affiche quant à lui un FMR de 1,5 x 10^{-12}, un FNMR de 1,5 à 2% et un FTER de 0,5% pour les criminels et de 2,5% pour les autres.

[34] *"Biometric Product Testing Final Report, Issue 1.0"* 19 mars 2001, *Centre for Mathematics and Scientific Computing*, *NPL*, Teddington, Royaume Uni.

Techniques testées	*FAR*	*FRR*	*FER*
Iris	0,0001 %	0,25 %	~ 0,5 %
Empreintes digitales (2)*	0,008 %	2,5 %	~1 %
Voix	0,03 %	2 %	~ 0
Empreintes digitales (1)*	0,08 %	6 %	~1 %
Géométrie de la main	0,70 %	0,5 %	~0
Empreintes digitales (optique)	0,45 %	11 %	~2 %
Face	0,45 %	17 %	~ 0

* Algorithmes différents

Des travaux sont par ailleurs en voie de réalisation pour définir de « bonnes pratiques » dans le domaine des tests de performance des produits biométriques. Telle est notamment la fonction du *Biometric Working Group* britannique.

3 - Comparaison des systèmes biométriques

L'analyse comparée des performances respectives des différentes techniques biométriques constitue un élément essentiel pour les décideurs publics ou privés et, depuis quelques années, les travaux de comparaison se sont multipliés. La perspective d'un développement de ces techniques dans le domaine civil notamment et l'apparition de nouvelles technologies biométriques expliquent en grande partie l'intensification des recherches dans ce domaine.

Néanmoins, la décision s'avère particulièrement difficile pour diverses raisons. D'une part, les comparaisons ne sont pas encore établies sur des bases réellement consensuelles. Elles prennent par ailleurs en compte une multiplicité de critères, ce qui semble plus dérouter les décideurs que les aider dans leur choix. D'autre part, alors que la décision devrait reposer sur deux choix successifs, le premier portant sur le principe de l'implantation d'un système biométrique et le second sélectionnant la technique biométrique qui sera utilisée, en l'occurrence, les deux choix paraissent intrinsèquement liés et dépendent de l'objectif poursuivi comme du contexte dans lequel le projet s'inscrit.

Le BWG a ainsi pris soin de préciser qu'aucune technique biométrique ne peut seule répondre à toutes les exigences et que, de surcroît, une solution biométrique n'est pas forcément adaptée à un besoin déterminé[35] pour lequel d'autres solutions peuvent sembler plus adéquates.

[35] "*No single biometric technology offers a solution to all user requirements. Furthermore, a biometric solution of your requirement is not always the best approach! Often, analysis of the*

Ce flou constitue un frein certain à la diffusion des techniques biométriques, l'investissement dans une technique déterminée impliquant le risque de choisir la mauvaise technique[36] .

Aussi assiste-t-on actuellement à diverses expériences visant à tester dans un environnement réel la performance de systèmes biométriques préalablement sélectionnés.

a) La variété des critères de comparaison.

Au Canada, l'EWA (*Electronic Warfare Associates*)[37] a entrepris une étude sur l'évaluation des systèmes biométriques d'authentification et d'identification. Dans cette étude sont distingués deux niveaux d'analyse : les tests de performance destinés à apprécier les unes par rapport aux autres les différentes applications et les tests de sécurité visant à déterminer les conditions de conformité d'un dispositif aux exigences de sécurité fonctionnelle et d'assurance, dans la perspective d'aider les consommateurs à choisir le produit qui leur convient le mieux.

Selon cet organisme, du point de vue de la sécurité, trois caractéristiques sont jugées essentielles : la robustesse, définissant le degré de stabilité de l'élément biométrique pendant une période donnée, la capacité de discrimination (unicité), la fiabilité des tests conduisant à déterminer le niveau de robustesse et d'unicité (« *evidence* »). Sur la base de ces trois critères, un « potentiel biométrique » est défini permettant d'apprécier la sécurité donnée par les différents systèmes.

Le tableau suivant, issu du rapport de l'EWA, synthétise les résultats provenant de différentes sources et concernant les paramètres ci-dessus énoncés :

---

requirement will reveal that existing solutions are adequate, or may be enhanced by other, non-biometric means" op.cit. p.4.

[36] "Biométrie, mythe et réalité", *Deutsche Bank Research*, 22 mai 2002 : *« As a consequence, an investment in a specific biometric system implies the risk of choosing the wrong technology. This poses a sizeable barrier to the diffusion of biometric technologies"*.

[37]" *Biometric technology security evaluation under common criteria*" – version 1.2 – septembre 2001.

Biométrie	Robustesse	Unicité	Fiabilité*	Potentiel
Empreintes digitales	Moyen - Haut	Haut	Très haut	Haut
Géométrie de la main	Moyen – Haut	Haut	Moyen	Moyen - Haut
Iris	Haut	Très haut	Haut	Haut – Très haut
Rétine	Haut	Très haut	Haut	Haut – Très haut
Face	Moyen	Haut	Bas	Moyen
Signature	Bas – Moyen	Moyen	Bas	Bas – Moyen
Voix	Moyen	Moyen - Haut	Moyen - Haut	Moyen – Haut
Odeur	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu
Oreille	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu
Imagerie thermique	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu
Frappe sur un clavier	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu

*des tests de robustesse (permanence) et d'unicité (capacité discriminante)

Ces appréciations recoupent peu ou prou celles issues d'autres recherches. Ainsi, par exemple, les travaux conduits en 1999[38], qui comparaient quatorze caractères sur la base de sept critères et de trois niveaux (haut, moyen et bas), donnaient un haut niveau de performance à l'empreinte digitale, l'iris, la rétine et l'ADN, tandis que la main (géométrie et veines), la voix et l'oreille bénéficiaient d'une note moyenne. S'agissant de l'universalité, de l'unicité et de la permanence, l'iris, l'odeur et l'ADN démontraient un haut niveau pour chacun des critères, l'empreinte digitale avait un niveau haut pour ce qui concerne l'unicité et la permanence mais moyen en matière d'universalité, tandis que la rétine obtenait un haut niveau pour l'universalité et l'unicité mais un niveau moyen pour la permanence.

[38] JL Wayman "*Technical testing and evaluation of biometric identification devices" "Biometrics:Personnal Identification in Networked Society*" (A. Jain, R. Bolle and S. Pankanti eds). Avaient été évalués : la reconnaissance faciale, les empreintes digitales, la géométrie de la main, la frappe sur le clavier, les veines de la main, l'iris, la rétine, la signature, la voix, la thermographie, l'odeur, l'ADN, la démarche et l'oreille. Les critères retenus étaient : l'universalité, l'unicité, la permanence, la facilité du « prélèvement » (*collectability*), la performance, l'acceptabilité et la « résistance » à la falsification (*circumvention*).

Caractères *Biometrics*	Universalité *Universality*	Unicité *Uniqueness*	Permanence *Permanence*	Facilité de collecte *Collectability*	Performance *Performance*	Acceptabilité *Acceptability*	Robustesse *Circumvention*
Face	Haut	Bas	Moyen	Haut	Bas	Haut	Bas
Empreinte digitale	Moyen	Haut	Haut	Moyen	Haut	Moyen	Haut
Géométrie De la main	Moyen	Moyen	Moyen	Haut	Moyen	Moyen	Moyen
Frappe sur le clavier	Bas	Bas	Bas	Moyen	Bas	Moyen	Moyen
Veines de la main	Moyen	Moyen	Moyen	Moyen	Moyen	Moyen	Haut
Iris	Haut	Haut	Haut	Moyen	Haut	Bas	Haut
Rétine	Haut	Haut	Moyen	Bas	Haut	Bas	Haut
Signature	Bas	Bas	Bas	Haut	Bas	Haut	Bas
Voix	Moyen	Bas	Bas	Moyen	Bas	Haut	Bas
Thermographie Faciale	Haut	Haut	Bas	Haut	Moyen	Haut	Haut
Odeur	Haut	Haut	Haut	Bas	Bas	Moyen	Bas
ADN	Haut	Haut	Haut	Bas	Haut	Bas	Bas
Démarche	Moyen	Bas	Bas	Haut	Bas	Haut	Moyen
Oreille	Moyen	Moyen	Haut	Moyen	Moyen	Haut	Moyen

Jain, 1999

Les travaux d'évaluation prennent ainsi en compte d'autres critères, en plus de ceux liés à la permanence, l'universalité, la généralité et aux taux d'erreurs. Sans prétendre être exhaustif, on peut néanmoins citer outre l'acceptabilité et la facilité d'utilisation déjà mentionnées, le temps d'enrôlement, le temps de comparaison, la complexité des algorithmes et la taille des gabarits[39], la capacité pour le système de déterminer si l'échantillon provient d'une personne vivante, la résistance aux facteurs environnementaux (froid, humidité, éclairage…), la facilité d'intégration, les besoins de maintenance et de formation, les coûts…

[39] Le rapport du GAO fournit les informations suivantes : face : 84 ou 1 300 octets ; empreintes digitales : 250 à 1 000 octets ; main : 9 octets, iris : 512 octets ; rétine : 96 octets ; signature : 1 000 à 3 000 octets ; voix : 10 000 à 20 000 octets.

L'International Biometric Group, une société américaine d'intégration et de conseil, a établi un classement en forme d'étoile de huit techniques biométriques en retenant quatre critères, le caractère plus ou moins « intrusif », la fiabilité, le coût et la facilité d'utilisation.

Les résultats de cette étude peuvent être présentés comme suit :

- des techniques les moins « intrusives » aux plus « intrusives » : la voix, la frappe sur le clavier, la signature, la main, la face, l'empreinte digitale, l'iris et enfin la rétine.

- des techniques les plus fiables aux moins fiables : l'iris, la rétine, l'empreinte digitale, la face, la main, la voix, et enfin à un niveau équivalent, la frappe sur le clavier et la signature.

- des techniques les moins chères aux plus chères : la frappe sur le clavier, la voix, la signature, l'empreinte digitale, la face, la main, la rétine et enfin l'iris.

- des techniques les plus faciles d'utilisation aux plus difficiles : la face, la signature, l'iris, la frappe sur le clavier, la voix, l'empreinte digitale, la main et enfin la rétine.

b) Le caractère déterminant des finalités et la préférence actuelle pour une démarche empirique et expérimentale

La variété des critères d'évaluation reflète la diversité des effets attendus de l'implantation d'un système biométrique dans un environnement particulier. On ne peut, à l'heure actuelle tout au moins, déterminer ***la*** technique qui répondrait le mieux à tous les objectifs recherchés, dans tous les domaines d'application. Or, si l'utilisation des techniques biométriques est susceptible d'apporter une réponse adaptée à un certain nombre de problèmes, la recherche d'une solution unique à toutes les éventualités qui peuvent se présenter aboutit semble-t-il à un blocage, comme si le choix était si difficile que l'inertie paraissait à bien des égards préférable.

De ce point de vue, le rapport du GAO s'avère significatif. Il s'agissait en l'occurrence d'évaluer les conditions de mise en œuvre d'une technique biométrique pour la sécurité des frontières. Les enjeux étaient considérables, tant sur le plan interne qu'au niveau international. D'une part, le domaine d'application était très vaste, compte tenu des dimensions frontalières, du nombre de points d'entrée officiels placés sur ses frontières (400) et du nombre de personnes entrant sur le territoire des Etats-Unis (500 millions en 2001, dont les deux-tiers de nationalité étrangère). D'autre part, les enjeux économiques et sociaux étaient considérables, liés aux coûts d'installation et de maintenance (entre 1,3 et 2,9 milliards de dollars pour la mise en place de « visas

biométriques » et entre 0,7 et 1,5 milliard par an ensuite) et aux incidences d'une utilisation des systèmes biométriques sur les usagers. En troisième lieu, les répercussions politiques paraissaient très importantes, notamment sur le plan international.

En dépit du contexte juridique précis dans lequel s'inscrivaient les travaux du GAO - de nouvelles lois votées par le Congrès américain exigeant que d'ici la fin 2004, tous les postes frontières puissent procéder à l'authentification des visas et documents d'entrée américains - ses conclusions restent très mitigées. Cette position s'explique aisément par l'importance des bouleversements susceptibles d'être générés par l'implantation d'un système biométrique d'une telle ampleur et qui ont été soigneusement analysés. Mais on ne peut manquer d'observer que la finalité exacte du dispositif envisagé restait floue, la sécurité recouvrant une multiplicité de procédés. C'est ainsi que le GAO a examiné quatre scénarios différents : vérification à partir d'une liste de contrôle préalablement à la délivrance de documents de voyage, même vérification mais préalablement à l'entrée sur le territoire, délivrance de « visas biométriques » et délivrance de « passeports biométriques ». Pour les deux premiers scénarios, la reconnaissance faciale a été retenue, car les photographies sont souvent les seules données biométriques disponibles sur les personnes interdites d'entrée sur le territoire. Pour les deux autres, l'étude a porté sur la reconnaissance faciale, l'iris et l'empreinte digitale. Dans ses conclusions, le GAO a émis de nombreuses réserves et insisté sur la place des dispositifs non exclusivement techniques dans le domaine de la sécurité mais le Département de la justice - qui a notamment pour mission de contrôler les passagers dans les zones frontalières - s'est montré très critique à son égard : il a observé, notamment, que la lutte contre le terrorisme se trouvait « marginalisée », la délivrance de visas ne concernant que 3% des visiteurs et rappelé que les procédures actuelles de contrôle des frontières ne permettent pas de prévenir efficacement l'entrée de terroristes.

D'autres exemples, plus modestes, révèlent le caractère déterminant des finalités recherchées pour choisir une technique biométrique plutôt qu'une autre. En particulier, il semble nécessaire de déterminer clairement si l'on entend mettre en place un dispositif d'authentification ou d'identification ainsi que le niveau de sécurité exigé.

On peut ainsi constater que face aux incertitudes techniques liées, notamment, à la diversité des résultats des tests effectués et des environnements, les démarches expérimentales et empiriques semblent privilégiées par les utilisateurs.

Tel est notamment le cas de certains dispositifs expérimentés dans les aéroports afin de contrôler l'accès à des zones réservées ou les flux de passagers sur certains vols[40].

Aéroports de Paris a ainsi mené une expérience sur six mois à partir de mars 2002, pour le contrôle d'accès des personnels aux zones d'accès limité dans la perspective d'accélérer et de sécuriser le système actuel de contrôle de 80 000 personnes qui repose sur la délivrance d'un badge et la vérification « manuelle » dudit badge par comparaison avec une pièce d'identité.

Le processus retenu par ADP comprend à la fois l'expérimentation de techniques utilisées dans un environnement réel et l'exécution de tests en laboratoire qui ont été confiés à la société THALES et qui sont actuellement en cours.

L'expérimentation, conformément aux orientations définies par la CNIL, a été menée avec la collaboration volontaire de 5 000 personnes sur trois sites, dont deux à Orly et un à Roissy. 190 000 contrôles ont été effectués pendant six mois. Les contrôles ont porté sur trois techniques préalablement sélectionnées, l'empreinte digitale, l'iris et la main, la reconnaissance faciale ayant été écartée car jugée insuffisamment fiable lors du lancement de l'expérimentation.

Plusieurs enseignements ont été tirés de cette expérience. D'une part, les systèmes permettent d'accélérer sensiblement le processus de vérification (de l'ordre de 30%), dès lors que la phase d'apprentissage a été concluante. D'autre part, les taux de faux rejets ont été variables : 0,1% pour l'empreinte digitale, 0,2% pour la main et 8% pour l'iris dont le processus d'apprentissage est le plus long et le plus difficile. Enfin, des recommandations ont été adressées aux producteurs afin que les besoins des utilisateurs soient mieux pris en compte, tant en ce qui concerne l'adaptation des techniques d'enrôlement aux gestes humains, les systèmes actuels paraissant parfois trop rigides, que la maîtrise par les utilisateurs eux-mêmes des taux de sensibilité, ce qui leur permettrait de moduler le degré de sécurité exigé en fonction des circonstances.

De même, une réflexion est en cours au sein de l'administration pénitentiaire concernant le contrôle à distance des détenus placés sous surveillance électronique qui n'étaient que 90 en janvier dernier mais dont le nombre devrait croître sensiblement, la loi de programme sur la justice fixant un objectif de 3 000 mesures et 750 bracelets électroniques devant être déployés d'ici la fin de l'année. Cette extension rend nécessaire la sécurisation du « contre-appel », l'identification de la personne qui répond reposant actuellement dans les neuf centres expérimentaux actuels sur la base d'un questionnaire permettant de

[40] On peut citer les expériences menées par l'aéroport anglais d'Heathrow (contrôle par l'iris), à Berlin (reconnaissance faciale), ou l'expérimentation menée par Air France sur les vols Paris-Tel Aviv qui a concerné sept vols et environ 400 passagers.

vérifier les connaissances du détenu (prénom de l'épouse par exemple), ce qui ne permet pas de lutter efficacement contre les usurpations d'identité.

Une étude a donc été engagée et réalisée par une société qui a recommandé la reconnaissance vocale en raison des contraintes de coût et des facilités d'utilisation que cette technique présente. La technique vocale a été retenue en effet car ce système n'implique pas l'installation de lecteurs qui devraient être maintenus et récupérés au terme de la période de placement sous surveillance électronique. Le taux de fausses acceptations reste néanmoins élevé, mais le dispositif est conçu comme un élément complémentaire et, en tout état de cause, les contrôles actuels basés sur le questionnaire s'avèrent eux-mêmes très aléatoires.

II - Espoirs et craintes à l'égard de l'usage des techniques biométriques d'identification

Les systèmes biométriques d'identification fascinent et inquiètent[41].

Cependant le débat ne se résume pas à une opposition irréductible entre les tenants des systèmes biométriques et leurs opposants.

En fait, la valeur des systèmes biométriques ne peut se mesurer dans l'absolu. On ne peut prouver qu'ils sont foncièrement bénéfiques et qu'ils apportent une garantie totale dans tous les domaines, comme on ne peut établir qu'ils sont intrinsèquement nocifs. De telles prises de position seraient excessives.

En revanche, la valeur des systèmes biométriques doit s'apprécier de manière relative, c'est-à-dire par rapport aux autres procédés actuellement utilisés pour identifier et authentifier les personnes et ce, tant sur le plan de la sécurité, que sur celui du respect des droits des personnes[42]. L'évaluation des systèmes biométriques devrait ainsi, pour être complète, s'accompagner d'une évaluation des autres dispositifs que les systèmes biométriques sont appelés à remplacer ou à compléter.

En outre, on oppose souvent les bienfaits dans le domaine de la sécurité des biens et des personnes que peuvent procurer les systèmes biométriques aux dérives qu'ils sont susceptibles de provoquer sur le plan des libertés. En réalité, depuis quelques années, on a pris conscience que la sécurité constitue une garantie pour l'exercice des libertés et une sorte de dialogue s'est instauré entre ceux qui sont « fascinés » par les techniques biométriques et ceux qui sont « inquiets » de leur développement, cet échange ayant porté ses fruits, notamment dans le domaine technique.

---

[41] Jennifer STODDART, Présidente de la commission d'accès à l'information du Quebec, "Des technologies de surveillance sous surveillance" – 23ème conférence internationale des commissaires à la protection des données – 24-26 septembre 2001.

[42] Des travaux ont été engagés au sein du *National Research Council* américain et un pré-rapport a été établi à ce sujet. *« Who goes there ? Authentification Through the Lens of Privacy ». Computer Science and Telecommunications Board* – 2003.

1 - Une sécurité garantie ?

L'argument promotionnel des techniques biométriques d'identification est presque exclusivement basé sur l'idée de sécurité au sens large.

Si historiquement, les techniques biométriques d'identification ont été utilisées dans le domaine policier pour faciliter la recherche des criminels, leur extension dans le domaine civil a conduit à un élargissement de la notion de sécurité, laquelle s'étend à la prévention de fraudes et à la sécurité juridique des personnes.

A la suite notamment des attentats survenus aux Etats-Unis en septembre 2001, l'intérêt d'une utilisation des techniques biométriques d'identification a été mis en exergue pour renforcer les moyens de lutte contre le terrorisme.

Les techniques biométriques d'identification sont ainsi présentées comme un moyen efficace de protection des biens et des personnes.

Certaines réserves sont néanmoins émises à ce sujet et deux types d'objections sont formulées à ce propos : les techniques biométriques ne seraient pas à l'abri d'un risque de falsification et le risque informatique devrait être pris en considération.

Aussi divers travaux ont-ils été engagés pour renforcer la sécurité de ces techniques.

a) Les atouts des systèmes biométriques

La mise en évidence des avantages d'une utilisation des systèmes biométriques repose sur une critique des méthodes d'authentification ou d'identification actuellement pratiquées.

Ces méthodes se fondent soit sur la possession d'un objet (carte, passeport, clef), soit sur des connaissances (code – *PIN Personnal Identification number* – mot de passe), soit sur un dispositif qui associe une carte et un code (*ATM - Automatic Teller Machine*) et qui assure une plus grande sécurité, mais reste vulnérable.

Or ces méthodes qui reposent sur « ce que l'on détient » ou « ce que l'on sait » présentent des défauts : un objet peut être perdu ou volé et un code ou un mot de passe peuvent être oubliés ou usurpés. L'identité entre le possesseur légitime de l'objet et le détenteur qui le produit n'est pas garantie. De même,

l'identité entre la personne à laquelle a été attribuée un code ou un mot de passe et celle qui l'utilise n'est pas vérifiée.

En revanche, les procédés biométriques s'attachent à « ce que l'on est » : la caractéristique biométrique est intrinsèquement liée à la personne et elle ne peut être reproduite facilement. Elle ne peut donc être aisément utilisée par un imposteur. Dépendants d'une caractéristique physique, biologique ou comportementale d'une personne déterminée, il n'est pas requis que celle-ci fasse un effort de mémorisation ou qu'elle conserve en sa possession un objet particulier.

Les systèmes biométriques constituent donc un instrument efficace de ***lutte contre la fraude*** dont les effets économiques et politiques sont loin d'être négligeables et constituent un véritable défi pour les sociétés développées.

Farzin DERAVI a ainsi souligné les motivations financières du développement des techniques biométriques. La sécurité des transactions est, en effet, essentielle pour le développement futur du commerce électronique et il y a de sérieux doutes sur les garanties offertes par les solutions actuelles. Les codes et les numéros d'identification comme les cartes n'apportent aucune information sur l'identité de la personne qui les utilise peut-être à mauvais escient. Un système d'identification permettrait par ailleurs de détecter les fraudes ou les intrusions.

Une enquête menée par le FBI auprès de 241 organisations a ainsi montré que 49% d'entre elles avaient été confrontées à des vols électroniques ou à des usages illicites de leurs réseaux représentant une perte globale pour les organisations concernées de 136,8 millions de dollars.

La fraude concernant les cartes de crédit est quant à elle estimée à l'échelle mondiale à 4 milliards de dollars US. Selon la *Federal Trade Commission*, les usurpations d'identité, c'est-à-dire l'utilisation frauduleuse de l'identité d'une autre personne, représentaient 42% des plaintes déposées auprès de la FTC en 2001 et 62% de ces usurpations étaient liées aux cartes de crédit ou à la fraude bancaire et avaient constitué une perte pour les services financiers de l'ordre de 98 millions de dollars. Dans l'Union européenne, cette fraude est actuellement estimée par la commission européenne à 600 millions d'euros par an, soit environ 0,07 % du chiffre d'affaires du secteur.

En 1998 différents travaux ont été engagés aux Etats-Unis pour étudier les conditions d'un déploiement des techniques biométriques dans ce domaine. Ainsi, par exemple, à l'initiative de la *National security agency,* des orientations ont été définies pour intégrer la biométrie dans les cartes à mémoire, les technologies apparaissant les plus adaptées alors étant l'empreinte digitale, la reconnaissance vocale et la reconnaissance faciale. Aux Etats-Unis, la Chambre des Représentants a, le 20 mai 1998, procédé à diverses auditions pour apprécier

les possibilités offertes par les systèmes biométriques dans les secteurs financiers et bancaires[43].

Mais la fraude électronique n'est pas la seule en cause. L'usage frauduleux de documents est malheureusement très répandu sans que l'on puisse disposer d'estimations précises sur ce point. Le rapport du GAO indique ainsi qu'en 2000 114 000 documents frauduleux ont été interceptés à la frontière, dont un tiers concernant des passeports ou des visas américains.

L'examen des législations comparées de différents pays européens concernant les cartes nationales d'identité[44] révèle une tendance vers la généralisation[45] et la sécurisation des cartes par divers procédés, et notamment l'introduction d'éléments biométriques, essentiellement les empreintes digitales. Néanmoins, dans la plupart des pays la donnée biométrique ne figure pas sur la carte elle-même. A l'exception du Portugal dont la carte comporte l'empreinte digitale de l'index droit, aucun pays ne fait figurer cette donnée sur la carte d'identité[46], étant toutefois précisé qu'en règle générale les cartes contiennent les photographies et la signature du titulaire. L'Espagne, l'Italie et la France procèdent ainsi seulement, lors de l'établissement des cartes, au relevé des empreintes digitales qui sont ensuite « archivées ».

Au cours des entretiens organisés par votre rapporteur, il lui a été indiqué que la mise en circulation des cartes d'identité infalsifiables s'était accompagnée en France d'un développement de la fraude « en amont », non seulement pour la carte d'identité mais aussi pour les passeports. De vrais titres sont ainsi délivrés sur la base de faux éléments d'identité (fausses pièces d'état civil ou pièces d'une autre personne).

La biométrie peut ainsi éviter un usage frauduleux de documents mais aussi renforcer la fiabilité du titre délivré. Une réflexion a été engagée en France depuis un an et se poursuit sur la mise en place d'un ***« titre fondateur »***[47] permettant de sécuriser la délivrance des titres mais aussi de simplifier les démarches des administrés, d'alléger les tâches de l'administration et de faciliter le développement de l'*e*-administration. L'intégration d'une donnée biométrique

---

[43] "*Biometrics and the future of money"* http///commdocs.house.gov/committees/bank

[44] Note du service des études juridiques du Sénat – février 2003 – http://wwww.Senat.fr

[45] A l'exception du Danemark qui dispose d'un fichier national de la population ; même au Royaume-Uni une réflexion est en cours visant à instituer une carte d'identité sur laquelle pourraient figurer des éléments biométriques, tels que l'empreinte digitale ou l'iris.

[46] En Allemagne, la possibilité d'introduire sous forme codée des données biométriques est prévue mais cette introduction reste subordonnée à l'intervention d'une loi fédérale qui devra déterminer l'élément biométrique susceptible d'être incorporé et en Italie un décret du 22 octobre 1999 relatif à la carte d'identité électronique prévoit que celle-ci puisse comporter tous les éléments nécessaires au calcul de la clé biométrique.

[47] Ce projet devrait être présenté avant l'été au gouvernement, aux maires et à la CNIL, de telle manière qu'une expérimentation soit possible en 2004, en vue d'un démarrage effectif en 2005 – Réponse du ministre de l'intérieur, de la sécurité intérieure et des libertés locales *JO Questions Sénat* – 20 février 2003 p.632.

dans un ou plusieurs titres constitue l'une des mesures envisagées dans le cadre de ce programme.

Cette question avait d'ailleurs été évoquée dans le livre blanc « Protection des données personnelles et administration électronique », publié en février 2002 par le gouvernement précédent, une triple évolution étant alors envisagée par le ministère de l'intérieur, à l'occasion du renouvellement des chaînes de production de la carte d'identité : la procédure de délivrance des titres d'identité, la numérisation de la carte d'identité et l'adjonction d'une fonction de signature électronique avec incorporation d'éléments de sécurisation tels que, par exemple, l'empreinte digitale.

Dans le domaine de la ***sécurité des échanges***, nécessaire au développement de l'administration électronique, la mission a observé que « la cryptographie à clef publique semble devoir être la technique à partir de laquelle il est possible de traiter simultanément ou de manière séparée ces trois éléments » que sont l'authenticité (prouver son identité à un interlocuteur, établir l'origine du message), la confidentialité et l'intégrité des données. Mais dans le cadre de l'examen des outils de sécurité, le rapport conclut cependant que « les solutions reposant sur des mesures biométriques cumulent les avantages des solutions immatérielles (absence de déploiement) et matérielles (on possède au sens physique la clef d'accès) »[48].

L'idée a en effet été parfois évoquée que la signature biométrique pourrait jouer un rôle dans le processus de génération des clés cryptographiques ou même servir de moyen de cryptage de la clé elle-même, avec l'avantage que l'utilisateur n'a pas à s'en rappeler et peut la produire à tout moment[49]. Dans cette perspective, « la clé biométrique » qui repose sur les propriétés probabilistiques des gabarits biométriques est présentée comme un substitut efficace aux clés secrètes qui peuvent être volées, cassées ou perdues.

Au demeurant, le sixième programme cadre européen de recherche et de développement mentionne au sein de l'objectif stratégique « vers un cadre

---

[48] La mission avait émis néanmoins une double réserve : d'une part, une forte incertitude technique et financière sur leur déploiement à grande échelle faisait, selon la mission, douter de l'utilisation des techniques biométriques à court terme et, traditionnellement liées à la surveillance et à la répression de la criminalité, elles apparaissaient excessives au regard des finalités de l'administration électronique courante.

[49] John DAUGMAN du Laboratoire informatique de l'Université de Cambridge – « *Biometric Key Cryptography* » - http://www.iridiantech.com
De même, lors d'un colloque organisé à Ottawa le 17 septembre 1996 sur les technologies d'amélioration de la confidentialité, ont été évoqués les avantages d'un système de chiffrement biométrique visant à protéger la vie privée et l'anonymat des empreintes digitales. George TOMKO, PDG de Mytec Technologie (actuellement dénommée Biopscrypt) a montré qu'en transformant une empreinte digitale en un cryptogramme, le chiffrement biométrique peut, sous certaines conditions, être utilisé pour authentifier l'identité et autoriser l'accès à des données sans compromettre l'anonymat du consommateur.

global de fiabilité et de sécurité » la recherche pluridisciplinaire sur la biométrie et ses applications.

En outre le recours aux techniques biométriques dans le domaine social aux Etats-Unis s'explique largement par le ***caractère peu fiable du système d'immatriculation*** utilisé par les administrations américaines.

Le numéro de sécurité sociale (SSN – *Social Security Number*) institué en 1936 et étendu en 1943, est en principe utilisé exclusivement par l'administration sociale. Mais dès 1961, les services des impôts (IRS - *Internal Revenue Service*) l'ont utilisé pour les contribuables et le numéro, comme la carte de sécurité sociale, sont désormais couramment utilisés dans le monde du travail, des affaires ou de l'éducation.

Pour fiabiliser le numéro de sécurité sociale, l'ANSI (*The American National Standards Institute*) avait proposé de définir dans les années 1970 un identifiant national incorporant le numéro de sécurité sociale, mais le projet fut retiré compte tenu de l'opposition du public américain à la notion de registre national ou de système unifié d'identification.

A la suite d'un rapport établi en 1980 par le Contrôleur Général qui estimait que 4,2 millions d'américains disposaient de plusieurs numéros, une loi (*The Social Security Amendments*) permit en 1983 à l'administration sociale de mettre en place un système de vérification et des cartes infalsifiables et une autre loi (*The Comprehensive Crime Control Act*) introduisit en 1984 la biométrie.

Dans les années 1990, plusieurs Etats américains ont alors utilisé l'empreinte digitale pour lutter contre la falsification d'identité permettant l'attribution de prestations à une seule et même personne se présentant sous plusieurs identités.

L'Etat de New-York a ainsi estimé que le « bénéfice » réalisé grâce à l'introduction de cette technique biométrique s'élevait à 42,6 millions de dollars sur l'année, 15 % des bénéficiaires ayant été rejetés par le système. Pour l'Etat du New Jersey, un taux de 12 % était affiché. Dans le comté de Los Angeles, le bénéfice annoncé était de l'ordre de 66,5 millions de dollars et l'Etat du Connecticut espérait, en 1996, économiser 7,5 millions de dollars la première année d'application[50].

---

[50] Néanmoins, un rapport établi en avril 1996 (*« Privacy issues surrounding personnal identification systems »* - James LABAN) soulignait que les économies réalisées n'étaient pas forcément liées à la détection directe des fraudeurs, mais au refus de certains bénéficiaires de se faire enrôler, l'Etat du Connecticut ayant lui-même insisté lors de l'institution de son système biométrique sur l'aspect dissuasif du dispositif plus que sur l'objectif de constatation des fraudes.
De surcroît, le montant des économies réalisées ne peut être établi sur une base certaine. En 1998, les chiffres suivants étaient présentés devant une sous-commission de la Chambre des Représentants, pour l'Etat de New York : durant les 19 premiers mois d'application, 925 000 personnes avaient été enrôlées, 172 cas de fraude avaient été constatés et 37 000 dossiers avaient

b) Les réserves émises à ce sujet

Plusieurs réserves ont été formulées sur la capacité des techniques biométriques de remédier aux insuffisances des systèmes actuels d'authentification ou d'identification.

Certaines d'entre elles se fondent sur ***une comparaison des systèmes biométriques et des systèmes traditionnels***, au niveau de maturité qui est respectivement le leur actuellement.

Ainsi par exemple une étude entreprise par la *Deutsche Bank*[51] souligne les défauts des systèmes biométriques par rapport aux modes actuels d'authentification, notamment dans le domaine bancaire c'est-à-dire dans un secteur marchand de masse où les personnes à authentifier sont des clients, où les opérateurs doivent tenir compte des contraintes de coût et où la sécurité constitue un élément essentiel[52] .

Selon cette étude, les systèmes traditionnels, comme les systèmes biométriques, sont vulnérables et sont soumis aux mêmes types d'attaques ou de manipulations. Un « hacker » peut ainsi intercepter le gabarit de référence ou le gabarit présenté lors de la phase de comparaison. Néanmoins, les conséquences ne sont pas les mêmes car, si un nouveau mot de passe ou un nouveau code peuvent être attribués, la caractéristique biométrique, elle, ne peut être modifiée et la solution consistant à associer une donnée biométrique à une carte exige l'implantation d'une double infrastructure (lecteur biométrique et lecteur de carte) et donc des coûts plus importants.

Par ailleurs, si les systèmes traditionnels d'authentification , en particulier dans le secteur bancaire, font l'objet de systèmes de certification et d'évaluation standardisés, en revanche, pour la plupart des techniques biométriques, le processus de standardisation est loin d'être achevé.

Enfin, alors que l'utilisation d'un mot de passe ou d'un numéro de code produit une réponse sûre à 100 % (vrai ou faux), la comparaison biométrique fait subsister un taux d'incertitude et le client « valide » risque d'être rejeté sans pourtant avoir commis la moindre erreur.

été fermés, représentant une économie de 314 millions de dollars, selon les propos tenus par J.S. DUNN, Président du *Biometric Consortium* ; en revanche, selon M. NITSCHE-RUGGLES de la SAGEM, les deux premières années d'application du programme new-yorkais avaient représenté une économie de 100 millions de dollars.

[51] *Deutsche Bank Research* « Biométrie, mythe et réalité », 22 mai 2002.

[52] L'étude indique ainsi que les pertes liées à la fraude de la carte Visa International Germany se sont élevées à 18,2 millions d'euros en 2001 ; ce qui ne représente que 0,14 % du volume des transactions.

L'auteur de cette étude en conclut que les dispositifs biométriques ne constituent pas une solution viable à court terme[53], mais qu'ils permettent d'assurer une meilleure sécurité des systèmes traditionnels sans toutefois prétendre les remplacer. La garantie d'un plus haut niveau de sécurité générant des coûts supplémentaires et offrant une moindre facilité d'utilisation, l'appui complémentaire des systèmes biométriques ne se justifie, selon lui, que pour la protection de zones de haute sécurité, telles que les sites nucléaires, ou pour des besoins militaires.

D'autres critiques mettent en évidence les ***incidences pratiques des taux d'erreurs*** et insistent sur la difficulté de trouver un compromis acceptable entre l'exigence de sécurité et la nécessité de ne pas troubler exagérément la ***tranquillité publique***.

L'étude précitée a ainsi mesuré les effets concrets des systèmes de surveillance basés sur la reconnaissance faciale à partir d'images filmées. Une évaluation conduite par le département de la défense américain[54] a révélé qu'avec un taux de fausses alarmes réduit à 1%, seulement 22 % des personnes recherchées étaient correctement identifiées lorsque l'angle de position variait. Un tel dispositif installé dans un aéroport assurant un flux de 100 000 voyageurs par jour permettrait probablement d'identifier un certain nombre de personnes recherchées qui emprunteraient cet aéroport, mais il conduirait aussi à détecter comme criminels 1 000 voyageurs innocents par jour, ce qui mobiliserait les forces de sécurité pour contrôler la situation de ces personnes identifiées de manière erronée.

Dans le même esprit, le *Parliamentary Office of Science and Technology* britannique, dans son rapport consacré à l'utilisation des systèmes biométriques[55], a observé que sur 63 millions de passagers transitant par l'aéroport d'Heathrow chaque année, un système biométrique utilisant l'empreinte digitale avec un taux de fiabilité de 98 % génèrerait plus d'un million d'erreurs par an, ce nombre étant réduit à 63 000 erreurs avec un taux de 99,9 %, ce qui représenterait tout de même mille erreurs chaque semaine en moyenne et serait susceptible d'ébranler la confiance des passagers et des équipes de sécurité.

Face aux doutes exprimés sur le niveau de sécurité garanti par les systèmes biométriques, diverses recherches ont été entreprises pour assurer une plus grande « sécurisation » desdits systèmes.

---

[53] Pour Armin Grüneich, les systèmes de surveillance biométrique ne peuvent présenter d'utilité significative dans la recherche des criminels à court ou moyen terme. Il estime que l'emploi des systèmes biométriques pour protéger des zones requérant un niveau intermédiaire de sécurité, tels que les aéroports, les usines et les bureaux est subordonné à l'arrivée à maturité de ces systèmes, soit deux à six ans. Pour la sécurité des réseaux et des produits électroniques, leur déploiement ne devrait pas être assuré avant une dizaine d'années.

[54] DoD *Counterdrug Technology Development Program Office, Facial Recognition Vendor Test 2000* – Rapport d'évaluation 16 février 2001.

[55] « *Biometrics and Security* », *Postnote* n° 165, novembre 2001.

Le risque de ***falsification*** (utilisation de lentilles de contact, reproduction d'empreintes digitales …) a été ainsi pris en considération. Certains produits sont ainsi censés détecter le caractère « vivant » ou artificiel de l'élément corporel présenté (cas des empreintes digitales notamment, certains lecteurs prenant en compte la chaleur des doigts, ou de l'iris, en vérifiant la réaction de l'œil à la lumière).

Des recherches ont par ailleurs été effectuées pour tester les résultats de systèmes reposant sur deux ou plusieurs données biométriques (***la « biométrie multimodale »***), mais les conclusions ne sont pas unanimes sur ce point.

De nombreux documents présentent en effet la biométrie multimodale comme un moyen efficace de renforcer la performance des systèmes biométriques. Plusieurs combinaisons sont envisageables : indépendamment et, dans ce cas, la personne est « acceptée » lorsque chaque test a donné un résultat positif, parallèlement et, dans ce cas, la personne est acceptée si au moins l'un des tests a donné un résultat positif. Des travaux sont par ailleurs engagés pour étudier les conditions dans lesquelles la décision finale pourrait résulter d'une « fusion » logique des opérations de comparaison[56].

Dans un système de comparaisons indépendantes où la décision d'acceptation intervient si chaque test a été passé avec succès, les fausses acceptations diminuent, mais les faux rejets augmentent[57]. En revanche, dans un système de comparaisons concurrentes où la décision d'acceptation s'aligne sur l'un des tests passé avec succès, les faux rejets diminuent, mais les fausses acceptations augmentent[58].

John DAUGMAN du *Computer Laboratory* de l'Université de Cambridge, qui a développé les algorithmes de la reconnaissance par l'iris, considère ainsi qu'un produit biométrique performant devrait être utilisé seul car les dispositifs multimodaux aboutissent, selon les cas, à ce que le taux de fausses acceptations soit meilleur que le plus fort avec un taux de faux rejets pire que le moins bon ou inversement[59].

---

[56] Farzin DERAVI, à propos d'une combinaison de la voix et du visage.

[57] Dans ce cas en effet le FAR final est égal au produit des FAR correspondant aux dispositifs utilisés.

[58] Dans ce cas en revanche le FRR final est égal au produit des FRR correspondant aux dispositifs utilisés.

[59] Par exemple, il a démontré que dans un système multimodal utilisant une technique dont l'EER est 1% et une autre technique dont l'EER est 1 ‰, testé avec 100 000 « imposteurs » et 100 000 « authentiques », les résultats s'établissent comme suit :

- combinaisons indépendantes (« et ») : 1 099 faux rejets et 1 fausse acceptation, soit 1 100 erreurs,
- combinaisons concurrentes (« ou ») : 1 099 fausses acceptations et 1 faux rejet, soit 1 100 erreurs.

Enfin, des travaux ont été engagés par divers organismes pour définir des ***standards de sécurité*** garantissant l'intégrité et l'inviolabilité des données traitées, notamment sur la base de la norme dite des « critères communs ».

2 - Des libertés compromises ?

Comme en contrepoint des arguments présentés par les promoteurs des systèmes biométriques qui se réfèrent essentiellement au principe de sécurité, leurs détracteurs soulignent les atteintes aux libertés que peut susciter un déploiement de tels systèmes.

Une analyse des opinions exprimées à ce sujet montre, d'une part, que les oppositions les plus virulentes sont formulées dans les sociétés de culture anglo-saxonne et, d'autre part, que les critiques s'inscrivent largement dans la problématique relative à la protection nécessaire des libertés individuelles face à la généralisation des techniques informatiques.

En fait, peu de critiques ont une portée générale ou systématique qui conduiraient à rejeter les systèmes biométriques dans leur ensemble et la plupart d'entre elles ne peuvent être correctement analysées que si l'on prend en considération le contexte national, tant culturel que juridique, dans lequel elles s'expriment.

D'ailleurs, les critiques formulées ont parfois été contestées et un certain nombre de ces objections ont été prises en compte par les producteurs eux-mêmes ou leurs organismes professionnels.

a) Les critiques formulées à l'encontre des systèmes biométriques

Trois niveaux d'analyse peuvent être identifiés. Le premier assimile la biométrie à une « technique répressive ». Le second repose sur la notion de vie privée. Le troisième se fonde sur les principes qui ont conduit à l'adoption de législations sur la protection des personnes face au développement de l'informatique en insistant sur les risques d'interconnexion liés à l'utilisation d'un identifiant biométrique.

La première conception émane essentiellement de personnalités isolées tandis que les deux autres approches sont plus généralement adoptées par

---

Le test de la première technique aurait donné 2 000 erreurs et le test de la deuxième technique aurait produit 200 erreurs. Dès lors, le système multimodal combinant les deux conduit globalement à 5,5 fois plus d'erreurs que le meilleur des deux tests.

des institutions publiques ou privées, et plus particulièrement les instances indépendantes mises en place pour protéger les données personnelles.

Roger CLARKE, professeur à l'*Australian National University*, abondamment cité dans les études relatives aux systèmes biométriques, représente la première sensibilité. Pour cet auteur, la biométrie constitue pour les libertés l'une des menaces les plus sérieuses parmi les « ***techniques de surveillance*** »[60] , ce qui explique, selon lui, le développement de ces techniques dans les pays autoritaires et leur application, dans les pays démocratiques, au contrôle de populations déterminées telles que les prisonniers, les salariés ou les personnes prises en charge par des services sociaux.

Le recours à la biométrie présente, selon cet auteur, des dangers particuliers qu'il a énumérés dans une étude diffusée en avril 2001 et qui peuvent être regroupés en deux catégories.

La première est d'ordre général et ne concerne pas spécifiquement la biométrie. Il s'agit, d'une part, de menaces liées aux systèmes informatiques (collecte de données sur les individus, multiplication des informations sur leur comportement, leurs déplacements et leurs actions, connexion facilitée par le recours à un identifiant unique des systèmes créés à l'origine pour des finalités précises, utilisation des données collectées pour restreindre les libertés individuelles) et, d'autre part, des positions personnelles de l'auteur en faveur du droit à l'anonymat et de la liberté d'utilisation de pseudonymes.

La seconde catégorie s'attache aux caractéristiques propres à la biométrie : celle-ci donne une information intrinsèquement liée à la personne elle-même (distinction entre « *information about the person* » et « *information of the person* ») ; la personne doit se soumettre physiquement au processus de vérification ; en cas de falsification ou d'usurpation, elle ne pourra pas se défaire de ses caractéristiques biométriques et pourra difficilement apporter la preuve qu'elle n'a pas commis les actes qui lui sont imputés.

Roger CLARKE a examiné les garanties susceptibles d'être apportées. Ni une autorégulation par les producteurs ou les utilisateurs, ni l'application des dispositions juridiques existantes ne lui semblent efficaces. Une évaluation des impacts sociaux reposant sur une large consultation et des procédures d'étude et de contrôle transparentes serait, à ses yeux, nécessaire et la définition d'une législation spécifique reste subordonnée à l'établissement de standards de sécurité qui devraient s'imposer aux producteurs et aux importateurs, aux installateurs et aux utilisateurs de systèmes biométriques[61]. Aussi propose-t-il comme solution un moratoire sur l'application de la biométrie.

---

[60] « *Biometrics and Privacy* » 2001, "*Human Identification in Information Systems : Management Challenges and Public Policy Issues* 1994 – http://www.anu.edu.au

[61] Roger CLARKE propose également des interdictions strictes en matière de collecte et de stockage de données biométriques (interdiction de création, de maintenance et d'utilisation d'une

Pour diverses organisations, tant publiques que privées, le développement de certains systèmes biométriques est susceptible de menacer la ***vie privée*** des individus, cette notion renvoyant au concept d'intimité.

Dans le cadre de ce courant de pensée, est parfois établi un lien entre les cartes d'identité et la biométrie, mais les réserves émises à ce sujet ne semblent ni unanimes, ni absolues, compte tenu, d'une part, de la diversité des systèmes juridiques relatifs à l'identité des personnes et, en particulier des régimes des titres d'identité et, d'autre part, du développement des procédures d'identification qui sont multiples (numéro d'immatriculation, cartes notamment) et dont les finalités sont elles-mêmes très variées.

Au sein des techniques biométriques, deux d'entre elles font l'objet cependant de critiques sévères, comme en témoigne le dernier rapport de l'*Electronic Privacy Information Center*[62] . Il s'agit de l'identification génétique et de la reconnaissance faciale basée sur un système de vidéo-surveillance.

S'agissant des empreintes génétiques, les craintes reposent à la fois sur le développement des recherches sur l'origine génétique de certaines maladies, voire de certains comportements, la constitution de bases nationales de plus en plus étendues concernant les auteurs de crimes ou de délits et les indices prélevés sur les lieux où ont été commis des crimes ainsi que les idées émises par certaines personnalités qui ont suggéré de collecter l'ADN dès la naissance[63].

En ce qui concerne les systèmes de reconnaissance faciale dont la fiabilité est d'ailleurs largement mise en doute, la critique porte essentiellement sur les effets jugés néfastes d'une utilisation de plus en plus répandue des caméras de vidéo-surveillance qui permettent de contrôler une population de plus en plus large sans que celle-ci en ait conscience[64].

Une étude diffusée par l'ACLU (*American Civil Liberties Union*)[65] et portant sur l'expérience de reconnaissance faciale par vidéo-surveillance menée dans la ville de Tampa en Floride concluait que cette technique n'était pas assez fiable pour justifier une mise en application qui représente de nombreuses menaces pour la vie privée.

La troisième approche met l'accent sur la ***protection des personnes*** vis-à-vis des conditions de collecte et d'utilisation des données biométriques.

---

base de données biométriques) et recommande le recours à deux caractéristiques pour les procédés d'authentification.

[62] « *Privacy and Human Rights* » 2002 – EPIC – Washington – *Privacy International London.*

[63] L'EPIC cite l'ancien maire de New York et un élu australien.

[64] Il convient d'observer que si l'EPIC évoque les dangers liés aux interceptions téléphoniques, il n'aborde pas la question de la reconnaissance vocale.

[65] « *Drawing a Blank : The failure of Facial Recognition Technology in Tampa, Florida*" – janvier 2002 –Ce système de vidéo-surveillance associé à un dispositif de reconnaissance faciale avait été mis en oeuvre à l'occasion du *Super Bowl* organisé à Tampa en Floride en janvier 2001.

La CNIL a ainsi abordé dans ses trois derniers rapports les problèmes spécifiques posés par les systèmes biométriques au regard des principes définis par la loi de 1978, dite « Informatique et Libertés »[66].

La « doctrine » de la CNIL sera examinée ultérieurement. Mais il convient de souligner à ce stade que la CNIL a mis en exergue deux risques principaux. D'une part, les éléments biométriques laissant des traces lui paraissent plus dangereux que les autres. Tel est le cas notamment de l'ADN et de l'empreinte digitale, mais aussi de la reconnaissance faciale associée à un système de vidéo-surveillance. Pour la CNIL, « l'empreinte digitale est presque aussi redoutable que les traces d'ADN » car elle est omniprésente : où que l'on aille, il est impossible de ne pas laisser de traces de sa présence[67]. D'autre part, la CNIL estimait qu'il « pourrait presque être soutenu que l'empreinte digitale est aux autres données biométriques ce que le NIR[68] est aux autres données personnelles : une information particulière qui présente un risque réel de relâchement du principe de finalité des fichiers ».

Dans le même esprit, la Commission d'accès à l'information du Québec[69] considère qu'une « mesure biométrique est plus qu'un identifiant numérique » car elle livre « des informations personnelles intimes sur la composition de notre corps et sur notre comportement en général » et s'est inquiétée de l'utilisation d'un « identifiant intime, unique et universel » qui rend très faciles le croisement des données provenant de multiples sources et le « traçage » des individus.

b) Les contre arguments présentés sur ce point

Divers arguments ont été opposés à ceux dénonçant les menaces que représente l'utilisation des systèmes biométriques pour les libertés et les droits des personnes.

En premier lieu, la ***détresse des victimes*** est parfois mise en avant, la notion de sécurité recouvrant à la fois la répression des contrevenants, la prévention des infractions et l'amélioration de la vie quotidienne des citoyens.

---

[66] En outre, dans le cadre de la 23ème Conférence internationale des commissaires à la protection des données qui s'est tenue à Paris les 24-26 septembre 2001, plusieurs interventions ont porté sur la biométrie.

[67] Rapport d'activité n°21 – 2000.

[68] Le numéro d'inscription au répertoire (NIR) est composé de 13 caractères qui se rapportent au sexe, à l'année, au mois, au département puis à la commune (n° INSEE) de naissance ainsi qu'à un numéro d'ordre et qui sont suivis d'une clé de contrôle. Le NIR est unique (deux personnes ne peuvent avoir le même) et invariable (pour les personnes nées en France, il est attribué à la naissance, et ne change plus ultérieurement, quelles que soient les modifications administratives que connaissent les communes ou les départements).

[69] « La biométrie au Québec : les enjeux », Document d'analyse, juillet 2002.

Tel est l'argument essentiel présenté par les promoteurs du système de reconnaissance faciale associé à un dispositif de vidéo-surveillance mis en place à Newham, dans la banlieue de Londres.

Lors de la dernière conférence internationale des commissaires chargés de la protection des données, R. Lack a ainsi rappelé qu'une étude conduite en 1997 et 1998 sur l'utilisation des techniques pour renforcer le sentiment de sécurité des habitants et diminuer la criminalité avait démontrer qu'un lien existait entre les inquiétudes ressenties par le public et la prise de conscience des risques encourus par les délinquants. Lors de l'implantation du dispositif, 75% des 250 000 habitants vivaient dans la crainte d'être agressés et actuellement ce taux a été ramené à 67% et continue à diminuer. Le dispositif a par ailleurs fait l'objet d'une large publicité et comporte de nombreuses garanties. Au début de l'année 1998, un sondage d'opinions avait révélé que 67% des personnes interrogées y étaient favorables et le dispositif a recueilli 93% d'opinions favorables à la fin de l'année 1999, le questionnaire ayant pris soin de demander aux personnes interrogées d'exprimer leurs opinions en prenant en considération les conséquences qui pouvaient résulter de la mise en place du dispositif sur les droits de l'homme, les droits civils et la vie privée. Le système de comparaison repose sur les fichiers de la police concernant les personnes condamnées pour crime et impliquées dans de telles affaires au cours des douze dernières semaines. Les fiches des personnes sont examinées par la police au moins toutes les douze semaines. Seuls sont sauvegardés les visages scannés correspondant « sans aucun doute » à une personne fichée et toutes les zones couvertes par le système sont signalées au public.

En second lieu, les systèmes biométriques sont présentés comme des instruments efficaces de ***protection des données personnelles***.

A titre d'exemple, le huitième rapport d'activité du Préposé fédéral à la protection des données (Suisse)[70] contenait les conclusions d'une étude menée par une école d'ingénieurs mandatée par le PFPD qui tendaient à démontrer que les systèmes d'authentification par empreintes digitales étaient techniquement au point et remplaçaient avantageusement l'authentification classique par mots de passe. Il y était affirmé que « ces nouvelles techniques d'authentification biométrique constituent **le seul espoir** de progrès dans le domaine de la sécurité d'accès aux innombrables services électroniques proposés par le marché » et qu'une « diffusion à large échelle de ces dispositifs d'authentification biométrique contribuera certainement à abaisser leur prix et surtout à améliorer le niveau général de sécurité et de protection des données ». Selon les termes de ce rapport, « comme la transformation d'une empreinte digitale en un gabarit est irréversible, il n'y a aucun risque de reconstitution d'empreinte à partir d'un gabarit, et du fait

[70] http://www.edsb.ch. Toutefois, dans son neuvième rapport d'activité, le PFPD a observé que « mis à part les avantages du point de vue de la sécurité et de la protection des données, l'identification biométrique implique également des risques considérables », et insisté sur la nécessité d'assurer la sécurité des systèmes d'exploitation biométriques.

que cette transformation n'est à l'heure actuelle pas du tout standardisée, il n'y a que très peu de risques de mise en relation, par le biais de gabarits correspondants, de bases de données censées rester indépendantes. Pour garantir cette indépendance qui préserve en fait la pseudonymité de l'utilisateur, il faut soit recourir à des caractéristiques physiques différentes pour chaque service, soit crypter individuellement chaque base de gabarits ou empreintes ».

Cette question a été largement débattue aux Etats-Unis devant la sous-commission de la Chambre des Représentants en mai 1998 et il n'est pas inutile d'exposer les arguments avancés sur ce point.

James L. WAYMAN, Directeur du *National Biometric Test Center* (Université de San José) a ainsi rappelé que les nombres émanant d'une donnée biométrique ne peuvent pas être utilisés pour reconstruire la taille et la forme de la partie du corps concernée et qu'ils n'ont aucune valeur en dehors du système qui les a produits[71]. Les systèmes biométriques ne peuvent trouver un individu ou le suivre, à l'exception des empreintes digitales et de la reconnaissance rétinienne. Mais le premier procédé repose sur un nombre tel de technologies différentes que les systèmes ne peuvent pas en fait communiquer et la deuxième technique exige une coopération des intéressés. Aussi le Professeur WAYMAN n'a-t-il pas hésité à placer le gabarit de son empreinte digitale sur son site *internet*, en précisant qu'il n'aurait certainement pas exposé ainsi le numéro de sa carte de crédit, le code de sa carte bancaire, ni le nom de jeune fille de sa mère et en insistant sur le fait que le gabarit de ses empreintes digitales est absolument inutilisable en dehors du système qui l'a créé. M. WAYMAN a même convié le FBI à télécharger ce gabarit qui, en tout état de cause ne lui sera d'aucune utilité.

John D. WOODWARD JR, *Attorney-at-law*, pour sa part a affirmé que les techniques biométriques ne menaçaient pas par elles-mêmes la vie privée, mais qu'au contraire, elles constituaient de réelles garanties au regard du respect de la vie privée[72] car elles assuraient l'intégrité de l'information, évitaient l'usurpation d'identité et permettaient de limiter l'accès aux données sensibles. A ce titre, elles font partie des techniques protectrices de la vie privée (*PET – Privacy enhancing technology*). Afin de prévenir les abus dans le secteur privé, M. D. WOODWARD préconisait la définition d'un code de bonnes pratiques en

---

[71] « *I want to talk a little bit about the fingerprint data that is encrypted on the front of the card. It is not the fingerprint that is encrypted on this card. It is numbers coming from the fingerprint that are put in the code on the card. There is no way to reverse that process and to reconstruct the fingerprint from those numbers. That is very, very important thing to note. Even if these numbers were sent to the FBI, the FBI could not reconstruct the fingerprint. These numbers are totally worthless to any other system but the specific system that created the card. That is true of all biometric devices.* ***The numbers that emanate from your biometric data cannot be reconstructed to produce the size and shape of the body part in question, nor are they of any value anyplace outside of the system that produced them***."

[72] « *Biometrics should not be automatically construed as privacy's foe. Quite to the contrary, biometrics is privacy's friend"*; John D.Woodmard est un auteur fréquemment cité, depuis notamment la publication d'une étude en 1997 intitulée "*Biometrics :Privacy's Foe or Privacy's Friend »* (Proceedings of the IEEE, vol.85, n°9, septembre 1997 p.1487).

observant que l'intervention régulatrice de la puissance publique dans ce secteur pouvait promouvoir les techniques biométriques. Il a ainsi défini les orientations suivantes : interdiction stricte de prélever « clandestinement » des données biométriques dans le secteur privé ; reconnaissance pour chaque individu du droit de déterminer si sa donnée biométrique peut figurer dans une base de données et les conditions dans lesquelles elle peut être utilisée ; possibilité pour chaque individu de corriger ou modifier sa donnée ; interdiction, sous réserve du consentement de l'intéressé, de divulguer la donnée à une autre partie, des exceptions raisonnables pouvant être définies dans le domaine de la recherche et dans celui de la lutte contre la criminalité ; obligation pour l'organisation gestionnaire d'une base de données biométriques de garantir la sécurité et la sauvegarde des données.

Enfin, le représentant de la SAGEM, M. NITSCHE-RUGGLES, a observé qu'une donnée biométrique restait une « identité anonyme », un gabarit ne donnant aucune indication sur le sexe de la personne, sur son âge, sur sa couleur de peau, sur sa taille, son poids, ni la couleur de ses cheveux, à la différence d'un document tel qu'un permis de conduire, lequel peut par ailleurs contenir des informations erronées.

En mars 1999, l'*International Biometric Industry Association* (IBIA)[73] qui regroupe plusieurs entreprises de développement, de production et d'intégration et qui a été constituée en septembre 1998, a défini un certain nombre de ***principes visant à préserver la vie privée***.

Dans le secteur privé, elle préconise l'adoption de « politiques » exposant clairement les conditions de collecte, de stockage, d'accès et d'utilisation d'une donnée biométrique et préservant le droit des personnes de s'opposer à la diffusion de cette donnée pour des finalités autres que celles initialement fixées. Dans le secteur public, elle estime que les conditions dans lesquelles les services nationaux chargés de la sécurité et du respect des lois peuvent acquérir, enregistrer et utiliser une donnée biométrique ou y avoir accès devraient être légalement encadrées. Dans les deux secteurs, elle recommande l'adoption de systèmes de contrôle destinés à protéger la confidentialité et l'intégrité des bases contenant des données biométriques

La ***variété des modes de stockage*** est par ailleurs souvent mise en évidence. Les gabarits peuvent ainsi être stockés dans une base centrale connectée à un réseau, mais aussi « sur place », dans le dispositif de capture, voire même sur un support portable comme une carte qui peut alors jouer le rôle d'un intermédiaire, le processus d'authentification biométrique étant limité à la vérification de l'identité du détenteur de la carte et la « transaction » s'opérant par d'autres moyens d'identification, tels qu'un code, un mot de passe ou un document habituel d'identité. Dans ce dernier cas, il s'agit alors seulement de

[73] http://www.ibia.org/privacy.htm « *IBIA Privacy Principles* »

vérifier que la donnée biométrique de la personne qui présente la carte d'accès correspond bien au gabarit enregistré sur la carte.

Enfin, comme cela a déjà été évoqué, la ***cryptographie à base biométrique*** est présentée comme une solution intéressante pour protéger la vie privée. Lors de la dix-huitième conférence internationale des commissaires à la protection des données, en septembre 1996, l'intérêt d'une telle technique a été mise en évidence par le Dr Georges J. TOMKO, notamment pour sécuriser les cartes contenant des données personnelles et les transactions sur Internet.[74].

3 - Panorama des domaines opérationnels d'application des techniques biométriques

Tenter de recenser les différents systèmes opérationnels s'avère délicat pour diverses raisons.

D'une part, il est relativement difficile de distinguer les systèmes mis en place à titre définitif et les dispositifs expérimentaux qui, lors de leur implantation, font l'objet d'une large publicité, mais dont les résultats et les perspectives d'avenir restent généralement beaucoup plus confidentiels. Tel est le cas, notamment, des expériences menées dans plusieurs aéroports européens.

D'autre part, des produits sont annoncés dans les domaines les plus variés, mais les informations sur les mises en application effectives, en particulier dans le secteur privé, sont beaucoup moins riches.

Enfin, il convient de souligner que certains domaines d'application échappent nécessairement à la transparence pour des raisons d'efficacité. Dans les secteurs de la sécurité publique, intérieure et extérieure, comme de la sécurité « privée », le secret est généralement considéré comme un gage de réussite.

A cet inévitable défaut d'exhaustivité s'ajoute la difficulté d'ordonner de façon cohérente les informations dont on dispose. Quelle typologie adopter ? La distinction secteur public / secteur privé s'avère souvent discutable, dès lors que l'on prend en compte des systèmes mis en place en dehors du domaine des compétences régaliennes des Etats. Une répartition entre systèmes de vérification et systèmes d'identification apparaît irréalisable, dès lors qu'on ne dispose pas d'informations précises sur les caractéristiques techniques et les finalités des différents systèmes.

---

[74] http://www.privcom.gc.ca. *"Biometrics Encryption – New Developments in Biometrics"*. Le Dr Georges TOMKO a fondé la société *Mytec technologies* en 1987 qui est devenue la société *Bioscrypt.*

Le champ de l'étude reste lui-même incertain. Dans quelle mesure un système d'identification utilisant des photographies statiques numérisées constitue-t-il un système biométrique ? Dans quelle mesure le recueil d'empreintes digitales ou de la signature selon des « méthodes traditionnelles », en dehors de tout capteur de type *live scan* se distingue-t-il d'un système biométrique ?

Aussi ne peut-on que dresser un panorama donnant une vision partielle et imparfaite des systèmes existants.

Trois secteurs peuvent être délimités : l'identification judicaire, la gestion des titres délivrés par la puissance publique et la gestion des accès physiques et logiques.

Mais avant d'exposer les éléments d'information disponibles, il semble intéressant de livrer les résultats d'un sondage effectué en septembre 2001 et en août 2002 aux Etats-Unis[75]. Si 50 % des personnes interrogées avaient entendu parler de la biométrie, seulement 3% en septembre 2001 et 5 % en août 2002 avaient déjà fourni au moins un caractère biométrique à une organisation. L'expérience la plus courante dans ce domaine porte sur la prise d'empreintes digitales (82 % des personnes concernées en août 2002), suivie par la signature dynamique (46 %), la voix (27 %), la face (22 %), les yeux (20 %), la géométrie de la main (19 %) et la dynamique de frappe sur le clavier (7 %).

Par ailleurs, il convient de souligner que les trois domaines identifiés peuvent entretenir entre eux des relations plus ou moins subtiles. Le Département de la Défense américain déploie actuellement un dispositif utilisant l'empreinte digitale, appelé « *Common Access Card (CAC)*» répondant à plusieurs finalités, notamment d'authentification, de gestion et de contrôle des personnels et la *General services administration* américaine expérimente l'utilisation d'une carte à puce multifonctions recourant à la technologie biométrique et destinée aux fonctionnaires fédéraux pour le contrôle des accès physiques et logiques et la gestion des dossiers médicaux ou fiscaux.

a) Le domaine de l'identification judiciaire

Dans le domaine de l'identification judiciaire, trois grandes techniques sont utilisées : l'empreinte digitale, l'empreinte génétique et la reconnaissance faciale.

Plusieurs Etats se sont dotés depuis de nombreuses années de fichiers d'empreintes digitales qui ont été informatisés. La technique de l'empreinte

[75] *International Opinion Research Corporation. "Public attituds toward the uses of biometric identification technologies by Gouvernment and the private sector"*. Ces sondages ont été effectués auprès de 1017 adultes en septembre 2001 et 1046 adultes en août 2002.

digitale est dans le domaine criminalistique bien maîtrisée, performante et largement répandue.

En France, le FAED (Fichier automatisé des empreintes digitales) a été officiellement créé en 1987 après avis favorable de la CNIL. Il a une double fonction : l'identification des personnes, permettant notamment la détection des emprunts d'identité et l'identification des traces papillaires relevées sur les lieux d'infraction afin de relier un indice à une identité déjà connue des services de police. Le système est pleinement opérationnel depuis 1992 et comptait au 1er juin 2002 plus de 1 500 000 individus dans sa base de données. En 2003, dans le cadre d'EURODAC, des bornes de numérisation seront installées, ce qui permettra l'enregistrement direct des empreintes de la personne (doigts et paume). La saisie des empreintes se fait actuellement par scanner avec délimitation de la zone mémorisée et la saisie des empreintes à partir des photocopies scannées n'est pas de très bonne qualité. Les fiches comportent des « déroulés » des dix doigts et la reconnaissance repose sur 12 minuties identiques. Les identifications policières ne sont pas entièrement automatisées : la machine fait un premier tri puis les spécialistes vérifient l'identité des douze minuties et en moyenne les spécialistes décident trois à quatre rejets sur un total de soixante-quinze fiches traitées. La durée de conservation des empreintes est limitée à vingt-cinq ans.

Au Royaume Uni[76], un fichier national d'empreintes digitales, le NAFIS *(National Automated Fingerprint Identification System)* contient 4,6 millions d'empreintes et est relié au Police National Computer qui comprend un fichier nominatif recensant les données de 6,1 millions de criminels, de délinquants et de personnes recherchées ou disparues. Des capteurs électroniques sont en voie de déploiement pour permettre la saisie directe et décentralisée des empreintes. Le Police and Criminal Evidence Act de 1984 autorise la police à prendre les empreintes digitales sans le consentement des intéressés dans certaines circonstances, mais prévoyait la destruction des empreintes lorsque la personne n'était pas condamnée. Depuis le Criminal Justice and Police Act de 2001, la police est autorisée à conserver les enregistrements.

En Allemagne[77], le fichier INPOL (*Informationssystem der Polizei*) géré par l'Office fédéral de la police criminelle, le BKA, comporte plus de 3 millions d'empreintes digitales.

Aux Etats Unis[78], le système IAFIS (*Integrated Automated Fingerprint Identification System*) géré par le FBI comporte 400 millions d'empreintes digitales. Les empreintes roulées des dix doigts de 40 millions de personnes sont enregistrées. Ce fichier est relié aux cinquante Etats et à quelques agences fédérales. Il est automatisé et permet en moyenne 48 000 contrôles par jour. Le fichier n'a pas uniquement une finalité d'identification judicaire. Les

[76] *Parliamentary Office of Science and Technology- Postnote* n°165, novembre 2001.
[77] Rapport de M. Christian ESTROSI sur le projet de loi sur la sécurité intérieure.
[78] GAO *op.cit.*

empreintes enregistrées ne concernent pas uniquement des personnes impliquées dans des affaires judiciaires. Le FBI disposerait ainsi de 210 millions de fiches avec en moyenne trois fiches par personne et sur 70 millions de personnes fichées, il y aurait 40 millions de criminels et 30 millions de personnes dont les empreintes digitales sont prises à des fins d'identification civile liée à l'exercice d'emplois sensibles (transport de fonds et aéroports par exemple).

Au Japon tous les commissariats de police sont dotés de bornes dédiées à la vérification des empreintes digitales.

Les fichiers d'**empreintes génétiques** sont également en voie d'extension.

En France, le FNAEG (Fichier national automatisé d'empreintes génétiques) créé par la loi n°98-468 du 17 juin 1998 relative à la répression des infractions sexuelles ainsi qu'à la protection des mineurs comporte actuellement 2 100 empreintes et 160 traces génétiques. Initialement cantonné aux crimes sexuels, son champ a été étendu par la loi du 15 novembre 2001 et par la loi du 18 mars 2003 pour la sécurité intérieure, ce qui laisse entrevoir un élargissement sensible de la dimension du fichier. Actuellement, les procédures de saisie sont très lourdes et le service réalise en moyenne dix-huit rapprochements par jour.

Plusieurs pays ont mis en place depuis une dizaine d'années des fichiers analogues (Etats-Unis, Canada, Espagne, Pays-Bas, Autriche, Belgique, Finlande, Suisse notamment)[79]. Au Royaume-Uni, le *National DNA Database*, mis en place en 1995, rassemble 2 millions de profils d'ADN et permet environ 900 rapprochements par semaine, tandis que le fichier INPOL allemand comporte les empreintes génétiques de 163 000 personnes[80].

D'autres procédés biométriques sont utilisés dans le domaine criminalistique, tels que les « traces technologiques » (informatique, GSM, voix notamment) et les photographies.

S'agissant notamment de l'exploitation de la **voix**, des équipements tels que les « débruiteurs » développés par le FBI et dédiés aux applications policières permettent d'améliorer la qualité de l'enregistrement, d'authentifier les bandes et d'identifier la voix. Cette identification repose elle-même sur diverses techniques, en particulier celle de la reconnaissance phonétique (les mots et les syllabes sont comparés et les normes exigent pour les laboratoires de police une similitude sur vingt mots de trois syllabes) et celle de la reconnaissance numérique qui correspond à une empreinte vocale avec une courbe de 128 points, la reconnaissance étant admise s'il y a concordance à 80%.

---

[79] Rapport de M. Christian CABAL, « La valeur scientifique de l'utilisation des empreintes génétiques dans le domaine judiciaire » - Office parlementaire d'évaluation des choix scientifiques et technologiques – n°3121 Assemblée nationale – n°364 Sénat – juin 2001.

[80] Rapport de M. Christian Estrosi *op.cit.*

En France, les **photographies** constituent un élément pris en compte mais les procédés d'identification semblent encore faiblement automatisés. Le système CANONGE contient ainsi un panel de photographies de personnes mises en cause. A partir de caractéristiques (couleur des yeux, taille,…), il est possible de sélectionner les photographies correspondant au signalement. Il est par ailleurs envisagé d'associer la photographie au fichier des personnes recherchées qui rassemble 300 000 fiches.

En revanche, la reconnaissance faciale à partir des caméras de surveillance ne semble pas exploitable pour l'instant car elle n'est pas assez fiable pour être utilisée dans un procès criminel. En France, la vidéo permet essentiellement à l'heure actuelle de procéder à des mesures anthropométriques mais cette opération reste subordonnée à la qualité de l'image. Plusieurs expériences ont néanmoins été conduites dans ce domaine, essentiellement en Grande-Bretagne où environ un million de caméras de vidéo-surveillance sont installées et aux Etats-Unis.

Enfin, s'agissant de l'analyse de **l'écriture**, elle s'opère actuellement en France sans le recours à des logiciels de comparaison car les systèmes biométriques de reconnaissance de l'écriture ne sont pas encore assez performants pour être utilisés dans le domaine criminalistique.

b) Le domaine de la gestion des titres délivrés par la puissance publique

S'agissant des cartes nationales d'identité, qui n'existent pas dans certains pays tels que les Etats-Unis, la Grande-Bretagne ou les Pays-Bas et qui ne sont obligatoires que dans certains autres Etats, tels que la Belgique ou la Suisse, il convient de noter que si généralement y figurent la photographie et la signature du titulaire, si exceptionnellement l'empreinte digitale y est apposée, si en outre, lors de l'établissement, les empreintes digitales sont collectées et archivées, il est très difficile de déterminer si de telles données biométriques sont susceptibles d'être utilisées dans le cadre d'un système d'identification, voire d'authentification, automatique.

Dans le cas de la France, il n'en est rien. En effet l'examen des textes réglementaires relatifs à la carte d'identité permettent d'écarter une telle éventualité. Le décret n°99-973 du 25 novembre 1999 qui reprend sur ces points les dispositions des décrets de 1987 prend soin d'énumérer les informations qui sont inscrites « de manière à permettre leur lecture à l'aide de procédés optiques » et il s'agit seulement du nom patronymique, des prénoms, du sexe, de la date de naissance et du numéro de la carte. D'autre part, il précise que le système ne peut retenir en mémoire que les éléments mentionnés aux 1°, 2° et 3° de l'article premier (du décret n°55-1397 du 22 octobre 1955 modifié), la photographie et la signature n'étant mentionnés qu'au dernier alinéa de l'article premier, après le 3° , tandis que le relevé des empreintes digitales est prévu à l'article 5. Enfin, le décret dispose que les informations nominatives contenues dans le système de gestion

informatisée ne peuvent faire l'objet d'aucune interconnexion avec un autre fichier. C'est ainsi que la CNIL a pu rappeler[81] que « le ministère de l'intérieur n'a pas donné suite au projet de numérisation du relevé d'empreintes digitales qui sont prises à l'occasion de la demande d'une carte nationale d'identité, afin de ne pas donner l'impression que pourrait se constituer, à l'occasion d'une démarche administrative, un outil de police judiciaire ». Le décret dispose cependant que l'empreinte ne peut être utilisée qu'en vue de la détection des tentatives d'obtention ou d'utilisation frauduleuse d'un titre d'identité, mais aussi de l'identification certaine d'une personne dans le cadre d'une procédure judiciaire.

Votre Rapporteur a pu toutefois percevoir le désir de certains responsables policiers de pouvoir confronter les traces non attribuées relevées sur des scènes de crime à un fichier plus global.

Dans son rapport d'activité pour l'année 2000, la CNIL a mentionné plusieurs pays utilisant l'empreinte digitale pour la gestion de la délivrance des cartes d'identité. Il s'agit en particulier du Nigeria, de la Malaisie et du Kosovo.

En Malaisie, une carte à puce biométrique multifonctions appelée GMP (*Government Multi-Purpose Card*) a été mise au point. Cette carte est censée servir de carte d'identité, de passeport, de permis de conduire, de dossier médical ; elle permettra de régler des factures et les impôts « via internet ». En Mauritanie, un titre d'identité dont l'unicité est garantie par la comparaison des empreintes digitales a été institué et, lors des élections qui se sont déroulées en 2001, des terminaux biométriques ont été installés dans certains bureaux de vote.

L'empreinte digitale est également utilisée pour la **gestion des prestations sociales** dans une dizaine d'Etats aux Etats-Unis (Arizona, Californie, Connecticut, Illinois, Massachussets, New Jersey, New York, Texas), ainsi qu'au Mexique et aux Philippines (depuis 1997).

Plusieurs Etats des Etats-Unis utilisent également l'empreinte digitale pour gérer la délivrance des **permis de conduire** (Hawaï, Texas, Colorado, Géorgie, Californie), en revanche d'autres Etats américains se sont opposés à l'implantation de tels systèmes[82].

La gestion des **titres délivrés aux étrangers** utilise aussi parfois **l'empreinte digitale**. Tel est le cas, en France, du fichier mis en œuvre par l'OFPRA en matière de contrôle et de gestion des demandes d'asile depuis 1987. En Grande-Bretagne, depuis l'été 2001, un système comparable fonctionne pour la gestion des titres des demandeurs d'asile, l'IAFS *(Immigration Asylum Fingerprint System)* ; il a été institué par l'*Immigration and Asylum Act* de 1999 et l'année dernière a été créée une carte contenant les empreintes digitales de chaque

[81] Rapport d'activité 2000, p.108.

[82] L'Etat de l'Alabama a ainsi retiré un projet visant à utiliser les empreintes digitales en 1999 et l'Etat du Michigan a adopté une loi interdisant l'introduction des empreintes digitales sur les permis de conduire.

demandeur d'asile (*l'Application Registration Card*) destinée à se substituer aux formulaires utilisés actuellement. Aux Etats-Unis, le système IDENT (*Automated Biometric Fingerprint Identification System*) est géré par l'INS depuis 1990 et comporte les empreintes digitales (deux index) et les **photographies** d'environ 5 millions de personnes de nationalité étrangère qui ont commis des crimes ou des infractions à la législation sur l'immigration.

La **reconnaissance faciale** connaît une application beaucoup plus réduite. Elle est cependant utilisée au Mexique pour le contrôle des **élections**[83] (60 millions d'images) et par une vingtaine d'Etats aux Etats-Unis pour la gestion des **permis de conduire**.

c) Le domaine de la gestion des accès physiques ou logiques

C'est dans ce domaine qu'un recensement s'avère le plus malaisé, car les dispositifs installés dans le secteur strictement privé ne font généralement pas l'objet d'une publicité, à la différence de ceux mis en œuvre par des organismes dont les missions ont une portée plus générale.

De ce point de vue, les rapports d'activité de la CNIL[84] permettent de suivre l'évolution de ce domaine en France, sans toutefois donner une vision exhaustive de la situation :

Empreintes digitales :

- Dispositif de reconnaissance par empreintes digitales pour l'accès à des zones hautement sécurisées de la Banque de France (avis favorable – délibération 97-044 du 10 juin 1997 – rapport annuel 1997 p.288).
- Déclaration de l'établissement de la Hague de la COGEMA pour un dispositif de lecteurs d'empreintes digitales d'accès physiques du personnel et des visiteurs aux zones du site dont certaines sont sous secret défense (récépissé délivré, compte tenu de la sensibilité extrême du site (rapport 2000 p.115).
- Contrôle d'accès pour les personnels de l'Education nationale aux bâtiments d'une cité académique (délibération 00-056 – rapport d'activité 2000 p.118 – avis favorable mais seulement pour l'accès aux zones sensibles).
- Contrôle d'accès aux zones de fabrication dans les locaux du groupement carte bleue (récépissé délivré le 25 avril 2001 – rapport 2001 p. 170).
- Contrôle d'accès des zones de fabrication de cartes à puce de la SAGEM (récépissé délivré le 25 avril 2002- rapport 2001 p.170) .

[83] GAO
[84] cf. Annexe 4

Contour de la main :

- Contrôle d'accès au musée du Louvre des salariés des entreprises sous-traitantes de nettoyage pour assurer la sécurité des biens et le contrôle des heures de travail (avis favorable pour une durée d'un an 00-006 du 25 janvier 2001– rapport 2000 p.117).
- Contrôle d'accès dans une bijouterie (récépissé délivré 12 février 2001 – rapport 2001 p.170).
- Contrôle des horaires du personnel soignant à domicile des personnes handicapées (*ibid.)*.
- Contrôle des horaires du personnel de nettoyage d'un centre commercial à La Défense (récépissé délivré en 2002).
- Contrôle d'accès à une cantine scolaire (avis favorable 15 octobre 2002- communiqué de presse de la CNIL).

Il convient cependant d'ajouter à cette liste l'initiative prise récemment dans le cadre de la gestion pénitentiaire pour le contrôle d'accès des détenus aux parloirs qui vise notamment à empêcher les évasions par substitution.

Le programme « 13 000 » prévoyait déjà, il y a une douzaine d'années, la mise en place de dispositifs biométriques basés sur les empreintes digitales et qui sont devenus obsolètes (temps de réponse trop long). Le principe d'un basculement vers de nouvelles technologies a été arrêté par une circulaire de l'administration pénitentiaire du 31 mai 2002. Actuellement onze établissements ont été dotés de nouveaux systèmes. La volumétrie de la main, dont le coût unitaire s'établit à environ 50 000 euros, a été implantée dans dix d'entre eux et la reconnaissance par empreinte digitale a été conservée par un établissement. La loi de finances pour 2003 permettra d'équiper neuf établissements supplémentaires, ce qui portera le taux d'équipement à moins de 12% (20 établissements sur 171).

S'agissant de la prison de la Santé, qui compte environ 1 400 détenus avec un nombre moyen journalier d'entrées compris entre huit et douze et dans laquelle trois parloirs sont organisés par semaine, chaque parloir durant 40 minutes et concernant 28 détenus, le système de reconnaissance basé sur la volumétrie de la main (comparaison de un à un) s'est substitué à un dispositif utilisant un tampon encreur. Une carte est créée à l'arrivée du détenu et supprimée à sa sortie. Cette carte est encodée au greffe de la prison à partir d'un fichier comportant les nom, prénom, date de naissance, numéro d'écrou, photographie et donnée biométrique de chaque détenu et les données sont détruites lorsque le détenu quitte l'établissement. L'enrôlement initial comporte trois saisies, le dispositif sélectionnant automatiquement la meilleure. Depuis l'introduction de cette technique, on constate que les cartes magnétiques mises en circulation dans l'établissement depuis quatre ou cinq ans subissent moins de pertes ou de dégradations, les détenus ayant désormais conscience qu'ils ont intérêt à conserver leur carte en bon état.

Le rapport établi par le GAO américain fournit également de précieuses informations sur les conditions d'utilisation des systèmes biométriques dans le domaine du contrôle d'accès.

L'iris et la géométrie de la main constituent les techniques semble-t-il les plus utilisées à l'heure actuelle, étant observé que divers dispositifs recourant à d'autres techniques sont testés dans divers environnements, parfois depuis plusieurs années.

La reconnaissance par l'**iris** a été déployée dans divers aéroports pour contrôler l'accès des employés à des zones réservées (aéroport international Douglas en Caroline du Nord depuis juillet 2000, aéroport de Francfort), pour faciliter les formalités des passagers réguliers (certaines compagnies britanniques pour les vols transatlantiques à l'aéroport d'Heathrow, aéroport de Toronto et de Vancouver depuis cette année, aéroport Schipol à Amsterdam depuis octobre 2001) ou pour contrôler les entrées et sorties des voyageurs (aéroport de Jeddah en Arabie Saoudite lors des pèlerinages depuis février 2002).

Elle est cependant également utilisée comme moyen de contrôle d'accès logique à des réseaux ou des ordinateurs (en Australie, à la Chambre des représentants américaine) ainsi que pour contrôler les déplacements des prisonniers américains et les flux de certains travailleurs entre Singapour et la Malaisie.

La technique de la **géométrie de la main**, dont le déploiement a été assuré depuis plus d'une vingtaine d'années, est actuellement implantée, selon le GAO, dans plusieurs dizaines de milliers de sites. Elle constitue la technique la plus largement répandue dans le domaine du contrôle d'accès physique (sites nucléaires, bâtiments, village olympique d'Atlanta, aéroports…) et est utilisée notamment aux Etats-Unis pour la gestion des horaires de travail.

S'agissant des aéroports, elle est notamment utilisée depuis 1991 à l'aéroport de San Francisco pour protéger les zones sécurisées, depuis 1998 à l'aéroport de Tel Aviv pour le passage des voyageurs réguliers et le contrôle de l'immigration et constitue la technique employée par les systèmes INSPASS et CANPASS (*Passengers Accelerated Service System*) mis en œuvre dans six aéroports américains et deux aéroports canadiens.

La **reconnaissance faciale** est généralement utilisée pour les contrôles d'accès aux casinos. Elle a fait l'objet d'un déploiement depuis juin 2001 à l'aéroport de Keflavik en Islande.

Quant à **l'empreinte digitale**, son implantation dans un environnement aéroportuaire fait actuellement l'objet de plusieurs expérimentations, même si les projets initiés dans ce domaine sont parfois relativement anciens. Selon le rapport établi par le *General Accounting Office* américain, divers projets expérimentaux utilisant l'empreinte digitale sont en cours de réalisation.

VOIR LA SUITE DU RAPPORT