Commission d'accès
à l'information
du Québec

La biométrie au Québec :
Les enjeux

Document d'analyse

Commission d'accès à l'information

Préparé par
Max Chassé
Analyste en informatique

Juillet 2002

AVANT-PROPOS

La Commission d'accès à l'information rend public un document d'analyse sur la biométrie qui vise à mettre en lumière les nouveaux enjeux qui accompagnent l'utilisation des systèmes technologiques d'identification.

Cette analyse n'a pas la prétention d'être complète ou de traiter de façon définitive l'ensemble des questions sur le sujet, mais de marquer un pas en avant dans une réflexion qui nous interpelle collectivement et individuellement.

Ce document d'analyse a été réalisé par M. Max Chassé avec la collaboration de M^{me} Sylvie Prigent, analyste en informatique, sous la direction de M^{e} Denis Morency, directeur de l'analyse et de l'évaluation.

LA BIOMÉTRIE AU QUÉBEC :
LES ENJEUX

INTRODUCTION

"*Perhaps the most beautiful and characteristic of all superficial marks are the small furrows with the intervening ridges and their pores that are disposed in a singularly complex yet even order on the under surfaces of the hands and the feet.*", Personal Identification And Description , Nature, Sir Francis Galton, 28 juin 1888[1].

Cette affirmation concernant les empreintes digitales, plutôt banale à notre époque, marquait le premier pas vers l'élaboration d'un système universel d'identification des criminels au service des policiers du monde entier. Sir Francis Galton (1822–1911) n'était pas le premier à remarquer les sillons et les creux existant à l'intérieur de nos mains et sous nos pieds, ni même à leur trouver d'utiles applications. Certains auteurs[2] mentionnent qu'il y a plus de 1000 ans les Chinois utilisaient l'empreinte digitale à des fins de signature de documents. Les caractéristiques de ces empreintes attirèrent aussi l'attention de l'anatomiste Marcello Malpighi (1628–1694) qui les étudia alors avec un nouvel instrument nommé microscope. Puis le physiologiste tchèque Jan Evangelista Purkinge (1787–1869) s'affaira à catégoriser les empreintes selon certaines caractéristiques. Une application pratique de prise d'empreintes fut réalisée par Sir William Herschel (1738–1822), fonctionnaire britannique au Bengale, excédé par le peu d'empressement des marchands locaux à respecter les contrats qu'il concluait avec eux. Il exigea alors de ceux-ci l'apposition de leurs empreintes digitales sur les documents contractuels. Puis le Dr Henry Faulds (1843–1930), chirurgien à Tokyo, donna une sérieuse impulsion au développement d'un système de classification par la prise d'empreintes. En octobre 1880, il écrivit dans la revue Nature : « *When bloody finger-marks or impression on clay, glass etc., exist, they may lead to the scientific identification of criminals »*[3]. À cette époque, le Dr Faulds écrivit au naturaliste Charles Darwin (1809–1882) pour l'informer de ses découvertes sur les empreintes digitales. Darwin, déjà vieux, déclina l'offre mais référa Faulds à son cousin, Sir Francis Galton.

Galton était à la fois physiologiste, anthropologue et psychologue. Il s'affaira notamment à appliquer la méthode statistique à l'étude de l'hérédité et des différences individuelles[4]. Ses découvertes l'ont amené sur des sentiers moins heureux puisque Galton est un des fondateurs de l'*eugénique*. En ce qui concerne les empreintes digitales, sa contribution fut de démontrer que celles-ci sont uniques et ne changent pas de façon notoire avec le vieillissement des personnes[5].

---

[1] L'article complet est reproduit sur le site Internet du Southern California Association of Fingerprint Officers (www.scafo.org/library/100801.html).

[2] CNIL, Deakin University Australia, SAGEM MORPHO inc, Dr Fu SUN

[3] BBC- History-Science and discovery-By people-Henry Faulds, British Broadcasting Corporation

[4] Petit Robert 2, dictionnaire universel des noms propres, Les Dictionnaires Robert – Canada SCC, Montréal , Canada , 1990.

[5] "Galton's formulation gives the probability that a particular fingerprint configuration in an average size fingerprint (containing 24 regions as defined by Galton) will be observed in nature." Cette probabilité est de $(1/16 \times 1/256 \times (1/2)^R$ ou 1.45×10^{-11} , On the individuality of fingerprints, Sharath Pankanti, IBM T.J.

Au moment où Galton travaillait sur les empreintes, un de ses contemporains, le Français Alphonse Bertillon (1853-1914), testait à la préfecture de police de Paris une méthode d'identification des prisonniers nommée anthropométrie judiciaire ou bertillonnage[6]. Bertillon procédait à la prise de photographies de sujets humains, mesurait certaines parties de leur corps (tête, membres, etc.) et en notait les dimensions sur les photos et sur des fiches à des fins d'identification ultérieure.

La dactyloscopie (procédé d'identification par les empreintes digitales) et le bertillonnage furent des techniques rapidement adoptées par les corps de polices du monde entier. Un policier argentin fut le premier à identifier un criminel par ses empreintes en 1892. Par la suite, la dactyloscopie s'imposa comme technique anthropométrique et le bertillonnage s'effaça graduellement.

« *De toutes les technologies liées à la biométrie, l'identification à partir d'empreintes digitales reste la plus courante (la moitié du marché).* »[7]. Plus d'un centenaire après sa mise au point par Galton, cette technique, améliorée maintes fois depuis, se porte plutôt bien. Les grands corps policiers ont accès à d'immenses banques de données où sont conservées des images d'empreintes digitales de millions de personnes.

Par exemple, en juillet 1998, le fichier automatisé des empreintes digitales (FAED), une application informatique commune à la police et à la gendarmerie en France, contenait 900 000 fiches individuelles. Nul doute que ce fichier s'est sensiblement enrichi depuis 1998, mais ceci demeure bien peu en comparaison des données contenues dans le système IAFIS (Integrated Automated Fingerprint Identification System) mis en place par le FBI aux États-Unis : « *IAFIS became operational on July 28, 1999, and provides the FBI with a totally electronic environment in which to process fingerprint submissions 24/7/365. Today over 42,8 million digitized criminal fingerprint records reside in the IAFIS database, which is far the world's largest biometric repository of any kind. It is at least four times larger than all of the fingerprint repositories in Europe combined.* »[8]. Le FBI dispose aussi d'une composante nommée IDIS (Interim Distributed Image System) qui permet un accès à distance au système IAFIS : « *These computer systems allow disaster relief teams to submit both ten-print and latent fingerprints electronically to the IAFIS from remote locations. IDIS systems have also been deployed in other recent*

Watson Research Center, Salili Prabhakar, Digital Persona Inc., Anil K. Jain, Dept. of Computer Science and Engineering Michigan State University.

[6] La criminologie et la criminalistique, VIIe colloque de l'Association intenationale des criminologues de langue française, 15 mai 2001, SUN Fu Ph.D., Alphonse Bertillon, "Le père de l'anthropométrie", www.interieur.gouv.fr/histoire/hom_fem/bertillon.htm, Bertillon's System, James Cook University, Tropical North Queensland, Australia, The History of Fingerprints, SAGEM MORPHO inc., www.morpho.com/news_room/library/reference/history.htm, Chapitre 4 Les contrôles d'accès par biométrie, CNIL, 21e rapport d'activité 2000.

[7] L'antidote high-tech au terrorisme, Bruno D. Cot, L'Express, 22 novembre 2001.

[8] Hearing How New Technologies (Biometrics) Can Be Used To Prevent Terrorism, Michael D. Kirkpatrick, FBI, devant le United States Senate Committee on the Judiciary Subcommittee on Technology, Terrorism, and Government Information, Washington, 14 novembre 2001.

events, such as the Summit of the Americas in Quebec. »[8]. L'utilisation de l'empreinte digitale à des fins d'identification des criminels par les policiers est prédominante, mais parallèlement elle est de plus en plus utilisée par des entreprises et des gouvernements à des fins de sécurité, d'identification et d'authentification. Cette technique est aussi en compétition avec plusieurs autres qui s'imposent de plus en plus sur le marché, comme par exemple la reconnaissance de la forme de la main.

Le Centre d'éducation physique de l'Université de Montréal (CEPSUM) utilise depuis quelques mois un système biométrique basé sur la reconnaissance de la forme de la main. En décembre, selon le directeur adjoint du CEPSUM, 8000 personnes utilisaient ce système[9]. Si l'Université de Montréal fait figure de précurseur au Québec, il y a déjà plusieurs années que des entreprises et organismes américains utilisent diverses techniques biométriques. Déjà en 1997, Wired[10] publiait un article qui faisait état de plusieurs systèmes alors en opération aux États-Unis. Voici quelques-uns des exemples présentés par Wired : le balayage des vaisseaux sanguins de la rétine de l'œil pour des détenus d'une prison de Cook County en Illinois; l'empreinte digitalisée des doigts pour les bénéficiaires de programmes sociaux *welfare* du Connecticut et de la Pensylvanie; un système de vérification de la voix pour les voyageurs traversant souvent la frontière entre le Montana et le Canada; la géométrie de la main pour identifier certains employés de Coca-Cola. Ces quelques exemples démontrant la diversité des techniques biométriques et les multiples applications auxquelles elles sont utilisables, permettent d'oser l'hypothèse que le projet de l'Université de Montréal est le premier d'une longue série à venir au Québec. Face au développement de ces technologies, le Québec a décidé d'intervenir législativement en 2001 afin d'encadrer l'utilisation de la biométrie par voie législative.

L'Assemblée nationale du Québec a sanctionné le 21 juin 2001 la *Loi concernant le cadre juridique des technologies de l'information* (L.Q. 2001, c.32) qui a pour objet d'assurer notamment la sécurité juridique des communications effectuées au moyen de documents, l'équivalence fonctionnelle des documents et leur valeur juridique, quels qu'en soient les supports, ainsi que l'interchangeabilité de ces derniers. Cette loi offre la possibilité d'utiliser divers modes d'authentification de l'identité d'une personne qui communique au moyen d'un document technologique et prévoit des moyens de faire le lien entre une personne et le document par lequel elle exprime sa volonté, ainsi que le lien du document avec une association, une société ou l'État. La loi précise que nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des mesures ou caractéristiques biométriques. D'autres dispositions, sur lesquelles nous reviendrons, sont prévues à l'égard de la biométrie. Il importe cependant de préciser que la loi exige que la création d'une banque de mesures ou caractéristiques biométriques soit préalablement divulguée à la Commission d'accès à l'information. La Commission peut rendre toute ordonnance

[9] L'UDEM devient le premier établissement à l'utiliser. L'identification biométrique fait son entrée, Marc Thibodeau, La Presse, le dimanche 23 décembre 2001.
[10] The Body as Password, Ann Davis, WIRED, 5.07 – JUL 1997 (www.wired.com/wired/archive/5.07/biometrics_pr.html).

concernant de telles banques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation y compris l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne. La Commission peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction, si celle-ci ne respecte pas ses ordonnances ou si elle porte autrement atteinte au respect de la vie privée.

Face à ces responsabilités et avant que l'utilisation de techniques biométriques ne se généralise, la Commission d'accès à l'information désire émettre une première série de principes d'application, qui permettront aux entreprises, aux ministères et aux organismes gouvernementaux de baliser leurs pratiques en cette matière. Pour ce faire, nous effectuerons d'abord, dans ce document, une revue des principales techniques existantes tant en ce qui concerne la biométrie physiologique que la biométrie comportementale, tout en prenant soin d'en noter les forces et les faiblesses connues. Nous nous attarderons ensuite à répertorier les utilisations principales qui sont faites de ces diverses technologies. Puis, nous dégagerons les impacts sur la protection des renseignements personnels et la vie privée des personnes que génère l'utilisation de la biométrie. Dans un autre document, nous présenterons les principes d'application en matière de biométrie au Québec découlant de cette analyse.

1. LES SYSTÈMES BIOMÉTRIQUES

Bien qu'il existe différentes techniques biométriques, celles-ci possèdent un schème de fonctionnement similaire. Tout d'abord, un système biométrique requiert une alimentation initiale. Pour ce faire, une lecture de certaines caractéristiques physiologiques ou comportementales d'une personne est effectuée par l'entremise d'un terminal de capture biométrique. Les paramètres résultant de cette lecture sont traités et génèrent une « signature » unique. Chaque « signature » est enregistrée dans un dépôt de données central ou parfois sur un support portable. L'ensemble de ce processus porte le nom d'enrôlement.

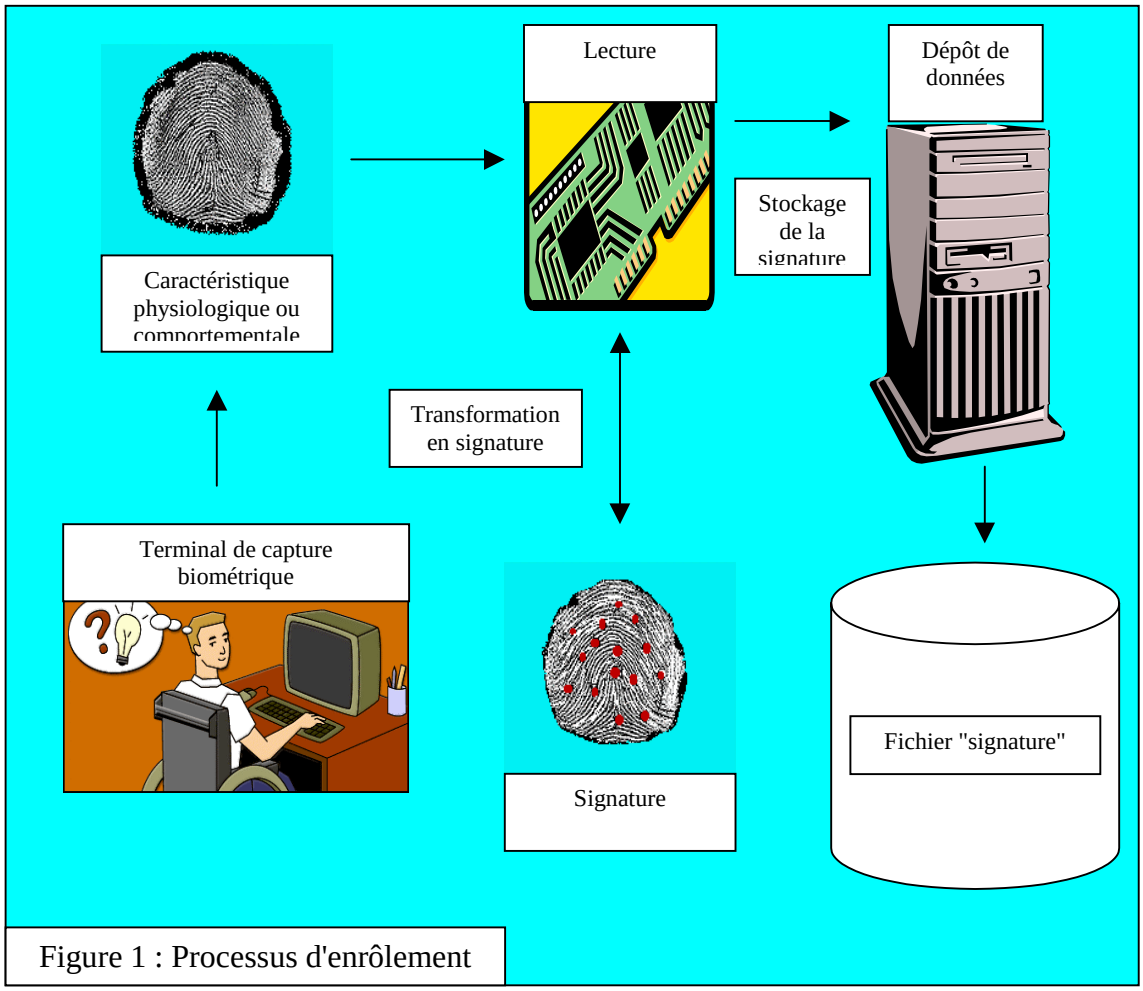

Figure 1 : Processus d'enrôlement

Lorsqu'une personne « enrôlée » ou enregistrée dans un dépôt de données biométriques doit s'identifier, un terminal de lecture biométrique est utilisé. Plusieurs techniques permettent aussi d'identifier une personne à son insu. Les caractéristiques biométriques soumises au terminal de lecture, volontairement ou involontairement, sont comparées aux « signatures » préalablement enregistrées dans un dépôt de données centralisé. Un support portable peut dans certains cas être utilisé.

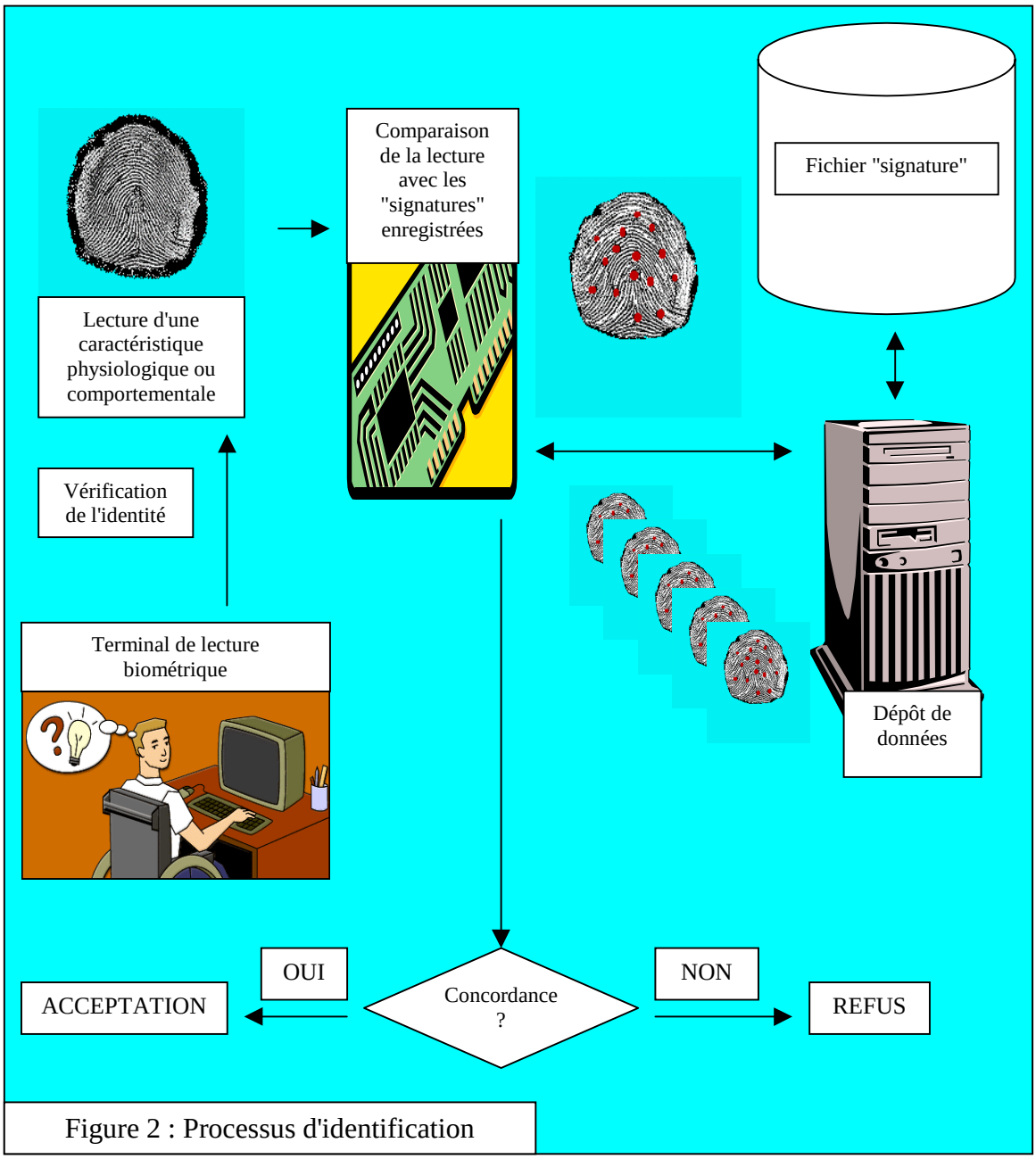

Figure 2 : Processus d'identification

1.1 Types de biométrie

Les systèmes biométriques sont généralement classés par l'industrie dans deux grandes catégories : la *biométrie morphologique* ou *physiologique* (en anglais : *physiological*) et la *biométrie comportementale* (en anglais : *behavioral*).

La *biométrie morphologique* est basée sur l'identification de traits physiques particuliers qui, pour toute personne, sont uniques et permanents. Cette catégorie regroupe la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la rétine et de l'iris de l'oeil.

La *biométrie comportementale*, quant à elle, se base sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, l'empreinte de sa voix, sa démarche et sa façon de taper sur un clavier.

À l'instar de la Commission Nationale de l'Informatique et des Libertés (CNIL) de France[11], il convient d'ajouter à ces deux catégories l'étude des traces biologiques regroupant de façon non exhaustive l'analyse de l'ADN, du sang et des odeurs.

De nouvelles techniques sont en développement et il ne serait pas surprenant que plusieurs de celles-ci s'ajoutent dans les années à venir à celles déjà commercialisées ou mentionnées ci-dessus. À titre d'exemple, mentionnons la forme de l'oreille et la thermographie faciale.

1.2 Systèmes à technologies multiples

Plusieurs techniques biométriques peuvent être utilisées dans un même système. Il existe par exemple un système combinant la reconnaissance de la voix avec la reconnaissance de l'écriture (signature)[12]. Les systèmes biométriques peuvent aussi s'utiliser en conjugaison avec d'autres systèmes ou d'autres technologies. Il existe des systèmes où l'image de l'empreinte digitale du pouce est emmagasinée sur une carte à microprocesseur et l'activation de cette carte nécessite l'utilisation d'un mot de passe. Ces technologies sont appelées multimodales.

1.3 Description des principales techniques biométriques commercialisées

A) Empreintes digitales :

L'identification à l'aide des empreintes digitales est chargée d'histoire. Il s'agit de la plus vieille technique biométrique déjà utilisée par les Chinois il y a un millénaire, ensuite remise à jour par le Britannique Galton il y a un siècle. Elle est depuis largement utilisée

[11] LES CONTRÔLES D'ACCÈS PAR BIOMÉTRIE, Chapitre 4 ,21e rapport d'activité, CNIL, 2000.
[12] LITRONIC ADVANCES INTERNET SECURITY WITH VOICE AND HANDWRITING BIOMETRICS, Pat Harriman, SSP Solutions, Aug 14, 2000 (www.litronic.com).

par l'ensemble des forces de l'ordre de la planète. Soutenue par l'apport des nouvelles technologies, son utilisation n'est désormais plus confinée à la chasse aux criminels.

Selon le International Biometric Group (IBG), l'empreinte digitale avec 48,8 % des revenus dominait le marché de la biométrie en 2000[13].

Fonctionnement :

Il existe deux principaux types de systèmes de capture des empreintes digitales : *optique* et *capacitive*. Une technologie plus récente a recourt aux ultrasons. Il existe aussi des systèmes de reconnaissance des empreintes digitales appelés Automatic Fingerprint Identification System (AFIS).

La technologie optique nécessite que l'utilisateur place un ou plusieurs doigts sur une vitre, à travers laquelle l'image recherchée est mise sous éclairage et capturée par une caméra. La technologie capacitive effectue l'analyse du champ électrique de l'empreinte digitale pour déterminer sa composition. L'utilisateur place ses doigts directement sur un microprocesseur spécialisé.

À l'aide de l'un de ces mécanismes, plusieurs caractéristiques uniques à chaque individu que sont les boucles, les tourbillons, les lignes et les verticilles (cercle concentrique au centre d'un doigt) des empreintes sont localisées, situées les unes par rapport aux autres et enregistrées. Les caractéristiques retenues s'appellent minuties et généralement une quarantaine sont extraites. Le FBI considère que deux personnes ne peuvent avoir plus de huit minuties en commun[14]. Ce sont ces minuties qui sont ensuite comparées lorsqu'une personne présente ses doigts dans un terminal de lecture biométrique.

Les AFIS permettent de numériser des empreintes relevées et de les comparer au contenu d'immenses bases de données, comme le IAFIS[15] du FBI américain.

Utilisations actuelles :

Ce type de système est utilisé par les institutions financières pour leurs employés et leurs clients. Il se retrouve également dans les magasins de détail, les hôpitaux, les écoles, les aéroports, les cartes d'identité, les passeports, les permis de conduire et de nombreuses autres applications.

Les systèmes AFIS sont utilisés principalement par les forces de l'ordre, les agences d'espionnage et les départements de services sociaux pour l'identification des personnes.

[13] Biometric Market Report 2000-2005, 2001 Comparative market share by technology (Does not include AFIS Revenues), International Biometric Group, 2001, (www.biometricgroup.com).
[14] Fingerprint Identification, Engineering Technology, Western Carolina University (http ://et.wcu.edu)
[15] Integrated Automated Fingerprint Identification System

Quelques fournisseurs :

Identix, Dermalog, Cross Match, Polaroid, Veridicom, Digital Persona, Sagem Morpho, Sonda, Cogent Systems, ActivCard (Ankari).

B) Forme de la main ou des doigts de la main :

Si l'une des premières formes de mesures biométriques fut la dactyloscopie, la reconnaissance de la forme de la main est considérée, quant à elle, comme l'ancêtre des technologies biométriques. À la fin des années soixante, Robert P. Miller déposa un brevet pour un appareil permettant de mesurer des caractéristiques de la main et de les enregistrer pour comparaison ultérieure[16]. Quelques années plus tard, Identimat, le premier système commercial basé sur cette technique, était installé dans une firme d'investissements de Wall Street[17].

Selon le International Biometric Group (IBG) la forme de la main occupait 10,4 % du marché des technologies biométriques en 2000[18].

Fonctionnement:

L'utilisateur place sa main sur un gabarit. Le tout est éclairé par une lumière infrarouge et l'image résultante est captée par une caméra digitale. Près d'une centaine de caractéristiques sont extirpées de l'image et converties en données stockées en mémoire, lors de la phase d'enrôlement ou comparées lors de la phase d'identification. Ces données concernent la longueur, la largeur et l'épaisseur de la main, de même que la forme des articulations et longueur inter-articulations. Certains systèmes ont un fonctionnement identique mais capturent des informations sur les doigts plutôt que sur l'ensemble de la main.

Utilisations actuelles :

Cette technologie est utilisée pour contrôler l'accès à des zones sensibles et où un grand nombre de personnes circulent comme lors de Jeux Olympiques, aux frontières, dans les aéroports et dans les grands parcs d'attractions (Disney). Plus de 90 % des centrales nucléaires aux États-Unis l'utiliseraient de même que l'armée américaine[19]. Plus récemment on a vu, surtout aux États-Unis, des applications dans des écoles, des hôpitaux, des cafétérias, des garderies, des prisons et des banques.

[16] An Overview of Biometric Authorization Systems Research Paper, Roger Heiniluoma, College of engineering, Texas A&M University, july 24, 2001.
[17] Biometric Solutions to Personal Identification, DigitalPersona Providers of U.areU. Fingerprint Recognition System (www.digitalpersona.com).
[18] Biometric Market Report 2000-2005, 2001 Comparative market share by technology (Does not include AFIS Revenues), International Biometric Group, 2001, (www.biometricgroup.com).
[19] Hand Geometry Applications, Department of Engineering Technology, Western Carolina University.

Certains employeurs y recourent aussi pour prévenir la fraude et le vol d'heures de la part des employés *(buddy punching,* pauses prolongées, grignotage de temps) en remplaçant la traditionnelle carte de poinçon par un système basé sur cette technologie. Les vendeurs de ce type de systèmes font actuellement beaucoup de publicité en ce sens en faisant miroiter la récupération de pertes substantielles à cet égard.

Quelques fournisseurs :

Recognition Systems Inc. (RSI), Dermalog, Biomet Partner (2 doigts de la main), Stromberg.

C) Forme du visage :

Le développement de systèmes biométriques basés sur la reconnaissance de la forme du visage est des plus récents. En 1982, les chercheurs Hay et Young dans un ouvrage intitulé *The Human Face* mentionnent que l'humain, pour reconnaître un visage, utilise les caractéristiques globales et locales qui le composent. Par la suite, différentes recherches furent effectuées afin de voir si cette capacité de reconnaissance pouvait être reproduite informatiquement. Ces recherches donnèrent naissance à plusieurs techniques de reconnaissance du visage dont les plus répandues sont les *eigenfaces* et son dérivé le *feature analysis*. C'est à partir des travaux du professeur Teuvo Kohonen [20] (1989), chercheur en réseaux neuronaux de l'Université d'Helsinki, et des travaux de Kirby et Sirovich[21] (1989) de l'Université Brown du Rhode Island, que fut mis au point par le MIT un système de reconnaissance du visage nommé *eigenface.*

Le reconnaissance de la forme du visage occupait en 2000 selon IBG 15,4 % du marché de la biométrie[22].

Fonctionnement :

L'image du visage est captée par une caméra. Le sujet peut se présenter volontairement devant celle-ci ou encore, son image peut être capturée à son insu.

Selon la technique utilisée, le système extrait des caractéristiques du visage qui sont conservées dans une base de données.

Par exemple, le *eigenface* décompose l'image bidimensionnelle capturée en une série d'images teintées avec des nuances de gris différentes. Les zones claires et foncées ainsi créées dans les images grisées sont des caractéristiques uniques du visage et ce sont elles que l'on nomme *eigenfaces*. On en extrait ainsi de 100 à 125 par visage. Quant au *feature*

[20] Self-organization and Associative Memory, Teuvo Kohonen, Springer-Verlag, Berlin, 1989.
[21] Application of the karhunen-loeve procedure for the characterization of human faces, IEEE Pattern Analysis and Machine Intelligence, vol. 12, no. 1, 1990.
[22] Biometric Market Report 2000-2005, 2001 Comparative market share by technology (Does not include AFIS Revenues), International Biometric Group, 2001, (www.biometricgroup.com).

analysis, son dérivé, il est un peu plus souple que le *eigenface* puisqu'il permet de mieux prendre en compte les déformations du visage, l'éclairage et les angles horizontaux et verticaux.

Il existe des techniques plus sophistiquées recourant à l'intelligence artificielle comme le *natural network mapping* qui détermine les similarités des caractéristiques globales d'un visage et dont l'algorithme apprend de ses expériences. À l'inverse, le *automatic face processing* est une technique plus rudimentaire calculant la distance et les ratios entre les yeux, le nez et la bouche.

Utilisations actuelles :

La reconnaissance du visage est utilisée comme système de surveillance ou d'identification par les autorités ou les corps policiers principalement dans les lieux publics, les aéroports, les frontières, les casinos, les plages, les guichets automatiques et les laboratoires.

Quelques fournisseurs:

Imagis Technologies inc, Bio4, Viisage technology.

D) Balayage de la rétine :

En 1936, le Dr Carleton Simon et le Dr Isadore Goldstein eurent l'idée d'utiliser la rétine de l'œil à des fins d'identification après qu'ils aient vu une photographie des vaisseaux sanguins d'une rétine[23]. Ils établirent que ces vaisseaux sont uniques pour chaque personne. Vingt ans plus tard, le Dr Paul Tower, dans une étude sur les jumeaux identiques, confirma cette unicité[24]. Au milieu des années soixante-dix, cette idée fut reprise dans le but de mettre au point un système d'identification biométrique commercialisable.

Cette technologie, probablement à cause de son coût élevé, est peu répandue et sa part de marché n'est pas répertoriée dans les études de marché d'IBG.

Fonctionnement :

L'utilisateur doit placer son œil à quelques centimètres d'un orifice de capture situé sur le lecteur de rétine. Il ne doit pas bouger et doit fixer un point vert lumineux qui effectue des rotations. À ce moment, un faisceau lumineux traverse l'oeil jusqu'aux vaisseaux sanguins capillaires de la rétine. Le système localise et capture ainsi environ 400 points de référence.

[23] Carleton Simon Papers Administrative History, M.E.Grenander Department of Special Collections and Archives, University at Albany, State University of New York (http://library.albany.edu) .
[24] Areas of Focus, Retina Scan, Information Security Office, Duke University Health System (www.iso.duke.edu) .

Utilisations actuelles :

Cette technologie est utilisée dans les cas où la sécurité est primordiale, notamment dans le domaine militaire, dans le secteur spatial (NASA) et par des agences d'espionnage comme la CIA.

Fournisseur :

Eyedentify inc.

E) Reconnaissance de l'iris :

L'idée d'utiliser l'iris de l'œil pour identifier les personnes fut proposée par l'ophtalmologiste Frank Burch en 1936. Deux autres membres de cette profession, Aran Safir et Leonard Fom, déposèrent un brevet concernant cette technologie en 1987. En 1989, ils demandèrent l'aide du professeur John Daugman de l'Université de Cambridge pour qu'il confectionne une méthode de calcul (algorithme) permettant d'utiliser cette technologie, travail complété en 1994. Les premières applications commerciales furent livrées quelques années plus tard[25].

Malgré qu'elle soit récente, cette technologie biométrique détenait selon IBG 6,2 % des parts du marché en 2000[26].

Fonctionnement :

La partie visible de l'iris comporte de nombreuses caractéristiques physiques différentes. Ce sont celles-ci qui sont recherchées lorsqu'une personne utilise ce type de système biométrique. L'image de l'iris d'une personne est lue par un appareil qui contient une caméra infrarouge ou ordinaire, lorsque la personne se place à une distance qui n'excède pas 40 centimètres de l'appareil. Environ 250 caractéristiques sont alors capturées.

Utilisations actuelles:

La reconnaissance de l'iris est utilisée dans le secteur financier pour les employés et les clients, pour le téléchargement de musique par Internet, dans les guichets automatiques (ATM Bank United), pour le paiement dans les supermarchés (Kroger du Texas), dans les institutions carcérales, dans les hôpitaux et dans les aéroports.

[25] History and Development of Iris Recognition, Computer Laboratory, University of Cambridge (www.cl.cam.ac.uk)
[26] Biometric Market Report 2000-2005, 2001 Comparative market share by technology (Does not include AFIS Revenues), International Biometric Group, 2001, (www.biometricgroup.com).

Fournisseur :

Iridian Technologies.

F) Reconnaissance de la voix :

C'est en 1962 que Lawrence Kersta,[27] un ingénieur du Bell Laboratories, établit que la voix de chaque personne est unique et qu'il est possible de la représenter graphiquement[28]. La voix est constituée de composantes physiologiques et comportementales. À cette époque, des travaux sur la voix furent aussi menés par des entreprises comme IBM et Texas Instruments et plusieurs corps policiers s'y intéressèrent. Dans les années quatre-vingt, plusieurs entreprises développèrent des systèmes de reconnaissance de la voix pour les corps policiers et les agences d'espionnage. Au début des années quatre-vingt-dix, le gouvernement américain demanda à ces entreprises de mettre au point un système pour le marché commercial.

Selon IBG, cette technologie biométrique détenait 4,3 % du marché en 2000[29].

Fonctionnement :

Initialement, une table de référence de la voix d'une personne doit être construite. Pour ce faire, celle-ci doit lire une série de phrases ou de mots à plusieurs reprises. Plusieurs caractéristiques de la voix sont alors extraites comme le débit, la force (pitch), la dynamique et la forme des ondes produites. Un individu ne parle pas toujours de la même manière, ce qui nécessite l'application d'une méthode permettant d'éliminer certaines de ces variations. Ces caractéristiques formant une empreinte unique sont ensuite traitées par un algorithme et conservées pour comparaison ultérieure. Il existe cinq principales méthodes de traitement de la voix : dépendante du sujet, indépendante du sujet, discours discontinu, discours continu et discours naturel.

Utilisations actuelles :

Ces systèmes sont utilisés par les corps policiers, les agences d'espionnage, les services d'immigration, les hôpitaux et en téléphonie.

Quelques fournisseurs:

IPI speech technologies, VeriVoice, Veritel, T-Netix, OTG, Nuance, Keyware, Graphco Technologies, Anovea et Voicevault.

---

[27] Spectographic voice identification : A forensic survey, Bruce E. Koenig, FBI, Engineering section, Technical Service Division, June 1986.
[28] Forensic Voiceprints, The Crime Library, Katherine Ramsland, (www.crimelibrary.com)
[29] Biometric Market Report 2000-2005, 2001 Comparative market share by technology (Does not include AFIS Revenues), International Biometric Group, 2001, (www.biometricgroup.com).

G) Reconnaissance de l'écriture (signature) :

Dès 1929, Osborn établit que l'écriture dépend de plusieurs facteurs caractéristiques. Pour imiter une signature, il faut donc non seulement imiter la forme de l'écriture mais aussi tenir compte de ces facteurs reliés notamment à la vitesse, aux conditions environnantes et à la dextérité musculaire[30].

Par la suite, diverses techniques de reconnaissance de la signature furent mises au point au bénéfice notamment des banques et des corps policiers. De façon non exhaustive, différents travaux, dont ceux de A.J. Mauceri (1965)[31], de R.N. Nagel et A. Rosenfeld (1977)[32] et de N.M. Herbst et C.N. Liu (1977)[33] menèrent graduellement au dépôt d'une centaine de brevets de reconnaissance dynamique de la signature.

Cette technologie représentait 2,7 % du marché de la biométrie en 2000 selon IBG[34].

Fonctionnement :

Les systèmes de reconnaissance de l'écriture analysent les caractéristiques spécifiques d'une signature comme la vitesse, la pression sur le crayon, le mouvement, les points et les intervalles de temps où le crayon est levé. L'utilisateur de cette technologie signe généralement avec un stylo électronique sur une tablette graphique. Ces données sont enregistrées pour comparaison ultérieure. Certains sytèmes ne font qu'enregistrer l'image statique de la signature pour comparaison.

Utilisations actuelles :

Ces systèmes sont utilisés dans les compagnies pharmaceutiques, les prisons, les services postaux et les banques.

Quelques fournisseurs :

Cyber-SIGN, CIC (Pen Op), MMI Group et Topaz Systems.

H) Dynamique de frappe au clavier :

Durant la seconde guerre mondiale, les services secrets militaires savaient distinguer les messages en code morse de l'ennemi par ce qu'ils appelaient « Fist of the sender » ou

[30] A Review of Dynamic Handwritten Signature Verification, Gopal Gupta and Alan McCabe, Department of Computer Science, James Cook University, australia, September 1997.
[31] Feasibility Studies of Personal Identification by Signature Verification, North American Aviation Co, A. J . Mauceri, Space ans Information System Division, 1965.
[32] Computer Detection of Freehand Forgeries, R.N. Nagel and A. Rosenfeld, IEEE Trans on Computers, 1977.
[33] Automatic Signature Verification Based on Accelerometry, N.M. Herbst and C.N. Liu, IBM, 1977.
[34] Biometric Market Report 2000-2005, 2001 Comparative market share by technology (Does not include AFIS Revenues), International Biometric Group, 2001, (www.biometricgroup.com).

l'écriture de l'expéditeur. En fait les militaires mesuraient le rythme de frappe pour déterminer qui était l'envoyeur. Au début des années quatre-vingt, la US National Science Foundation commanda une étude afin d'établir si cette particularité pouvait être utilisée pour identifier des personnes par le rythme de frappe sur un clavier[35]. À cette époque, le National Bureau of Standards américain effectuait aussi une étude concluant à l'existence de caractéristiques uniques lorsqu'une personne tape sur un clavier[36]. Elle confia le mandat au Stanford Research Institute (SRI) qui travailla sur la problématique jusqu'en 1985 et développa une technologie biométrique basée sur la dynamique de frappe au clavier.

Selon IBG, cette technologie occupait 0,4 % du marché de la biométrie en 2000[37].

Fonctionnement :

Un système basé sur la dynamique de frappe au clavier ne nécessite aucun équipement particulier, chaque ordinateur disposant d'un clavier. Il s'agit d'un dispositif logiciel qui calcule le temps où un doigt effectue une pression sur une touche et le temps où un doigt est dans les airs (entre les frappes). Cette mesure est capturée environ mille fois par seconde. La séquence de frappe est prédéterminée sous la forme d'un mot de passe. Initialement l'utilisateur doit composer son mot de passe à quelques reprises afin que soit constitué un gabarit de référence.

Utilisations actuelles :

Ce dispositif biométrique est utilisé comme méthode de vérification pour le commerce électronique et comme mécanisme de contrôle d'accès à des bases de données.

Fournisseur :

BioPassword.

I) Forme des veines de la main :

Ce système a été inventé par l'ingénieur britannique Joe Rice en 1984[38]. Avant de commercialiser la découverte, une étude fut commandée à Cambridge Consultants afin d'établir que les veines de la main sont uniques pour chaque individu[39].

---

[35] Authentification by Keystroke Timing : Some Preliminary Results, R.Gaines W.Lisowski S.Press and N.Shapiro, Rand Report R-256NSF, Rand Corp, 1980.
[36] The History of BioPassword, Net Nanny Software Intenational Inc (www.biopassword.com).
[37] Biometric Market Report 2000-2005, 2001 Comparative market share by technology (Does not include AFIS Revenues), International Biometric Group, 2001, (www.biometricgroup.com).
[38] Engineer discovers a rich vein in security (Daily Telegraph London), Museum Security Mailinglist Reports (www.museum-security.org).
[39] www.veinid.com

Fonctionnement :

L'utilisateur place sa main dans une chambre ou un gabarit de lecture. Les caractéristiques des veines sont lues par une caméra infrarouge qui en tire une image en deux dimensions. Cette image est ensuite digitalisée et enregistrée pour comparaison future.

Cette technologie n'est pas répertoriée par IBG dans ses études de marché.

Utilisations actuelles:

Quelques applications dans le secteur militaire fonctionnent actuellement.

Quelques fournisseurs :

Neusciences, ABI, Veinid et Sol Universe.

2. PERFORMANCES DES SYSTÈMES BIOMÉTRIQUES

Les technologies biométriques constituent un assemblage complexe de composantes optiques, électroniques et logicielles (algorithmes). Chacune de ces composantes a des lacunes, des faiblesses et des limites. En raison de cela, leur calibrage s'avère souvent difficile. Certaines technologies sont plus fiables que d'autres et certains manufacturiers offrent des produits plus ou moins performants pour une technologie donnée. En conséquence, ces systèmes ne donnent pas une réponse précise sur l'identité d'une personne mais une réponse relative qui s'exprime par un taux de similitude qui n'atteint jamais 100 %.

« Il est impossible d'obtenir une coïncidence absolue (100 % de similitude) entre le fichier signature créé lors de l'enrôlement et le fichier signature *créé lors de la vérification*. » – Les technologies biométriques, Performances des systèmes, Biométrie Online.

FAUSSES ACCEPTATIONS ET FAUX REJETS

Pour mesurer la performance des systèmes biométriques, deux mesures principales furent créées : le taux de faux rejets (TFR) exprime le pourcentage de personnes autorisées qui sont rejetées par le système qui n'arrive pas à les reconnaître, le taux de fausses acceptations (TFA) donne le pourcentage de personnes non autorisées qui sont acceptées de façon erronée par le système.

Dans un système de sécurité, il est évidemment préférable d'avoir un TFA très bas. Or, ces TFA et TFR sont mathématiquement reliés et ont une influence l'un sur l'autre, ce qui fait qu'en deça d'un certain seuil le TFR augmente lorsque le TFA diminue[40]. À ce moment un maximum d'individus non autorisés sont rejetés correctement par le système mais par la même occasion celui-ci récuse indûment un grand nombre de personnes autorisées. Ce type de système devient rapidement inutilisable, les rejets étant beaucoup trop nombreux. C'est pour cette raison que les concepteurs de technologies biométriques sont contraints de faire un compromis en gardant le TFA à un niveau plus haut que souhaité afin de garder un TFR acceptable.

Les technologies biométriques sont par conséquent affligées de nombreux problèmes qui doivent être compensées par le recours à des artifices.

COMBINAISONS TECHNOLOGIQUES

« De nombreux procédés biométriques commercialisés ne sont pas considérés comme suffisamment fiables pour discriminer une personne de l'autre; aussi, malgré les argumentaires développés par les industriels du secteur, doit-on le plus souvent associer

[40] A Manager's Guide to Biometrics, Craig Kaucher, Professor of Systems Management, Information Ressources Management College, National Defense University, Ft.Lesley J. Mc Nair and Norfolk VA.

la biométrie à un mot de passe ou à une carte magnétique ou à puce. » – CNIL 21e rapport d'activité 2000[41].

Nous avons aussi vu qu'il est possible de combiner plusieurs technologies biométriques, ce qui devrait logiquement donner naissance à un système plus performant. Cette assertion est supputée et rejetée par le professeur John Daugman (Cambridge University) qui affirme avec démonstration mathématique à l'appui : « *Either method of combining the two biometric tests produces 5.5 times more error than of the stronger of the two tests had been used alone »*[42].

DE NOUVELLES UTILISATIONS

Le International Biometric Industry Association (IBIA) fut créée en septembre 1998 dans le but de promouvoir, de défendre et de supporter l'industrie biométrique[43]. De nombreuses entreprises en vue de ce secteur industriel en sont membres. Récemment le président de cet organisme, M. John Siedlarz, exposa publiquement ses inquiétudes à propos des nouvelles utilisations réalisées avec les technologies biométriques :
« Before Sept. 11, he noted [M Siedlarz] the biometrics industry had moved from protecting physical infrastructures into protecting information – like data used in e-commerce transactions… His recommandation to the biometrics industry? "Put some breaks on this (technology) and put some thought into how you're going to make it work" as a comprehensive solution that works with other kinds of security. »[44]

DES PERFORMANCES INÉGALES

Deux utilisations récentes de la reconnaissance de la forme du visage furent vertement critiquées à cause de leur piètre performance et de la menace qu'ils font peser sur la vie privée des personnes.

Le dimanche 28 janvier 2001 avait lieu au Raymond James Stadium de Tampa en Floride le XXXVe Super Bowl. À cette occasion, la police de la ville de Tampa a filmé, à leur insu, le visage de plusieurs dizaines de milliers de personnes qui entraient dans le stade[45]. Ces images furent ensuite, avec l'aide d'un système de reconnaissance de la forme du visage, comparées avec celles contenues dans des bases de données locales de la Floride et fédérales par les forces de l'ordre. Les policiers voulaient avec ce système identifier les terroristes et les criminels dans la foule. Or le système n'a permis d'effectuer aucune

[41] LES CONTRÔLES D'ACCÈS PAR BIOMÉTRIE, Chapitre 4 , page 102, 21e rapport d'activité, CNIL, 2000.
[42] Combining Multiple Biometrics, John Daugman, The Computer Laboratory, Cambridge University (www.cl.cam.ac.uk/users/jgd1000/combine/combine.html).
[43] www.ibia.org
[44] Put brakes on biometris : IBIA, Technology not one-stop security solution for governments, says association's chair, Zachary Houle, Technology in government, Volume 9, Issue 4, April 2002.
[45] ACLU Calls for Public Hearings on Tampa's "Snooper Bowl" Video Surveillance, American Civil Liberties Union (ACLU), Freedom Network, Thursday, February 1, 2001.

arrestation[46]. Ceci souleva des doutes sérieux quant à la performance de ce type de système.

Malgré ce revers, la police de la ville de Tampa a installé à l'été 2001 une douzaine de caméras couplées au système de reconnaissance du visage Face-IT de la firme Visionics Corporation, sur une rue passante de la ville, capturant ainsi le visage des citoyens y déambulant. L'American Civil Liberties Union (ACLU) a produit un rapport sur le sujet intitulé *Drawing a blank* : *The failure of facial recognition technology in Tampa, Florida*[47]. Selon les informations transmises par la police de Tampa à l'ACLU, le système n'a jamais permis d'identifier correctement un seul visage dans la base de données des suspects, ni permis aucune arrestation. Qui plus est le système a détecté plusieurs faux positifs (des supposés criminels) allant même jusqu'à confondre des images d'hommes et de femmes. Ce système a été désactivé le 11 août 2001.

Ces expériences récentes soulèvent un doute sérieux quant à l'utilisation de systèmes biométriques à large échelle. La Commission d'accès à l'information approfondira cette problématique dans des travaux qu'elle entreprendra sous peu concernant la vidéosurveillance.

Bien sûr les systèmes de reconnaissance du visage de même que les autres types de systèmes offrent de bien meilleures performances lorsque le sujet consent à être identifié et que la capture de données biométriques se fait dans de meilleures conditions. Reste que chaque technologie possède ses propres faiblesses et qu'il faut se méfier des TFA et des TFR réclamés par les vendeurs de solutions à des fins de marketing. Ces résultats sont parfois des extrapolations calculées sur une base théorique ou issues de tests réalisés dans des conditions idéales[48].

[46] Super Bowl Surveillance, Facing Up to Biometrics, John D. Woodward Jr., Rand Arroyo Center,, RAND 2001.
[47] **Drawing a Blank**: *The failure of facial recognition technology in Tampa, Florida*, An ACLU special report, Jay Stanley and Barry Steinhardt, ACLU, January 3, 2002.
[48] Evaluation techniques for biometrics-based authentification systems (FRR), Ruud M Bolle, Sharath Pankanti and Nalini K Ratha, IBM Thomas J Watson Research Center, Yorktown Heights, NY.

3. IMPACTS SUR LA VIE PRIVÉE ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

La biométrie est présentée au grand public comme un remède universel propre à terrasser plusieurs maux : terrorisme, fraude, vol d'identité et atteinte à la vie privée, pour n'en citer que quelques-uns. Aux employeurs elle est présentée comme une solution au vol de temps par les travailleurs, comme un moyen facile de produire les données de base servant au calcul de la paye. Aux utilisateurs elle est présentée comme un moyen confortable de s'identifier; plus de cartes qu'on égare et de mots de passe qu'on oublie. Ce qui saute d'abord aux yeux c'est qu'un remède pour l'un n'est pas toujours bon pour l'autre. Par exemple, l'employeur qui installe un système biométrique pour enregistrer les entrées et sorties de son personnel peut y voir une solution au vol de temps dont il croit être victime. Pour les employés le recours à la biométrie par leur employeur peut constituer un système de surveillance des plus invasifs pour la vie privée. En fait, bien que la plupart des techniques biométriques soient des outils de sécurité fort efficaces, ils ne brillent pas par leur innocuité en ce qui concerne la protection de la vie privée des personnes qui les utilisent. Il faut ici faire clairement la distinction entre le concept de sécurité et celui de protection de la vie privée et des renseignements personnels; il n'est pas rare que des mécanismes de sécurité atteignent à la vie privée des personnes qui les utilisent, comme la Commission d'accès à l'information l'a déjà démontré dans un avis récent sur l'infrastructure à clés publiques gouvernementale[49]. Ces atteintes à la vie privée concernent la collecte supplémentaire de renseignements personnels pour faire fonctionner le système de sécurité, le traitement de ces renseignements et la possibilité de traçage et de constitution de profils.

Roger Clarke, professeur à l'Australian National University et spécialiste international de la vie privée, n'hésite pas à considérer que la biométrie a des implications extrêmement sérieuses pour les droits humains en général et particulièrement pour la vie privée[50]. Malgré cela, il semble que le public soit tolérant envers ce type de technologie comme le rapporte Simon G. Davies de l'University Of Essex : « *There may be many factors at work in the apparently greater public acceptance of privacy-invasive schemes. Proposals are being brought forward in a more careful and piecemeal fashion, which may be lulling the public into a false sense of security. There is increasing popularity of computers and networks for personal use. The use of personal information systems by Nazi German to enable the identification and location of a target race are becoming a vague memory* »[51].

Si une appréhension certaine des défenseurs de la vie privée envers les systèmes biométriques existe depuis un certain temps, il est inquiétant de constater que l'industrie de ce secteur commence à peine à s'interroger sur ces aspects. Dans un article récent le

[49] www.cai.gouv.qc.ca/fra/docu/a011107.pdf

[50] Biometrics and Privacy, Roger Clarke, Principal Xamax Consultancy, Visiting Fellow Department of Computer Science Australian National University, Notes of 15 april 2001 (www.anu.edu.au).

[51] TOUCHING BIG BROTHER, How biometric technology will fuse flesh and machine, Simon G Davies, Department of law, University Of Essex, United Kingdom, Information Technology & People, Vol7, No. 4 1994.

journaliste Zachary Houle du journal Technology in Government rapporte que l'IBIA, la Biometric Foundation et le West Virginia University collaborent au sein d'un projet appelé National Biometric Security Project. Un des mandats du groupe est le suivant : « *The group is looking at privacy issues, like what would happen if businesses and governments took carte blanche control of personal biological records* »[52].

La prise de mesures biométriques implique nécessairement une atteinte à la vie privée des individus, contrairement à l'attribution d'une carte d'accès ou d'un mot de passe. Il s'agit d'un moyen fort d'identification des personnes. D'ailleurs jusqu'à tout récemment, il était réservé à la protection de lieux qui pour des raisons valables devaient être hautement sécurisés : armée, défense nationale, espionnage, centrales nucléaires, etc. Dans ces cas le besoin de sécurité est si fort que l'atteinte à la vie privée des utilisateurs de ces systèmes est justifiable. Mais, étant connus les risques pour la vie privée, la biométrie est-elle adaptée à tous les milieux et aux divers niveaux de sécurité requis? Son utilisation est-elle nécessaire dans une cantine scolaire ou un centre sportif? Les enjeux de sécurité sont-ils les mêmes à ces endroits que dans les locaux de la CIA? Le moyen n'est-il pas disproportionné par rapport aux besoins réels de sécurité? Ces questions sont d'autant plus importantes que la biométrie offre un côté séduisant auquel les utilisateurs de badges, de cartes et de mots de passe seront sensibles : elle offre un grand confort et une facilité d'utilisation appréciables. Par exemple, elle peut remplacer l'utilisation d'une kyrielle de mots de passe qu'il faut constamment changer et se rappeler. Elle peut remplacer ces cartes et ces badges qui doivent être portés au cou et que l'on perd, que l'on oublie et que l'on égare. C'est bien connu, personne n'oublie ou ne perd son iris ou son pouce. La facilité vient ainsi diluer la prise en compte des risques pour la vie privée.

Il existe effectivement de nombreux risques menaçant la vie privée quant à l'utilisation de la biométrie comme moyen d'identification. Les prochains paragraphes tenteront de présenter les principaux enjeux et risques de l'utilisation d'identifiants biométriques.

UNE MESURE OU UNE CARACTÉRISTIQUE BIOMÉTRIQUE EST PLUS QU'UN SIMPLE IDENTIFIANT NUMÉRIQUE

La mesure ou la caractéristique biométrique diffère passablement des autres identifiants, généralement un code ou un numéro qui nous est attribué. Ces numéros peuvent être constitués de données personnelles à propos d'une personne comme son nom et sa date de naissance, mais n'ont pas la capacité de livrer des informations personnelles intimes sur la composition de notre corps et sur notre comportement en général. Toute mesure ou caractéristique biométrique est un identifiant unique universel qui est composé de telles informations intimes. À ce sujet Roger Clarke écrit : « *Biometric technologies don't just involve collection of information about the person, but rather information of the person, intrinsic to them* »[53].

[52] Put brakes on biometris : IBIA, Technology not one-stop security solution for governments, says association's chair, Zachary Houle, Technology in government, Volume 9, Issue 4, April 2002.
[53] Biometrics and Privacy, Roger Clarke, Principal Xamax Consultancy, Visiting Fellow Department of Computer Science Australian National University, Notes of 15 april 2001, p. 5. (www.anu.edu.au).

UN IDENTIFIANT INTIME BAVARD

Un identifiant aussi collé à notre physiologie et à notre comportement que la mesure ou la caractéristique biométrique transporte souvent des informations sur notre état d'esprit et sur notre état de santé.

La Commissaire à la vie privée de l'Ontario, madame Ann Cavoukian, fait un survol fort intéressant de cette problématique : « *However, it is certainly technically possible to identify various health and medical conditions from some biometric data. Recent scientific research suggests that finger-prints and finger imaging might disclose medical information. Certain chromosomal disoders (e.g.,Down's and Turner's syndromes), as well as certain non-chromosomal disorders (e.g.,leukemia and breast cancer) have been indicated by unusual fingerprint patterns. By examining person's retina or iris, it can be determined if that individual is suffering from diabetes, arteriosclerosis, or hypertension, as well as diseases of the eye* »[54]. Quant à Craig Horrocks celui-ci soutient dans un article écrit dans Computerworld que le balayage de la rétine ou de l'iris permet de savoir si une personne est droguée et que la reconnaissance du visage par *eigenface* permet de savoir si quelqu'un est fâché[55].

Notons ici que plusieurs technologies biométriques sont facilement piratables; par exemple, une simple photographie pourrait déjouer un mécanisme de détection du visage et une personne malveillante pourrait couper le pouce d'une personne pour le présenter à un lecteur d'empreintes digitales. Pour contrer ces problèmes, certains manufacturiers ajoutent à leurs produits un mécanisme de mots de passe ou de badge. D'autres préfèrent ajouter des mécanismes de détection que la personne est vivante comme la vérification de la température du corps ou vérifier la circulation du sang[56]. Ces derniers types de mécanismes recueillent évidemment des données médicales supplémentaires sur les personnes.

Il faut cependant comprendre que les produits biométriques vendus sur le marché ne visent pas systématiquement à déterminer l'état de santé d'une personne, mais que cette possibilité existe. Quant aux technologies biométriques comportementales, elles visent précisément à mesurer les comportements des personnes : il n'y a donc aucune ambiguité à cet égard.

---

[54] Consumer Biometric Applications : A Discussion Paper, Ann Cavoukian Ph.D., Information and Privacy Commissioner/Ontario, September 1999.

[55] Biometrics benefits in eye of beholder, Craig Horrocks, Opinion, Computerworld, 6 august 2001.

[56] At face value- on biometrical identification and privacy, dr. R Hes mr. drs. TFM Hooghiemstra drs JJ Borking, with contributions from: PJA Verhaar, TGA van Rhee and HAM Luiijf (TNO Physics and Electronics Laboratory – The Hague), The College Beschermingpersoonsgegevens (Dutch data protection authority), september 1999.

DES RISQUES DE DÉRIVE

L'utilisation et la généralisation des identifiants traditionnels présentent des dérives connues. Cette généralisation est accentuée au Québec parce que la vérification d'identité se fait de façon courante en présentant une carte contenant un identifiant (NAM, NAS, numéro de permis de conduire).

Étant connues les dérives actuelles qui existent à propos de l'utilisation d'un identifiant national comme le NAS, utilisé à toutes les sauces par le secteur privé et le secteur public, il y a tout lieu de s'inquiéter à propos de l'utilisation de tout identifiant intime, unique et universel, ce qu'exprime le professeur Davies en ces termes: « *The history of identification systems throughout the world provides evidence of 'function creep' application to additional purposes not announced, or perhaps even intended, at the commencement of the scheme »*[57].

Un ou plusieurs identifiants universels utilisés autant par le secteur public que le secteur privé rendent très faciles le croisement des données provenant de multiples sources et le traçage des actions posées par les individus. Il n'y a aucun ambage quant à l'identité de la personne visée; il ne reste qu'à accoler le contenu de dépôts de données existants ou l'historique transactionnel à cet identifiant et le tour est joué. Le Dr George Tomko écrit : *« But biometrics also have the ability to track individuals and their transactions, and to be used as a universal identifier which can associate or link various sources of personal information to an individual – in either case – without their consent »*[58].

Actuellement les organismes au Québec ne peuvent partager les données recueillies sur les personnes, sauf dans certaines circonstances. Ce cloisonnement des organismes est la meilleure garantie de protection de la vie privée : « *Informational chaos and functional separation amongst agencies have ensured that the individual has not become a servant to the state. Variety, choice, and chaos have also had the effect of insuring the free movement, rights, and free choice of individuals against errrors in the system »*[59]. La Commission d'accès à l'information abonde dans le même sens : « *La centralisation de l'information peut certes sembler une solution intéressante du point de vue économique et au niveau de l'accès à l'information par un plus grand nombre de personnes. Mais les lois de protection des renseignements personnels font toutes le même pari : le cloisonnement de l'information au sein de plusieurs organismes demeurera toujours la meilleure garantie de confidentialité et l'obstacle le plus approprié pour éviter que l'État*

[57] TOUCHING BIG BROTHER, How biometric technology will fuse flesh and machine, Simon G Davies, Department of law, University Of Essex, United Kingdom, Information Technology & People, Vol7, No. 4 1994.
[58] Biometrics as a Privacy-Enhancing Technology : Friend or Foe of Privacy ?, Dr. George Tomko, Chairman Photonics Research Ontario, Privacy Laws & Business 9th Privacy Commissioners Data Protection Authorities Workshop, Spain, September 15th 1998.
[59] Idem.

ne puisse dresser des profils sur les individus ou autrement s'immiscer dans leur vie privée »[60].

La Commission observe une propension à la centralisation et à l'intégration des systèmes d'information et s'interroge sur la menace que ces tendances font peser sur l'outil de protection de la vie privée qu'est le cloisonnement. En aucun cas celui-ci ne saurait être remplacé par l'augmentation des mesures de sécurité. L'avènement de l'utilisation d'identifiants universels risque d'exacerber cette tendance au décloisonnement : « *There are no natural barriers to data-sharing, many countries lack laws to preclude it, and a strong tendancy exists for organisations to break down such legal impediments as do exists. Hence the multiple purposes to which a biometric scheme is applied can readily extend beyond a single organisation to encompass multiple organisations in both the private and public sectors »*[61].

Il y a lieu de s'interroger sur ce qu'il adviendrait du cloisonnement si le gouvernement et des tiers songeaient à offrir centralement des services de biométrie et d'identification des personnes. Ce type de services va à l'encontre du principe de cloisonnement. Des organisations qui ne devraient pas détenir de données personnelles sur des individus en exigent désormais aux seules fins de faire fonctionner un système de sécurité. Cela favorise la copie et la dissémination de données personnelles en plusieurs lieux, d'où une perte de contrôle par les individus des données qui leur appartiennent.

IDENTIFIANT NON MODIFIABLE ET VOL PERMANENT D'IDENTITÉ

Pour des raisons prédéterminées par les administrations, les identifiants en général peuvent être modifiés lorsqu'un tel besoin se présente. Par exemple, un identifiant national comme le NAM pourrait être modifié par les autorités pour des cas exceptionnels, comme un changement de nom. Les mesures ou les caractéristiques biométriques étant des identifiants capturés directement sur les personnes, ceux-ci sont non modifiables. En cas de compromission de cet identifiant par fraude, par malveillance ou par erreur, il n'y a donc plus de possibilité de réparer le préjudice. On ne pourrait taxer l'Institute of Electrical and Electronics Engineers (IEEE) de démagogie à cet égard; il convient donc d'examiner sa position sur les identifiants universels :

« The concept of an identifier that is both unique to an individual and "universal" in the sense of being always used by that individual to identify himself or herself in interactions with society, is fraught with danger. While such an identifier could provide convenience to the individual in assembling a detailed, intimate understanding of his or her interactions with society, similar convenience could well accrue also to many other parties and thus simultaneously be very attractive to many forms of painful misuse at the expense of the

[60] MÉMOIRE DE LA COMMISSION D'ACCÈS À L'INFORMATION CONCERNANT L'AVANT-PROJET DE LOI SUR LA CARTE SANTÉ DU QUÉBEC, Remis à la Commission des Affaires sociales, Commission d'accès à l'information, 8 février 2002.

[61] Biometrics and Privacy, Roger Clarke, Principal Xamax Consultancy, Visiting Fellow Department of Computer Science Australian National University, Notes of 15 april 2001, p. 5. (www.anu.edu.au).

individual's privacy and security…Policy makers must be made aware that : conventional identifiers can be changed, but only at great inconvenience; biometric identifiers are existential identifiers and, if compromised, are essentially incapable of modification…»[62].

La stabilité des mesures ou des caractéristiques biométriques comme identifiant pourrait devenir un véritable cauchemar pour les personnes victimes de vol d'identité. Même si ces personnes réussissaient à prouver leur innocence, leur identifiant intime serait compromis à tout jamais : « *Cases of identity theft have been reported already, which have had very serious consequences for the victims. Organisations cannot distinguish the acts and transactions of the two individuals using the one identity, and hence they are merged together* »[63]. De même un individu malveillant qui réussirait à accoler ses données biométriques à l'identité d'une autre personne pourrait causer un tort immense et difficilement réparable à la personne victime d'un tel stratagème.

FARDEAU DE LA PREUVE

Une des caractéristiques d'un identifiant universel est que la personne qui effectue une transaction en y ayant recours confère un caractère d'irrévocabilité. En théorie personne d'autre qu'un individu ne peut utiliser son propre corps. Il peut certes le modifier par des chirurgies ou accidentellement, mais certaines caractéristiques biométriques demeurent malgré tout inchangées.

Les mécanismes assurant l'irrévocabilité sont fort prisés dans le monde virtuel où la plupart des transactions sont réalisées avec des inconnus. Cette irrévocabilité, dans le cas de la biométrie, se construit sur l'unicité des mesures ou des caractéristiques biométriques recueillies. Comment un utilisateur de bonne foi peut-il démontrer son innocence en cas de problème? Comment peut-il découvrir et exposer les failles d'un système complexe dont il ignore le fonctionnement? Pour certains, l'utilisation banale de la biométrie renverse la présomption d'innocence qui doit prévaloir pour toute personne accusée d'un crime, d'une fraude ou de toute autre action répréhensible. L'Information and Privacy Commissioner/Ontario rapporte ce fait : « *Use of biometric identification is interpreted by some as a questioning of their reputation and trustworthiness. They perceive a requirement to give a biometric as a reversal of the presumption of innocence – as shifting the burden of proof* »[64].

CONSENTEMENT

En apparence, pour utiliser la biométrie, le consentement de l'utilisateur est requis afin de réaliser la procédure initiale d'enrôlement. En pratique certaines technologies offrent la

[62] AGAINST USE OF UNIVERSAL IDENTIFIERS (UIDs), IEEE-USA Position Statement, February 15, 2001 (www.ieee.org).
[63] Biometrics and Privacy, Roger Clarke, Principal Xamax Consultancy, Visiting Fellow Department of Computer Science Australian National University, Notes of 15 april 2001, p. 5. (www.anu.edu.au).
[64] Consumer Biometric Applications : A Discussion Paper, Ann Cavoukian Ph.D., Information and Privacy Commissioner/Ontario, September 1999.

possibilité d'esquiver cette procédure. Pensons à la reconnaissance faciale où le visage d'une personne peut être capturé sans son consentement et même à son insu. Pensons aussi au rythme de frappe sur un clavier où le logiciel de capture peut être installé sans qu'un utilisateur ne le sache.

En 1985 la revue National Geographic publia une photo de Steve McCurry (prise en 1984) d'une jeune Afghane aux yeux verts âgée de 12 ans. Celle-ci, orpheline, vivait dans un camp de réfugiés après un bombardement soviétique. L'Afghanistan suscitant de nouveau l'intérêt, McCurry s'est mis à la recherche de l'Afghane 18 ans plus tard en 2002 et retrouva Sharbat Gula, maintenant agée de 30 ans et la photographia de nouveau. Or avant que National Geographic ne publie la photo, des recherches furent entreprises pour s'assurer qu'il s'agissait bien de la même personne. Florence Aubenas du quotidien Libération nous apprend : « *Il fallait vérifier que les yeux verts de Sharbat étaient bien ceux de l'image. Tout a été mis en œuvre : une méthode par "reconnaissance des caractéristiques faciales*", utilisée par le FBI, puis un programme informatique qui permet d'identifier les personnes recherchées dans les aéroports américains, enfin une analyse scientifique de l'iris »[65]. L'identification fut positive et l'Afghane aux yeux verts trône de nouveau dans la revue National Geographic d'avril 2002.

Une des techniques employées dans cette aventure est la reconnaissance de l'iris. La prestigieuse revue approcha pour réaliser ce travail le professeur John Daugman et la firme Iriscan : « *The inventor of automatic iris recognition, John Daugman, a professor of computer science at Cambridge University, England mathematically determined that the eyes belong to the same person »*[66].

Normalement, le produit d'Iriscan nécessite une procédure d'enrôlement et la présentation de l'œil du sujet à environ 40 centimètres d'une caméra pour fonctionner. Or, pour identifier l'Afghane, Iriscan a utilisé deux simples photos prises à 17 ans d'intervalle. « *Therefore, Iridian's Research Lab scanned the photographic images into digital format and used development software to process the digital image, disabling the security measures normally used to detect photographs »*[67].

Cet exemple révèle que même des technologies, qui normalement nécessitent un consentement des utilisateurs, peuvent facilement être modifiées pour identifier une personne sans son consentement.

[65] Les deux visages de dix-huit ans de guerre, Florence Aubenas, Libération, le jeudi 14 mars 2002.
[66] A Life Revealed, Seventeen years after she stares out from the cover of National Geographic, a former Afghan refugee comes face-to-face with the world once more., National Geographic, vol. 201 no 4, april 2002.
[67] National Geographic's Afghan Girl Positively Identified By Iris Recognition, Iridian Technologies Reveals the Science Behind the Authentication, Iridian Technologies Press Releases, Moorestown, NJ, March 18 2002.

RÉSEAUX ET BANQUES DE DONNÉES CENTRALISÉES

Plusieurs vendeurs de sytèmes biométriques arguent que l'utilisation de leurs produits va permettre de mieux protéger la vie privée, que la biométrie est un puissant outil de protection des renseignements personnels. Cette assertion est basée sur le fait que désormais seules les personnes autorisées à accéder aux données personnelles y accèderont effectivement; quelqu'un peut perdre ou dévoiler son mot passe mais pas son doigt ou son iris.

Outre le fait que certains systèmes soient piratables par la présentation de pièces contrefaites (exemple : photographie d'un visage), d'autres raisons font que les données personnelles protégées par ces systèmes peuvent être mises en péril. Les mesures ou caractéristiques biométriques capturées par les terminaux voyagent dans plusieurs cas sur des réseaux et sont engrangées dans des bases de données, souvent avec d'autres renseignements personnels sur les individus. Les nombreuses vulnérabilités de ces réseaux, des logiciels qui les soutiennent et des bases de données donnent flanc aux attaques. « *The security around the entire financial and network computing infrastructure is based on PINs or passwords. A biometric response of "yes" still has to generate a PIN or password to access the service, thereby introducing another weak link in the chain* »[68].

Certains promoteurs des banques de données centralisées essaient de convaincre que leur approche est meilleure que toute autre en matière de protection de la vie privée, puisqu'ils n'ont qu'un seul dépôt à sécuriser. D'éminents experts en sécurité considèrent cependant que les banques centralisées sont risquées. Récemment, le Dr Stefan Brands, spécialiste mondialement reconnu en sécurité de l'information et en cryptographie, monsieur Henri Quiniou, ingénieur en systèmes informatiques et monsieur Frédéric Légaré, cryptographe, ont déposé un mémoire à la Commission des affaires sociales concernant le projet de carte à microprocesseur et de dossier de santé centralisé de la RAMQ. Le 28 mars 2002, lors d'une séance de cette Commission, monsieur Légaré fit bénéficier les personnes y assistant des connaissances en sécurité de l'information du trio d'experts : « *Si toute l'information est sur ma carte à puce, c'est beaucoup plus compliqué pour quelques personnes x, y, z d'accéder à cette information-là; je parle des personnes non autorisées. Tandis que, s'il y a une banque de données centrale, c'est toujours possible d'accéder à cette information. Mais c'est beaucoup plus facile d'accéder à cette information-là pour une tierce personne malhonnête et qui s'y connaît un peu en informatique ou qui s'y connaît beaucoup d'accéder...* ». C'est sans compter que toute banque de données centrale excite la convoitise des personnes malveillantes. Si une telle banque contient des renseignements personnels sur un grand nombre de personnes et que ces renseignements sont sensibles, cette convoitise n'est qu'attisée.

Ainsi, tout individu malveillant pourra attaquer un système biométrique par la voie des réseaux ou des lacunes des logiciels pour parvenir à ses fins : « *Biometric systems may*

[68] Biometrics as a Privacy-Enhancing Technology : Friend or Foe of Privacy ?, Dr. George Tomko, Chairman Photonics Research Ontario, Privacy Laws & Business 9th Privacy Commissioners Data Protection Authorities Workshop, Spain, September 15th 1998.

work well for the good guys. However, the good guys are not the problem. The security of existing biometric systems at keeping the bad guys out yet to be proven »[69].

DISCRIMINATION

La biométrie pourrait être utilisée par des organismes ou des individus peu scrupuleux pour les discriminer. Cette discrimination pourrait être basée sur les mesures physiques d'une personne. D'ailleurs l'eugénique (dont Francis Galton est le père), qui est bien vivante de nos jours[70], utilisait notamment des mesures physiques pour classer les « naissances nobles ».

Outre ce type de danger, d'autres formes de discrimination sont possibles. Notamment pensons à la prise de décision automatique concernant une personne basée seulement sur le profil virtuel de la personne. Madame Ann Cavoukian nous renseigne à ce sujet : « *These fosters the following concerns : that information will be used out of context to the detriment of the data subject; that unjust decisions about them will be made simply on the basis of that profile; that automatic decision-making will be based on facts of doubtful completeness, accuracy, relevance, or utility; and that all of this will be done without the data subject 's permission »*[71].

Les détournements de finalités dans l'utilisation des données est donc particulièrement à surveiller.

L'EMPREINTE DIGITALE : UN PROBLÈME PARTICULIER

L'utilisation de l'empreinte digitale comme moyen d'identification a une forte connotation policière. Il existe, comme déjà mentionné, d'immenses dépôts de données contenant les empreintes de dizaines de millions d'individus. Une fois que de nouveaux fichiers d'empreintes existeront, ils risquent d'être couramment saisis (ou le système réquisitionné) par la police comme les bandes vidéo actuellement ou comme les documents sous toutes formes des journalistes. La CNIL[72] met ainsi en garde contre ce phénomène : « *Quoiqu'il en soit, la connotation policière ne résulte pas uniquement de ce que la prise d'une empreinte digitale est, à l'origine, une technique policière. Elle est bien plus généralement liée à ce que dans la plupart des cas, si ce n'est tous, la constitution d'un fichier d'empreintes digitales, même à des fins qui ne sont pas illégitimes, va devenir un nouvel instrument de police, c'est-à-dire un outil de comparaison qui pourra être utilisé à des fins policières, nonobstant sa finalité initiale »*[73].

---

[69] Idem.
[70] Eugenics, SCOPE NOTE 28, National Reference Center for Bioethics Literature, The Joseph and Rose Kennedy Institute of Ethics, Georgetown University, Washington.
[71] Consumer Biometric Applications : A Discussion Paper, Ann Cavoukian Ph.D., Information and Privacy Commissioner/Ontario, September 1999.
[72] Commission nationale de l'informatique et des libertés
[73] LES CONTRÔLES D'ACCÈS PAR BIOMÉTRIE, Chapitre 4 ,21e rapport d'activité, CNIL, 2000.

Bien sûr les vendeurs des technologies à base d'empreintes digitales minimisent ces problématiques en invoquant l'incompatibilité des systèmes entre eux. Ils invoquent aussi l'impossibilité de reconstituer une empreinte car il n'y a que des minuties et ultimement des zéros et des uns dans la base de données. La CNIL réfute ces arguments en ces termes : « *Dans le souci d'écarter cet argument, certains opérateurs n'hésitent pas à mettre en avant l'incompatibilité de leur système avec celui employé par la police. Ils font valoir que leur modèle n'est pas une empreinte digitale au sens de la collection des minuties recueillies par la police et qu'il serait impossible de fabriquer cette empreinte digitale à partir du profil de doigt réalisé par leur système… Ainsi, le fait que la base de données ne soit pas une base de données d'images et ne puisse pas être comparée avec une base de données policière est indifférent. Le problème est de savoir si une empreinte relevée sur un verre, une table, un téléphone peut ou non être comparée, une fois analysée, y compris par l'étude des minuties, avec les éléments de référence inclus dans le fichier de ces entreprises… C'est moins l'empreinte digitale qui fait problème, que le stockage d'une numérisation de cette empreinte, que l'information se présente comme une image ou sous la forme d'un code ou d'un numéro* »[74]. Le Dr George Tomko abonde dans le même sens : « *I want to point out that even if the actual fingerprint pattern is not stored, but only a digital template is stored which cannot be converted back to the original fingerprint pattern, you still have the same problem. If the police obtain access to a similar finger scanner, tap into the output of the camera in the scanner, and place some digitized latent fingerprints through the system, they will generate a similar unique template within the accuracy limits of the device* »[75].

Les empreintes digitales sont partout et nous en laissons constamment dans l'environnement. « *Sans doute, l'empreinte digitale présente-t-elle, à la différence d'autres caractéristiques, une spécificité : elle est le seul élément biométrique qui soit omniprésent : où que l'on aille, il est impossible de ne pas laisser de traces de sa présence : les objets que l'on touche (un verre, une table, une lampe de chevet, etc.) mais également désormais un vêtement, c'est-à-dire des objets à surface non lisse. À cet égard, l'empreinte digitale est presque aussi redoutable que les traces ADN* »[76]. L'utilisation de l'empreinte digitale comme procédé d'identification biométrique est donc à limiter au maximum.

UTILISATIONS ANONYMES

Une mesure ou une caractéristique biométrique capturée par un système ne peut être anonyme parce qu'elle constitue elle-même un identifiant. Cependant, il peut exister des systèmes où l'utilisation de la biométrie est anonyme.

---

[74] Idem.

[75] Biometrics as a Privacy-Enhancing Technology : Friend or Foe of Privacy ?, Dr. George Tomko, Chairman Photonics Research Ontario, Privacy Laws & Business 9th Privacy Commissioners Data Protection Authorities Workshop, Spain, September 15th 1998.

[76] LES CONTRÔLES D'ACCÈS PAR BIOMÉTRIE, Chapitre 4 , page 102, 21e rapport d'activité, CNIL, 2000.

Une des avenues les plus intéressantes en matière de protection de la vie privée est l'utilisation locale de la biométrie. Dans ce type de systèmes les données capturées initialement sont enregistrées sur un support portable comme une carte à microprocesseur. Cette carte est détenue exclusivement par la personne à qui appartiennent les données biométriques et n'est gardée sur aucune autre banque de données externes.

Cette approche est intéressante dans la mesure où les traitements et les données résident sur le support portable, sont protégés par un mécanisme de sécurité et qu'il n'existe aucune possibilité pour l'organisation qui offre le procédé de capturer autrement l'information contenue sur la carte, pas même pour des fins de sauvegarde en cas de perte. Cette approche pour être sûre aurait avantage à être complétée par une homologation des produits afin de s'assurer qu'aucune donnée n'est capturée à l'insu des utilisateurs.

Une autre approche d'utilisation anonyme consiste à déposer les mesures ou caractéristiques biométriques capturées dans un fichier central où aucune autre donnée d'identification des personnes n'est saisie. « *Une finalité de vérification peut se contenter d'accepter ou de refuser un accès, ou donner droit à une classe de services, sans pour autant qu'il y ait nécessité d'identification de l'individu. On citera à cet égard les exemples du contrôle d'accès à des zones dangereuses et sécurisées, ou encore une application basée sur la reconnaissance de la géométrie de la main pour la reconnaissance de l'accès des abonnés au parc d'attraction de Disney World en Floride* »[77]. Cependant, dans une telle architecture, la personne ne possède pas un contrôle complet sur ses mesures ou caractéristiques biométriques. Le détenteur des données pourrait réaliser des comparaisons avec d'autres banques de données, contenant le même type de mesures ou caractéristiques biométriques, pour trouver l'identité des personnes. Il pourrait aussi céder ou communiquer la banque à un tiers qui poursuivrait les mêmes objectifs.

[77] Enjeux des techniques de biométrie – Une première approche, Meryem Marzouki, Association IRIS, Paris, 24 septembre 2001.

4. ENVIRONNEMENT JURIDIQUE

Les mesures ou caractéristiques biométriques sont des renseignements personnels puisqu'elles concernent un individu et permettent de l'identifier. Au Québec, la protection des renseignements personnels est régie par deux lois d'application, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) (Loi sur l'accès) et la *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1) (Loi dans le secteur privé).

Plus récemment, le législateur a introduit certaines dispositions particulières concernant la biométrie aux articles 44 et 45 de la Section II du Chapitre III de la *Loi concernant le cadre juridique des technologies de l'information* (L.Q. 2001, c.32) (Loi sur les technologies de l'information). Le Chapitre III de cette loi s'intitule L'ÉTABLISSEMENT D'UN LIEN AVEC UN DOCUMENT TECHNOLOGIQUE et la Section II concerne LES MODES D'IDENTIFICATION ET DE LOCALISATION.

Dans un environnement électronique, des mesures particulières doivent être mises en œuvre afin d'assurer l'équivalence fonctionnelle d'un document et sa valeur juridique. Aussi, lorsque l'identité de la personne liée à un document est assurée par un moyen biométrique, cette nouvelle loi trouve application en conjugaison avec la Loi sur l'accès et la Loi dans le secteur privé selon qu'il s'agisse d'une utilisation de la biométrie dans le secteur public ou le secteur privé.

Les articles 44 et 45 de la Loi sur les technologies de l'information s'énoncent comme suit :

> 44. Nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des mesures ou caractéristiques biométriques. L'identité de la personne ne peut alors être établie qu'en faisant appel au minimum de mesures ou caractéristiques permettant de la relier à l'action qu'elle pose et que parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance.
>
> Tout autre renseignement concernant cette personne et qui pourrait être découvert à partir des mesures ou caractéristiques saisies ne peut servir à fonder une décision à son égard ni être utilisé à quelque autre fin que ce soit. Un tel renseignement ne peut être communiqué qu'à la personne concernée et seulement à sa demande.
>
> Ces mesures ou caractéristiques ainsi que toute note les concernant doivent être détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus.
>
> 45. La création d'une banque de mesures ou caractéristiques biométriques doit être préalablement divulguée à la Commission d'accès à l'information. De même, doit être divulguée l'existence d'une telle banque qu'elle soit ou ne soit pas en service.

La Commission peut rendre toute ordonnance concernant de telles banques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation y compris l'archivage ou la destruction de mesures ou caractéristiques prises pour établir l'identité d'une personne.

La Commission peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction, si celle-ci ne respecte pas ses ordonnances ou si elle porte autrement atteinte au respect de la vie privée.

Les diverses lois en vigueur édictent donc les règles en matière de collecte, d'utilisation, de conservation, de communication auxquelles l'administration publique et l'entreprise privée doivent s'astreindre.

COLLECTE : NÉCESSITÉ ET CONSENTEMENT

La collecte de renseignements personnels est soumise à la règle de la nécessité (art. 64 de la Loi sur l'accès; art. 4 et 5 de la Loi dans le secteur privé). La notion de nécessité a toujours été interprétée par la Commission dans son sens le plus strict et rigoureux comme synonyme d'indispensable. Cette nécessité s'apprécie évidemment dans son contexte.

Ces dispositions impératives amènent l'organisation voulant procéder à la collecte d'une mesure ou caractéristique biométrique à faire la démonstration, non pas d'une simple utilité ou commodité, mais du fait qu'on ne peut rigoureusement pas se passer de cette donnée. Le consentement de la personne à fournir un renseignement personnel ne permet pas de passer outre cette règle.

La Loi sur les technologies de l'information ajoute une nouvelle obligation lorsqu'il s'agit de la collecte d'une mesure ou caractéristique biométrique : le consentement exprès de la personne concernée.

Il est d'emblée exclu que la collecte puisse se faire autrement qu'auprès de la personne concernée. Donc ces mesures ou caractéristiques biométriques ne peuvent être recueillies à l'insu de celle-ci que ce soit au moment de l'enrôlement ou de la vérification de l'identité.

Aussi, on exige de requérir un consentement exprès à la collecte de la mesure ou caractéristique biométrique. La Commission, en matière de consentement, a déterminé les qualités d'un consentement valide. Celui-ci doit être libre, éclairé et donné à des fins spécifiques.

- Le choix de la personne de se voir identifier par un moyen biométrique devra être respecté. Son refus d'utiliser un tel moyen pour s'identifier devra prévaloir malgré la démonstration de la nécessité.
- Un consentement éclairé devra permettre à l'individu de comprendre les impacts de l'utilisation de la biométrie et d'en mesurer les risques, de connaître comment les

données recueillies seront protégées, utilisées, communiquées et à quel moment elles seront détruites.
- Un consentement donné à des fins spécifiques permettra à l'individu de connaître précisément quelles données seront recueillies et utilisées.

De plus, l'article 44 précise qu'une quantité minimale de caractéristiques peuvent être recueillies lorsque justifiées.

FINALITÉ ET UTILISATIONS

Pour justifier la nécessité de la collecte, il faut préalablement avoir déterminé la finalité poursuivie par la constitution du fichier de renseignements personnels et l'utilisation qui sera faite des renseignements recueillis. Ces utilisations doivent par ailleurs être déclarées à la personne concernée au moment de la collecte (art. 65 Loi sur l'accès et art. 8 Loi dans le secteur privé).

Dans le cadre juridique couvert par la Loi sur les technologies de l'information, la donnée biométrique servira essentiellement à identifier l'individu pour y lier un document. La nécessité d'identifier la personne dans le cadre de la finalité poursuivie devra être intrinsèquement indispensable.

Les mesures ou caractéristiques biométriques ne devront donc être utilisées qu'afin d'identifier l'individu et tout autre information révélée par ces données ne pourra être utilisée à quelque autre fin que ce soit.

CARACTÈRE CONFIDENTIEL : CONSERVATION ET DESTRUCTION

Les mesures ou caractéristiques biométriques comme la plupart des renseignements personnels sont confidentielles et doivent être protégées par des mécanismes propres à assurer leur caractère confidentiel (art. 53 Loi sur l'accès, art. 10 Loi dans le secteur privé). La qualité des données conservées se doit d'être protégée afin d'utiliser des renseignements exacts et à jour (art. 72 Loi sur l'accès et art. 11 Loi dans le secteur privé). L'intégrité des renseignements entreposés est cruciale lorsqu'il s'agit de mesures biométriques puisque la fonction d'identification d'un individu ne peut être approximative sans risquer de générer de la discrimination.

Les mesures ou caractéristiques biométriques sont assorties d'une exigence plus urgente de destruction. On précise à l'article 44 que ces données doivent être détruites lorsque l'objet qui fonde la vérification d'identité est accompli ou lorsque le motif qui la justifie n'existe plus.

ACCÈS PAR LE PERSONNEL DE L'ORGANISATION

L'accès par le personnel de l'organisation est usuellement restreint aux seules personnes qui ont qualité pour recevoir et qui doivent utiliser ces renseignements dans l'exercice de leurs fonctions (art. 62 Loi sur l'accès et art. 20 Loi dans le secteur privé). Les privilèges

d'accès devraient, à l'égard des données biométriques, être des plus restreints puisque le mécanisme d'enrôlement et de validation de l'identité est partie intégrante des systèmes biométriques et que ces données ne devraient pas pouvoir être manipulées directement.

COMMUNICATION

Les renseignements personnels, dont les mesures ou les caractéristiques biométriques, exigent pour être communiqués un consentement de la personne concernée ou une disposition législative qui autorise cette communication (art. 59 Loi sur l'accès et art. 13 Loi dans le secteur privé).

DROITS D'ACCÈS ET DE RECTIFICATION

Les droits d'accès et de rectification des renseignements personnels détenus par l'administration publique (art. 83 et 89 Loi sur l'accès) ou l'entreprise privée (art. 27 et 28, Loi dans le secteur privé et art. 40 Code civil) demeurent applicables aux données biométriques.

CONSTITUTION DE BANQUES DE CARACTÉRISTIQUES BIOMÉTRIQUES

L'article 45 de la Loi sur les technologies de l'information initie une nouvelle obligation pour les organisations qui souhaitent utiliser la biométrie et constituer une banque de mesures ou de caractéristiques biométriques. Ces organisations doivent, préalablement à la création d'une telle banque, divulger cette création à la Commission. De même, les banques existantes en opération ou non doivent aussi être signalées à la Commission.

La Commission se voit investie d'un pouvoir d'ordonnance concernant ces banques de renseignements personnels particulièrement sensibles. Ainsi, elle pourra en déterminer la confection, l'utilisation, la consultation, la communication et la conservation, de même elle pourra interdire ou suspendre la mise en service d'une banque ou ordonner sa destruction si cette banque porte atteinte au respect de la vie privée.

Toutefois, un système de sécurité qui ne ferait que permettre l'ouverture d'une porte pour entrer dans un local, sans que l'heure d'entrée, que l'identité de la personne ou que toute autre donnée ne soient enregistrée ou journalisée et à partir duquel il serait impossible de créer un document (registre, rapport…) ne serait pas soumis à l'article 45 de la Loi sur les technologies de l'information. Ceci implique aussi qu'aucune journalisation des accès ne soit effectuée.

De même, et toujours à titre d'exemple, un système où les mesures ou caractéristiques biométriques seraient conservées uniquement sur un support portable comme une carte à microprocesseur ou sur le disque dur d'un ordinateur personnel, dont seule la personne concernée a le contrôle entier, y incluant toute copie, ne serait également pas soumis à l'article 45 de la Loi sur les technologies de l'information.