UNIVERSITÉ DU QUÉBEC À MONTRÉAL

LA BIOMÉTRIE, SA FIABILITÉ ET SES IMPACTS SUR LA PRATIQUE DE LA DÉMOCRATIE LIBÉRALE

MÉMOIRE
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN SCIENCE POLITIQUE

PAR
FRÉDÉRIC MASSICOTTE

NOVEMBRE 2007

Remerciements

La rédaction de ce mémoire était la dernière étape avant de compléter ce programme de maîtrise en science politique à l'Université du Québec à Montréal. Je tiens à remercier M. Alex Macleod, mon directeur de mémoire, qui a apporté corrections et commentaires sur ce travail pour en permettre son aboutissement.

Table des matières

LISTE DES GRAPHIQUES, TABLEAUX, SCHÉMAS ET PHOTOS V
LISTE DES SIGLES VII
RÉSUMÉ IX
INTRODUCTION 1
LES DÉBATS SUR LA BIOMÉTRIE 6
POURQUOI LA BIOMÉTRIE ? 15
LE CONCEPT DE CONTRÔLE DE L'ACCÈS AUX FRONTIÈRES PERSONNELLES 16
Sphère privée et sphère publique *22*
Degrés de vie privée *25*
PLAN DU MÉMOIRE 26
CHAPITRE 1 : BRÈVE HISTOIRE DE LA BIOMÉTRIE 28
BERTILLONNAGE 30
EMPREINTES DIGITALES ET DES PAUMES DES MAINS 31
GÉOMÉTRIE DE LA MAIN 37
RECONNAISSANCE FACIALE 38
IRIS 39
RÉTINE 40
VEINES 41
PAR LA VOIX 41
PAR LA SIGNATURE 42
L'ADN 43
SYSTÈMES EXPÉRIMENTAUX 44

CHAPITRE 2 : LES DIVERSES TECHNOLOGIES BIOMÉTRIQUES MODERNES 46
ADN 50
MAIN (EMPREINTES DIGITALES, GÉOMÉTRIE DE LA MAIN ET ANALYSE DES VEINES) 54
VISAGE (RECONNAISSANCE FACIALE, ANALYSE DE L'IRIS ET DE LA RÉTINE) 58
BIO-DYNAMIQUE (ANALYSE DE LA VOIX, ANALYSE DE LA SIGNATURE) 61
FONCTIONNEMENT DES SYSTÈMES BIOMÉTRIQUES 64
FIABILITÉ DE CES TECHNOLOGIES 68
L'ADN *68*
Reconnaissance faciale *71*
Empreintes digitales *73*
Les autres technologies biométriques *74*
Problèmes techniques *77*
Une technologie facilement déjouable *79*
CHAPITRE 3 : IMPACTS DE LA BIOMÉTRIE SUR LA PRATIQUE DE LA DÉMOCRATIE LIBÉRALE 84
BIOMÉTRIE ET LA PRATIQUE DE LA DÉMOCRATIE LIBÉRALE 90
BASES DE DONNÉES 91
PANOPTICON 93
LA BIOMÉTRIE ET LA LUTTE CONTRE LA CRIMINALITÉ ET LE TERRORISME 100
RISQUE DE GLISSEMENT 106
Étude de cas : l'utilisation du numéro d'assurance sociale aux États-Unis *117*
CONCLUSION 123
ANNEXE 131
BIBLIOGRAPHIE 137

Liste des graphiques, tableaux, schémas et photos

Graphique 1A - Parts des marchés mondiaux en 2001 page 47

Graphique 1B : Revenus totaux et mondiaux provenant de la vente de technologies biométriques de 1999 à 2005 page 48

Tableau 1 : Tableau synthèse sur les données biométriques page 49

Tableau 2 : Comparaison entre deux lectures du même vecteur et un autre vecteur contenu dans la base de données page 66

Schéma 1 : Caractéristiques des minuties d'une empreinte digitale page 55

Schéma 2 : Veines du doigt et sa reconnaissance page 57

Schéma 3 : Ondelette de Gabor page 59

Schémas 4 et 5 : Exemples d'analyse de signature dynamique page 62

Schéma 6 : Analyse spectrale de la voix page 64

Schéma 7 : Élevation, section et plan de coupe du Panopticon de Jeremy Bentham page 94

Photo 1 : Autoradiographie d'ADN page 53

Photo 2 : Géométrie de la main page 56

Photo 3 : Reconaissance par les veines de la main page 57

Photo 4 : Technique de moulage d'une empreinte digitale page 130

Photo 5 : Technique pour la fabrication d'une empreinte digitale page 131

Photo 6 : Version améliorée et très discrète d'une empreinte digitale fabriquée page 132

Photo 7 : Déjouer un lecteur facial grâce à un ordinateur portable page 133

Photo 8 : Technique pour prélever une empreinte digitale latente à partir d'un lecteur à empreinte digitale page 134

Photo 9 : Un journaliste met une photo d'iris, avec un trou au milieu, devant son œil afin de déjouer un système à iris page 135

Liste des sigles

ADN - Acide DésoxyriboNucléique

AFDC (Aid to Families with Dependent Children)

AFIS - Automated Fingerprint Identification System

CAS - Carte d'Assurance Sociale

CSE - Child Support Enforcement

EBGM - Elastic Bunch Graph Matching

FERET - FacE RecogniTion

GRC – Gendarmerie Royale du Canada

IA - Intelligence artificielle

IAFIS - Integrated Automated Fingerprint Identification System

INSPASS - Immigration and Naturalization Service Passenger Accelerated Service System

IR - Infrarouge

IRS - Internal Revenue Service

LDA - Linear Discriminant Analysis (analyse linéaire discriminante)

NAS - Numéro d'Assurance Sociale

NIP - Numéro d'Identification Personnel

NSA - National Security Agency

NIST - National Institute of Standards and Technology

PCA - Principal Components Analysis (analyse en composantes principales)

PCR - Polymerase Chain Reaction (amplification en chaîne par polymérase)

RFLP - Restriction Fragment Length Polymorphism

SAAQ - Société de l'assurance automobile du Québec

STR - short tandem repeats

UKPS - United Kingdom Passport Service

VNTRs – Variable Number of Tandem Repeats

Résumé

La biométrie, c'est-à-dire la technologie qui mesure les caractéristiques du vivant, est de plus en plus utilisée depuis une dizaine d'années, surtout dans le domaine de la sécurité. Celle-ci connaît une croissance exponentielle depuis les attentats du 11 septembre 2001, surtout que cet acte terroriste a été suivi par ceux de Madrid en 2004 et de Londres en 2005. Le terrorisme a par conséquent imposé le thème de la sécurité à tous les acteurs de la société, tant les décideurs que les simples citoyens. La biométrie s'impose donc de plus en plus aux yeux des États comme solution sécuritaire par excellence ce qui n'est pas sans inquiéter les organisations de défense des droits de l'Homme.

Ce mémoire aborde deux questions centrales : est-ce que l'application généralisée de technologies biométriques peut être garante de l'atteinte d'un niveau idéal de sécurité personnelle et collective d'une part et est-ce que, d'autre part, l'utilisation de ces technologies menace le droit à la vie privée.

La démocratie libérale, un concept clé dans ce travail, est fondée sur le concept du privé : le citoyen privé qui est protégé du gouvernement avec des droits inaliénables dont celui, dans la plus pure tradition de John Locke, de la propriété privée et qui a donné vie au concept de la sphère privée vue comme un sanctuaire sur lequel même les plus puissants, en particulier le gouvernement, ne pourraient empiéter. C'est pourquoi l'idée de vie privée est le concept central de ce travail et le sous-tendra tout au long de celui-ci. Ainsi seront définis et explicités les concepts de sphère privée et de sphère publique qui seront aussi complétés avec les différents degrés de vie privée.

Le cadre analytique de ce mémoire abordera cette question en utilisant le concept du contrôle informationnel (c'est-à-dire le contrôle qu'un individu peut ou non exercer sur l'information que des organisations possèdent sur lui) et celui du contrôle sensoriel (l'accès et le non-accès physiques et mentaux aux organes sensoriels des autres ou des institutions).

Ce mémoire est divisé en trois chapitres. Les deux premiers sont essentiellement factuels et empiriques : le premier aborde l'histoire de la biométrie tandis que le deuxième présente son aspect technologique et sa fiabilité. Le troisième chapitre, normatif, est le cœur du mémoire, et analyse les conséquences de la biométrie sur la vie privée et par conséquent sur la

pratique de la démocratie libérale. C'est dans ce chapitre que les deux fonctions explicitées dans le cadre analytique seront utilisées.

D'abord, le contrôle informationnel sera surtout utilisé pour la première section sur les banques de données de plus en plus omniprésentes ainsi que pour la quatrième et dernière section portant sur le risque de glissement vers une situation non initialement prévue (de l'anglais *creep function*) du fait de la perte sournoise de contrôle des informations que les institutions et les organisations détiennent sur les gens avec en exemple une étude de cas sur le numéro d'assurance sociale aux États-Unis. La troisième partie portant sur le terrorisme sera aussi abordée en partie sous cet angle.

La deuxième fonction, le contrôle de l'accès sensoriel, est celle qui permet ou non d'avoir une sphère privée avec tout ce que cela implique et permet d'analyser les 2^{e} et 3^{e} parties de ce chapitre, c'est-à-dire le *Panopticon* et son risque de normalisation des comportements et de la société en général et puis la lutte contre la criminalité et le terrorisme qui tend à justifier fallacieusement un peu tout et n'importe quoi dans le domaine biométrique.

C'est un travail essentiellement normatif, autour d'une thématique qui oriente la réflexion sur le sujet de la vie privée, la sécurité et de la démocratie. C'est donc la question du droit à la vie privée qui sous-tend ce travail.

Mots clés : Biométrie, démocratie libérale, sphère privée, vie privée, sécurité, technologies de sécurité.

Introduction

La biométrie, c'est-à-dire la technologie qui mesure les caractéristiques du vivant, est de plus en plus utilisée depuis une dizaine d'années, surtout dans le domaine de la sécurité, par exemple dans les aéroports. Le domaine de la sécurité connaît une croissance exponentielle depuis les attentats du 11 septembre 2001, surtout que cet acte terroriste a été suivi par ceux de Madrid en 2004 et Londres en 2005. Le terrorisme a par conséquent imposé le thème de la sécurité à tous les acteurs de la société, tant les décideurs que les simples citoyens. Chacun cherche un moyen de régler ce problème, personne ne veut que prendre le métro devienne un sport extrême.

C'est ainsi que de plus en plus d'États ont jonglé avec l'idée d'imposer une carte d'identité biométrique obligatoire que tous les citoyens devraient avoir sur eux en tout temps et qui pourrait être demandée par les policiers, et déjà il est certain que les passeports seront biométriques d'ici quelques années. C'est un peu la tentation technologique qui semble affecter les autorités des démocraties libérales, cette tendance à croire à la perfection technologique pour régler des problèmes non technologiques, qui voient en la biométrie une solution aux problèmes de sécurité induits par le terrorisme et la criminalité.

De l'autre côté, plusieurs organisations de défense des droits de l'Homme évoquent la menace que l'implantation de technologies biométriques fait peser sur les droits et libertés. Même les simples citoyens n'ont qu'à se rappeler des livres *1984* et *We* ou des films comme *Gattaca*, *Ennemi d'État* (*Enemy of the State*) et *Rapport minoritaire* (*Minority Report*) pour comprendre le sérieux de la situation et se rendent comptent de

jusqu'où les choses peuvent aller. C'est pourquoi les défenseurs des droits de l'Homme estiment qu'il faut y penser deux fois avant de s'embarquer dans cette voie. Mais surtout qu'avant toute chose il faut qu'un véritable débat ait lieu pour comprendre la nature de la biométrie et ses conséquences et aboutissements. À l'opposé, les gouvernements veulent accélérer les choses et parlent d'équilibre entre liberté et sécurité, diminuant la première pour favoriser la seconde.

La société contemporaine se trouve ainsi dans la période la plus intéressante du dossier biométrique, c'est-à-dire celle où elle n'a encore pris aucune décision quant à l'avenir de la biométrie comme technologie de sécurité, sera-t-elle refusée ou acceptée seulement dans certains endroits ou encore partout ?

Mais qu'est-ce que la biométrie ? La biométrie est la mesure des caractéristiques physiques d'un individu, que ce soit ses empreintes digitales, la forme de son visage ou encore son ADN. La biométrie est surtout employée dans le domaine de la sécurité et de la lutte au crime, l'utilisation la plus connue étant les banques d'empreintes digitales des criminels et des empreintes laissées sur le lieu des crimes. Mais la biométrie est aussi utilisée pour contrôler l'accès à certains endroits ou encore à certains objets, par exemple certains ordinateurs portables nécessitent une empreinte digitale pour les utiliser.

Plus précisément, la biométrie constitue un caractère physique ou comportemental qui est universel, unique à chaque personne, permanent dans le temps et finalement qui puisse être répertorié et mesuré fiablement à

des fins de comparaisons[1]. Plus schématiquement, les technologies biométriques doivent idéalement posséder plusieurs caractéristiques[2] :

1. L'unicité : chaque attribut biométrique doit varier énormément d'une personne à l'autre au point que l'ensemble des variations rend cet attribut unique.

2. La robustesse : un attribut biométrique devrait être permanent tout au long de la vie d'une personne.

3. La quantifiabilité : cet attribut doit être mesurable et quantifiable.

4. L'acceptabilité par la population (les empreintes digitales sont souvent associées à la criminalité).

5. L'universalité : quelle proportion de la population a cet attribut (certaines personnes n'ont pas d'empreintes digitales par exemple[3]).

Notre sujet sera limité dans le temps à la période qui commence vers la fin du XX^{e} siècle, c'est-à-dire à partir du moment de l'apparition sur le marché et en quantité massive de solutions biométriques abordables aux problèmes sécuritaires, jusqu'à nos jours. Les limites spatiales sont plus floues, car l'implantation de la biométrie comme système de sécurité est en voie d'adoption dans plusieurs pays et régions du monde, mais affecte en particulier les démocraties libérales, l'objet de ce travail.

---

[1] Prabhakar, Salil, Sharath Pankanti et Anil K. Jain, « Biometric Recognition: Security and Privacy Concerns », In *Security & Privacy Magazine IEEE*, 1, 2, mars-avril 2003, pp. 33-35.
[2] K Sethi, Ishwar, « 7 : Biometrics : Overview and Applications », In J. Strandburg, Katherine et Daniela Stan Raicu (sous la dir.), *Privacy and Technologies of Identity – A Cross-Disciplinary Conversation,* Springer Science+Business Media, Inc. 2004. pp. 122 à 123.
[3] Van Den Nieuwendijk, Hans, *No Fingerprints?*, [en ligne], http://www.xs4all.nl/%7Edacty/noprints.htm, (consulté le 23 septembre 2006).

Ce mémoire aborde deux questions centrales : est-ce que l'application généralisée de technologies biométriques peut être garante de l'atteinte d'un niveau idéal de sécurité personnelle et collective d'une part et est-ce que, d'autre part, l'utilisation de ces technologies menace le droit à une vie privée. Bref, introduire la biométrie en vaut-il la peine, face aux coûts qu'elle risque d'entraîner pour l'avenir de la démocratie ? Car il est évident qu'il faut se demander dans quelle mesure les technologies biométriques apportent la sécurité ou non, mais aussi si l'application de la biométrie rétrécit l'espace privée et, si oui, dans quelle mesure. Ce n'est qu'à la suite d'une telle analyse qu'il sera possible d'en arriver à une conclusion éclairée.

Cette problématique est importante du fait que la vie privée est un aspect essentiel de toute démocratie libérale. Mais notre époque comporte aussi un nouveau phénomène, celui du terrorisme apocalyptique qui diffère de beaucoup du terrorisme politique classique de la deuxième moitié du XX^{e} siècle. Ce terrorisme, symbolisé par les attentats du 11 septembre aux États-Unis, a marqué les consciences collectives et alimenté les questions sur les possibilités d'un terrorisme utilisant des armes chimiques, biologiques ou encore, la somme de toutes les peurs, l'arme nucléaire. Devant ces menaces, il est normal que tous demandent, exigent même, que l'État se porte garant de sa plus importante fonction régalienne : la protection de ses citoyens. La biométrie est présentée par ses partisans non seulement comme une partie de la solution au problème du terrorisme, mais bien comme la meilleure solution possible. Passeports, discours sur une carte d'identité biométrique ou encore les lecteurs biométriques qui font leur apparition ici et là, toutes les personnes en autorité assurent à tous que tout sera mieux avec la biométrie. C'est devant les nombreuses initiatives de biométrisation de la vie en société

en vue de sa sécurisation qu'il est nécessaire de se poser la question de savoir si en voulant une sécurité absolue, la société n'est pas en train de menacer un des fondements de la démocratie libérale : l'espace privé.

Cette problématique amène la possibilité de faire un des quatre constats suivants. Soit la biométrie procure une meilleure sécurité sans menacer l'espace privé. Ou la biométrie apporte la sécurité, mais menace la sphère privée. Ou encore la biométrie ne fonctionne pas, mais ne menace pas l'espace privé. Et comme dernière possibilité, la biométrie n'apportera pas la sécurité et en plus menacera la sphère privée. Ce mémoire entend trouver lequel de ces quatre constats s'applique lorsqu'il est question de l'implantation de la biométrie dans une démocratie libérale. Cela revient à poser les questions sur la façon dont la biométrie affecte le fonctionnement de la démocratie libérale et surtout une de ses caractéristiques fondamentales, l'espace privé, qui semble menacé d'un rétrécissement irrémédiable. En définitive, ce mémoire s'interroge sur un aspect fondamental de ce débat, dans quelle mesure est-il possible de mener la quête de sécurité sans brimer les principes de la démocratie libérale dont l'espace privé en est l'incarnation ?

L'idée de vie privée est le concept central de ce travail et le sous-tendra tout au long de celui-ci. C'est à cause de l'importance que la démocratie libérale, autre concept essentiel et crucial de ce mémoire, accorde à la sphère privée qu'il faut faire de celle-ci un concept clé dans l'analyse de la biométrie et de ses impacts sur la démocratie et la vie privée. La démocratie libérale est fondée sur le concept du privé : le citoyen privé qui est protégé du gouvernement avec des droits inaliénables dont celui, dans la plus pure tradition de John Locke, de la propriété privée et qui a donné vie au concept de la sphère privée vue comme un sanctuaire sur lequel même les

plus puissants, en particulier le gouvernement, ne pourraient empiéter. En 1763, William Pitt, Comte de Chatham en Grande-Bretagne et premier ministre, disait : « The poorest man may in his cottage bid defiance to all the forces of the Crown. It may be frail -- its roof may shake -- the wind may blow through it -- the storm may enter -- the rain may enter -- but the King of England cannot enter; all his forces dare not cross the threshold of that ruined tenement »[4]. Par cette citation, il faut conclure que plus une société est libérale, plus la sphère privée y est développée et protégée. En regard de ce que doit être une démocratie, il est évident que plus une société est démocratique, plus la dignité du citoyen y est respectée et prisée, donc que la vie privée y est honorée et estimée.

Les débats sur la biométrie

Si la biométrie est un sujet récent, il reste néanmoins que le débat sur les technologies de sécurité et les libertés ne date pas d'hier, c'est en fait un souci que les intellectuels ont depuis longtemps. Ici seront présentées les principales contributions sur le sujet. Il faut cependant noter que puisque que la biométrie est une technologie extrêmement récente et évolue rapidement, il est normal que l'internet soit une importante source d'information sur le sujet, surtout afin d'être à jour dans la compréhension de la biométrie et de ses impacts.

Un des concepts principaux qu'il faut explorer dans le cadre de la problématique est celui de la vie privée. Il y a quatre auteurs qui ont beaucoup contribué à la réflexion juridique sur cette notion. Commençons par

---

[4] Alba, Bonnie, « Americans' Illusive Privacy - 'Man No Longer King of His Castle' », 6 mars 2006, [en ligne], http://www.americanchronicle.com/articles/viewArticle.asp?articleID=6572, (consulté le 13 janvier 2007).

deux d'entre eux, Samuel Warren et Louis D. Brandeis, deux universitaires qui allaient devenir juges à la Cour suprême des États-Unis. Ces pionniers en matière de vie privée sont les premiers qui ont voulu la faire reconnaître comme un véritable droit, une valeur unifiée et sacrée[5]. Leur contribution majeure est leur article « The Right to Privacy » de 1890 dans la *Havard Law Review*[6]. Ils abordent dans cette revue la nécessité de mieux protéger la vie privée dans un monde de plus en plus technologique, notamment la presse qui abusait selon eux du premier amendement (liberté d'expression), surtout avec l'apparition de la photo. Donc c'est un contrepoids au premier amendement que les futurs juges envisageaient avec leur « right to be left alone ». Encore aujourd'hui, leur influence est notoire.[7]

Ensuite, il faut citer Alan F. Westin, professeur de « Public Law and Government » à l'Université Columbia, premier auteur à donner une définition complexe et à plusieurs variables de ce qu'est la vie privée. Il propose cette définition dans sa plus grande œuvre sur le sujet, *Privacy and Freedom*, publiée en 1967. Selon Westin, la vie privée contient quatre variables[8] :

1. L'autonomie personnelle, qui implique d'être capable de décider quand entrer et sortir de la sphère publique;

2. Le soulagement émotionnel, qui permet de mettre de côté les rôles sociaux (un professeur de français n'aurait pas à porter la même attention à la qualité de son français une fois qu'il est à la maison) et

---

[5] Schoeman, Ferdinand, « 1 : Privacy : philosophical dimensions of the litterature », In Schoeman, Ferdinand David (sous la dir.), *Philosophical Dimensions of Privacy,* Cambridge, Cambridge University Press, 1984, pp. 15-16.
[6] Warren, Samuel et Louis D. Brandeis, « The Right to Privacy », *Harvard Law Review*, IV, décembre, 1890.
[7] *Idem.*
[8] McLean, Deckle, *Privacy and it's Invasion*, Westport, Praeger Publishers, 1995, p. 51.

de décompresser du stress causé par les activités exercées dans la sphère publique;

3. L'introspection, qui permet par l'intimité de recentrer sa pensée sur soi-même afin d'intégrer les diverses expériences de vie;

4. La communication privée, qui permet d'échanger franchement avec des gens du cercle intime.

Cette définition et les concepts que Westin développe dans son livre permettent aussi de regrouper à peu près tous les auteurs, même les plus modernes, sur la définition de la vie privée. Il y a, avant son temps, le principe d'accessibilité (que Westin appelle *autonomie personnelle*) de Ruth Gavison (en 1980)[9]. Même le grand philosophe Ferdinand Schoeman pourrait s'y retrouver avec sa définition de la vie privée basée sur la protection de l'individu contre les charges sociales excessives (*social overreaching*) (que Westin appelle *soulagement émotionnel et introspection*)[10].

Alan F. Westin a aussi publié plusieurs titres sur la vie privée bien avant que cette question ne devienne vraiment préoccupante, notamment *Information Technology in a Democracy* en 1971, *Databanks in a Free Society* en 1972, *Computers, health records, and citizen rights*, en 1976 et *E-commerce & privacy: What net users want*, en 1998.

Le dernier de ces auteurs est Jeffrey Reiman, l'un des premiers à analyser la vie privée à partir d'une approche fonctionnaliste et qui donne

---

[9] Gavison, Ruth, « Privacy and the Limits of Law » In *Yale Law Journal*, 89, 1980, p. 421 et pp. 428-436.

[10] Schoeman, Ferdinand, *Privacy and Social Freedom*, Cambridge, Cambridge University Press, 1992, p. 1.

trois fonctions de la vie privée qui constituent sa définition de celle-ci, soit les fonctions extrinsèques, intrinsèques et psycho-politiques. D'abord, extrinsèquement, il ne faut pas oublier que la vie privée protège les individus de la pression sociale à se conformer (éviter le ridicule), et que même si les gens peuvent faire face à la pression sociale, il s'agit d'une charge injuste envers ceux qui pensent différemment[11]. Il rejoint le concept de soulagement émotionnel et d'autonomie personnelle de Westin sur ce point.

Intrinsèquement, la vie privée n'est pas seulement là pour protéger les libertés. Elle fait partie de la liberté, du fait que sans vie privée, c'est la capacité d'agir qui est bloquée, la liberté étant la base pour qu'un choix soit un choix[12]. Mais la vie privée est aussi la reconnaissance de l'autre comme une personne à part entière, comme propriétaire de sa propre vie[13].

Enfin, sur le plan psycho-politique, il y a une corrélation entre la vie privée et l'âge adulte. Plus l'enfant vieillit, plus il acquiert une vie privée et lorsqu'il devient adulte, il l'obtient totalement. Sans vie privée, il ne pourrait y avoir qu'une infantilisation de la société[14], où il n'y a plus ni dignité humaine ni individualité et l'individu devient fongible (interchangeable, remplaçable) et opine en faveur du plus petit dénominateur commun (la rectitude politique en est un symptôme). Les gens finissent par intégrer ces opinions et la société devient stérile et conformiste[15]. Cela *totalitarise* la société car conformité et élections, et donc démocratie, ne vont pas ensemble[16]. Reiman permet ainsi

---

[11] Reiman, Jeffrey, « Driving to the Panopticon : A philosophical exploration of the risks to privacy posed by the information technology of the Future ». In Rössler, Beate, (sous la dir.), *Privacies : Philosophical evaluations*, Palo Alto, Stanford University Press, 2004. pp. 202-203.
[12] *Ibid.*, pp. 203-205.
[13] *Ibid.*, pp. 205-206.
[14] *Ibid.*, pp. 206-208.
[15] *Idem.*
[16] *Ibid.*, p. 208.

de relier directement la vie privée et la démocratie comme concepts inséparables.

Un autre thème qui est important pour cette problématique est celui de la sphère privée et de la sphère publique. Trois auteurs se dégagent dans ce débat. W. L. Weinstein est le premier à vraiment développer l'idée de vie privée, ce que les autres penseurs n'abordaient que légèrement lorsqu'ils parlaient de la sphère publique, leur vrai sujet d'étude. Il développe l'idée de vie privée, son origine, sa nature de norme sociale et les conditions de son existence[17]. En opposant la sphère privée à la sphère publique, il montre les bases normatives des deux concepts mais aussi que les deux sphères empiètent l'une sur l'autre, tant la publique sur la privée que la privée sur la publique.[18]

Helen Nissenbaum est une autre intellectuelle qui a contribué sur le sujet dans « Protecting Privacy in an Information Age: The Problem of Privacy in Public », d'abord en illustrant la nécessité de tenir compte de l'intégrité contextuelle qui fait en sorte que quelque chose relevant du domaine public dans une situation donnée peut faire partie de l'espace privé dans une autre situation, donc même les informations non confidentielles doivent jouir d'une certaine protection. Mais elle ajoute aussi l'aspect technologique au débat de la dichotomie privée et publique. Elle démontre pourquoi la présence de plus en plus croissante de la technologie, qui permet de faciliter la surveillance et les empiètements sur la vie privée, doit permettre d'étendre l'espace privé en dehors de la sphère privée telle qu'elle est définie traditionnellement. Elle

---

[17] Weinstein, W. L., *Privacy,* New York, Atherton Press, inc., 1971. pp. 27-28.
[18] *Ibid.*, p. 33.

critique aussi la technologisation de l'information qui menace l'anonymat public et explique les dangers que cela comporte[19].

Sur l'anonymat public, Peter Hope-Tindall, ancien conseiller spécial pour les dossiers de cryptage et de biométrie à la « Ontario Information and Privacy Commission », apporte sa contribution en démontrant que même dans la sphère privée il est possible d'avoir une certaine attente de vie privée. Il propose les concepts d'observabilité (un individu doit s'attendre à être vu en public), de capacité de lier (*linkability*) (il n'est pas possible pour quelqu'un de faire le lien entre les actions d'une personne sur la rue et son nom à moins de la connaître) et l'idée d'anonymat ou pseudonymité (si dans un lieu donné personne ne sait le nom de quelqu'un, il peut prétendre être n'importe qui).[20] Alors même en public il reste une forme d'anonymat, une forme de sphère privée.

Un troisième thème important est celui de la technologie en tant que moyen pour amener la sécurité. Le premier contributeur sur ce thème est Bruce Schneier avec ses multiples articles dans sa revue *Crypto-Gram*[21] ainsi que son livre *Beyond fear : Thinking Sensibly About Security in an Uncertain World*[22]. Bruce Schneier se concentre sur les failles des systèmes qui se veulent parfaits. Il démystifie la biométrie et la sécurité et prône une approche modérée face à la sécurité notamment qu'il faut davantage accorder

---

[19] Nissenbaum, Helen, « Protecting Privacy in an Information Age: The Problem of Privacy in Public », University Center for Human Values, Princeton, Princeton University, Law and Philosophy, 17, 1998 : pp. 559-596.

[20] Hope-Tindall, Peter, *Public Space, Private Space: Where do we draw the line ?*, Information Rights Salon, 29 octobre 2002, diapositives #7 à 14 [en ligne], http://www.fis.utoronto.ca/research/inforights/PHT-Presentation.ppt, (consulté le 15 février 2006).

[21] Schneier, Bruce, « Fun with Fingerprint Readers », In *Crypto-Gram Newsletter*, 15 mai 2002, [en ligne], http://www.schneier.com/crypto-gram-0205.html#5, (consulté le 8 février 2006).

[22] Schneier, Bruce, *Beyond Fear : Thinking Sensibly About Security in an Uncertain World*, Springer+Business Media, 2003.

d'importance à l'élément humain de la sécurité plutôt qu'à l'élément mécanique ou aux gadgets de la sécurité. Il attire l'attention sur le fait que les avancées technologiques peuvent rendre plus vulnérable et non moins, et qu'il faut donc analyser sérieusement les choses avant de s'engager dans une technologie et de l'adopter. Aussi, il propose une grille d'analyse de la biométrie très intéressante[23] :

1) Quel problème la « solution » va-t-elle régler ?

2) Dans quelle proportion le problème sera-t-il réglé ?

3) Est-ce que des problèmes nouveaux vont émerger de l'implantation de la solution ?

4) Coût économique et social.

5) Cela en vaut-il la peine ?

Le deuxième auteur retenu sur ce thème est Charles Mann, autre spécialiste de la biométrie et de la sécurité, qui met en garde les gens contre la tentation technologique, un peu comme le fait Bruce Schneier. Son article phare en ce domaine est « Homeland insecurities », publié en 2002. Il affirme que mettre en place une mesure visant à améliorer la sécurité ne veut pas nécessairement dire plus de sécurité pour la population, dans certains cas c'est même l'inverse ! Il donne l'exemple des manufacturiers qui, au cours des années 1990, ont implanté dans les automobiles des systèmes anti-démarreurs pour diminuer le nombre de vols de voiture. La réaction des criminels a été de faire des « carjacking », c'est-à-dire voler la voiture pendant qu'elle fonctionne en expulsant *manu militari* son propriétaire. Alors

[23] Ackerman, Linda, *Biometrics And Airport Security*, Privacyactivism.org, 17 février 2003, [en ligne], http://www.privacyactivism.org/Item/64, (consulté le 1er juin 2006).

les gens sont maintenant à la fois victimes de vol et de voies de fait, au lieu de simplement s'être fait voler[24]. Les systèmes biométriques aggravent la situation. Par exemple, en utilisant la biométrie pour remplacer les clés de voiture, les voleurs doivent utiliser des moyens draconiens pour arriver à leurs fins : en Malaisie, des voleurs de voiture ont coupé un doigt à leur victime afin de pouvoir voler une voiture munie d'un système anti-vol biométrique[25].

Peu de gens contestaient la fiabilité des systèmes biométriques ou bien les résultats publiés par l'industrie de la biométrie et ce sont trois journalistes allemands, Lisa Thalheim, Jan Krissler et Peter-Michael Ziegler qui l'ont fait. Ils ont testé plusieurs systèmes (iris, reconnaissance faciale, empreintes digitales) et en ont publié les résultats. Leur article, « Biometric Access Protection Devices and their Programs Put to the Test, Body Check », démontrait que les performances de ces systèmes étaient lamentables car ils sont excessivement faciles à déjouer, même avec des méthodes très simples. Ils ont expliqué les différents moyens de déjouer ces systèmes qui seront repris plus loin dans ce mémoire[26].

Dans la même lignée, le docteur Tsutomu Matsumoto a été le premier à déjouer un système biométrique. Avec de la gélatine à bonbon, il a moulé des empreintes digitales et 80% des lecteurs d'empreintes digitales ont été bernés.[27]

---

[24] Mann, Charles C., « Homeland Insecurity », *The Atlantic Monthly*, septembre 2002, p. 1.
[25] Kent, Jonathan, *Malaysia car thieves steal finger*, BBC News, Kuala Lumpur, [en ligne], http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm, (consulté le 15 février 2006).
[26] Thalheim, Lisa, Krissler, Jan, Ziegler, Peter-Michael, *Biometric Access Protection Devices and their Programs Put to the Test, Body Check*, [en ligne], http://www.heise.de/ct/english/02/11/114/, (consulté le 8 janvier 2006).
[27] Matsumoto, T., H. Matsumoto, K. Yamada, S. Hoshino, « Impact of Artificial Gummy Fingers on Fingerprint Systems », In *Proceedings of SPIE*, Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

Une dernière source digne de mention, et qui tend à inclure les trois thèmes développés précédemment, est la Commission de l'éthique de la science et de la technologie, mise sur pied par le gouvernement du Québec. Celle-ci a vraiment fait une énorme contribution à la recherche sur la biométrie en publiant deux rapports sur l'utilisation des données biométriques à des fins de sécurité. La commission est composée d'une trentaine de personnalités du monde universitaire provenant de différents secteurs. Son premier rapport[28] suggère des pistes d'enquête sur l'utilisation de la biométrie. Son deuxième rapport[29] propose des réflexions sur les questions posées par le premier rapport. La commission traite non seulement de la technologie en tant que telle, mais aussi de son application dans les mesures de sécurité, de son encadrement normatif et de l'éthique qui lui est liée.

C'était, en résumé, les grandes contributions aux thèmes biométriques et sécuritaires ainsi qu'aux autres dossiers qui y sont rattachés, notamment celui de la vie dans l'espace public et celui de la vie privée. Il va de soi que ce n'est qu'un bref résumé d'un vaste éventail de contributions très diversifiées et intéressantes.

Face à tous ces auteurs, il est du ressort de ce mémoire d'apporter une contribution au domaine. Car si le concept de vie privée a été bien développé, il existe encore des lacunes en ce qui concerne l'analyse du rapport entre cette dernière et la biométrie. La plupart des travaux sur le sujet consistent à des articles d'opinion ou des textes de quelques pages. Il n'y a

---

[28] Commission de l'éthique de la science et de la technologie, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques – Documents de Consultation*, [en ligne], http://www.ethique.gouv.qc.ca/fr/ftp/Biometrie-consultation.pdf, (consulté le 30 mars 2006).

[29] Commission de l'éthique de la science et de la technologie, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques – Documents de Réflexion*, [en ligne], http://www.ethique.gouv.qc.ca/fr/ftp/Biometrie-reflexion.pdf, (consulté le 30 mars 2006).

pas eu d'analyse appliquant systématiquement le concept de liberté à la biométrie. Ce mémoire aura donc pour objectif de contribuer sur ce sujet qui est de plus en plus d'actualité et qui nécessite de s'y attarder scientifiquement.

Pourquoi la biométrie ?

Les arguments pour la biométrie se résument en 2 catégories :

Praticité : Les mots de passe comme les cartes de crédit, les cartes de débit, les cartes d'identité ou encore les clés peuvent être oubliés, perdus, volés et copiés. En plus, aujourd'hui tous et chacun doivent se rappeler une multitude de mots de passe et avoir en leur possession un grand nombre de cartes. De son côté la biométrie serait immunisée contre ce genre de maux en plus qu'elle serait simple et pratique, car il n'y a plus ni cartes ni mots de passe à retenir[30].

Sécurité : La biométrie serait plus sécuritaire que les méthodes actuellement utilisées. Elle permettrait une identification précise et possible même sans papiers d'identification qui peuvent être contrefaits. Aussi, elle permettrait d'améliorer la sécurité des documents protégés biométriquement, donc de limiter la fraude. Ensuite, elle pourrait éviter la fraude dans de nombreux systèmes en évitant les dédoublements. Par exemple, un prestataire de l'assistance sociale ne pourrait pas recevoir plusieurs prestations sous différents noms[31]. La biométrie serait capable de réduire,

---

[30] GlobalSecurity.org, *Biometrics*, http://www.globalsecurity.org/security/systems/biometrics.htm, (consulté le 20 août 2007).
[31] European Commission - Directorate-General - Joint Research Centre, *Fact sheet on biometrics*,

sans l'éliminer, le crime et le terrorisme car, à tout de moins, elle complique la vie des criminels et des terroristes.

Le concept de contrôle de l'accès aux frontières personnelles

Toutes les théories sur la liberté individuelle et la démocratie libérale reconnaissent la nécessité de la vie privée pour l'épanouissement de l'individu[32]. Et certains prétendent même que la vie privée est un droit naturel, non créé, relevant de la dignité humaine[33]. En fait, comme l'affirment Benn et Gaus, la vie privée est primordiale dans la constitution d'une société, puisque c'est elle qui détermine le rapport que les gens entretiennent face aux institutions, aux gouvernements, au voisinage, envers la vie sociale, etc., car la confidentialité indique quelle est la limite de l'accès à l'Autre[34].

Ainsi, la vie privée est à la fois un concept qui invoque des normes sociales, du fait que cela suppose que des normes existent et qu'elles définissent ce qui est hors limite, et une notion qui dépend des normes sociales puisque nul ne peut parler de la vie privée sans faire référence aux normes sociétales[35]. Et il faut donc savoir quelle est la valeur normative de la vie privée. Par exemple, est-ce que ce sont les fonctions de la vie privée qui déterminent la valeur de celle-ci ou est-ce qu'elle a intrinsèquement une

---

http://www.jrc.ec.europa.eu/download/press/20050330_biometrics_fact_sheet.pdf, (consulté le 20 août 2007).

[32] McLean, *op. cit.*, pp. 56-57

[33] Neill, Elizabeth, *Rites of Privacy and the Privacy Trade : On the Limits of Protection for the Self*, McGill-Queen's University Press, 2001, pp. 14-16.

[34] Schoeman, Ferdinand David, « 1 : Privacy : philosophical dimensions of the literature », In Schoeman, Ferdinand. (sous la dir.), *loc. cit.*, p. 4.

[35] Benn, Stanley I., « 1 : Privacy, Freedom and Respect for Persons », In Pennock J. Roland et John W. Chapman (sous la dir.), *Privacy*, New York, Atherton press, inc., 1971, p.2.

valeur en soi[36] ? Ou encore, peut-être que la vie privée n'est qu'un simple dérivé d'autres droits, comme l'affirme Judith Jarvis dans une approche réductionniste[37].

Ce mémoire abordera ces questions en utilisant le concept de contrôle de l'accès aux frontières personnelles qui provient à la fois de Charles Fried (le contrôle informationnel qu'un individu a sur lui-même, les renseignements qu'il choisit de divulguer ou non) et de Sisela Bok (le contrôle sensoriel, l'accès et le non-accès physiques et mentaux aux organes sensoriels des autres ou des institutions[38]). Ce concept fait en sorte que la vie privée doit permettre aux gens de contrôler leurs frontières personnelles[39], c'est-à-dire ce qui touche à leur Être. Elle servira à analyser les conséquences de la biométrie sur la vie privée dans le troisième chapitre du mémoire. Mais d'abord, précisons les fonctions qui relèvent de cet accès qui sont doubles, soit le contrôle informationnel et le contrôle sensoriel.

La première fonction qui est celle du contrôle informationnel inclut évidemment, comme l'affirme Charles Fried, le contrôle de l'information que les gens ont ou non sur eux-mêmes[40]. Donc, le contrôle de l'accès et les codes sociaux qui y sont associés déterminent ce qui peut être révélé à propos de qui[41]. C'est pourquoi toute politique sur le respect de la vie privée doit insister sur les limites quant à l'obtention, l'utilisation, la protection, la distribution et l'entreposage sécuritaire des renseignements personnels,[42] car

---

[36] Rössler, Beate, « 1 : Privacies : An overview ». In Rössler, Beate, (sous la dir.), *Privacies : Philosophical evaluations*, Stanford University Press, 2004, pp. 9-11.
[37] *Ibid.* pp. 9-13.
[38] Rössler, loc. *cit.*, pp. 7-9.
[39] McLean, *op. cit.* p. 52.
[40] Rössler, *loc. cit.*, pp. 7-9.
[41] McLean, *op. cit.*, pp. 52-53.
[42] Tapscott, Don, et Ann Cavoukian, *Who knows : safeguarding your privacy in a networked world*, Random House of Canada, 1995, pp. 30-31.

les contraintes sur l'accès aux informations personnelles permettent non seulement d'empêcher les intrusions, mais surtout de rehausser l'acceptabilité sociale de ne pas être obligé de tout dévoiler. Cela permet aussi d'affirmer que de vouloir tout savoir sur quelqu'un est, en soi, une marque de non-respect. Comme l'écrit le Conseil de l'Europe en 1989 : le respect de la dignité humaine est intimement lié à la nécessité de ne pas être déshumanisé par des techniques statistiques de traitement des données[43]. Sur ce point, le concept d'intégrité contextuelle, qui veut dire que ce qui est publiquement disponible dans un lieu et à un moment donné ne peut pas être nécessairement obtenu de façon légitime dans un autre contexte, peut être utile[44]. Une partie de ce travail utilisera cette fonction du contrôle informationnel, c'est-à-dire le contrôle qu'un individu peut ou non exercer sur l'information que des organisations possèdent sur lui. Cette fonction servira donc à analyser la question des banques de données toujours plus présentes dans les sociétés contemporaines. Aussi, le risque de glissement vers une situation non initialement prévue (de l'anglais *creep function*) sera analysé avec cette fonction, car elle relève d'une perte sournoise du contrôle de l'information que les institutions ou les organisations détiennent sur les gens avec en exemple une étude de cas sur le numéro d'assurance sociale aux États-Unis. La question du terrorisme sera aussi abordée.

L'autre fonction, la sensorielle, c'est l'accès et le non-accès physiques et mentaux aux organes sensoriels des autres ou des institutions[45], comme Sisela Bok l'explique si bien lorsqu'elle affirme que la vie privée est la condition selon laquelle une personne est protégée de l'accès des autres.

---

[43] Borking, John, « 3 : The use and value of privacy-enhancing technologies », In Lace, Susanne, (sous la dir.), *The Glass Consumer : Life in a surveillance society*, Southampton, UK., The Policy Press (Bristol), 2005, pp. 69-71.
[44] Nissenbaum, *loc. cit.*, pp. 559-596.
[45] Rössler, *loc. cit.*, pp. 7-9.

Que celui-ci soit physique ou encore la protection contre l'attention des autres (regard), c'est le contrôle de l'accès qui est important[46]. Cela implique que le droit à la vie privée est la capacité qu'a quelqu'un d'empêcher les autres d'avoir accès à lui-même, de leur en priver[47]. Évidemment ce contrôle ne sera pas total du fait que, selon Ruth Gavison, seule une personne qui est complètement inaccessible jouit d'une vie privée totale[48]. Mais ce contrôle est fondamental pour la cohésion d'une société, puisque depuis toujours, il y a eu des codes, verbaux, physiques, locationnels, spatiaux, etc. pour imposer des limites aux accès. Que ce soit les vêtements qui créent une distance ou encore les portes, les manières, l'étiquette, ou, symbole de la vie privée, la salle de bain qui de tout temps a été considérée comme hors limite pour tous lorsque la porte est fermée. C'est important afin de réguler l'ouverture/ fermeture, l'accès / le non-accès[49].

Toujours pour la même fonction, ce contrôle de l'accès permet aussi à chacun de faire une nécessaire introspection pour évoluer. La solitude, donc un déni d'accès sensoriel à tous, est nécessaire aux processus mentaux de la pensée et l'individu ne peut se développer qu'en passant du temps avec lui-même pour, entre autres, apprendre, lire, faire le point sur sa vie[50]. Car en coupant sélectivement l'accès sensoriel que les gens ont les uns envers les autres, ils peuvent mieux maintenir une bonne santé mentale du fait qu'ils ont besoin d'une place où ils n'ont plus à maintenir les mêmes standards de respectabilité en ce sens que les codes sociaux sont plus relâchés dans la sphère privée que dans la sphère publique. Le meilleur exemple étant l'excellent documentaire de Jean-Claude Labrecque, *À hauteur d'homme*, où

---

[46] *Idem*.
[47] Reiman, *loc. cit.*, p. 199.
[48] Rössler, *loc. cit.*, pp. 7-9.
[49] McLean, *op. cit.*, pp 52-53.
[50] *Ibid.*, pp. 53-54.

il était montré le premier ministre d'alors, M. Bernard Landry, dans toute son intimité qui sacrait et frappait violemment du poing sur une table : un comportement inacceptable pour le titulaire de la fonction de premier ministre si ces paroles avaient été prononcées dans la sphère publique, mais pas pour le même homme dans sa sphère privée. Cela tient au fait que les rôles sociaux ne peuvent être maintenus indéfiniment et qu'il faut un endroit où il est possible de décompresser, la sphère privée. C'est important car les gens vont, face à la pression sociale et aux standards, soit rejeter ces standards et risquer la marginalisation, soit ils endurent et risquent la détresse psychologique ou encore ils rejettent les rôles sociaux dans leur sphère privée (l'homme qui est docteur dans la sphère publique doit avoir un comportement beaucoup plus exemplaire que lorsqu'il n'est plus qu'un homme ordinaire dans la sphère privée)[51]. Dans la même veine, les relations intimes et profondes sont exclusives puisqu'elles ne peuvent être partagées qu'avec un petit nombre[52] et sous certaines conditions environnementales (luminosité, gens aux alentours, etc.) et l'accès est par conséquent nécessaire à leur existence.

Cette deuxième fonction est celle du contrôle de l'accès sensoriel. Cette fonction est celle qui permet ou non d'avoir une sphère privée avec tout ce que cela implique et permet d'analyser d'autres thèmes qui seront abordés dans ce mémoire comme les aspects *Big Brother* et *Panopticon* qui caractérisent la biométrie.

Donc, ces deux fonctions du contrôle qu'un citoyen exerce face à l'accès que les autres ont à lui constituent la base même de la vie privée qui regroupe toutes les fonctions que celle-ci pourrait avoir. Avec ces fonctions

---

[51] *Idem.*
[52] Benn, *loc. cit.*, pp. 16-18.

de la vie privée, il est possible de traiter tous les aspects que ce mémoire entend traiter, que ce soit la problématique des bases de données, la criminalité, le terrorisme, le risque de glissement ou le panopticon. Puisqu'en utilisant les deux fonctions associées à la vie privée, il est possible d'analyser les conséquences de l'implantation des technologies biométrique sur la vie privée.

La vie privée étant ainsi définie et certains impacts sur la démocratie ayant été abordés, il est possible de comprendre l'importance de la problématique que pose la biométrie face à la démocratie. Ensuite, il faut savoir si la technologie peut procurer une sécurité qui rendrait acceptable de diminuer l'adhésion de la société aux principes et fonctions reliés à la vie privée. Car tout aussi importante et cruciale à la démocratie que peut être la vie privée, la sécurité de la population, par exemple le fait d'être libre de marcher dans les rues sans crainte d'être tué par des terroristes, ne peut être rejetée du revers de la main du fait que la sécurité est aussi un aspect important de la démocratie. Si cette technologie peut apporter la sécurité, surtout face aux attentats terroristes utilisant des armes de destruction massive comme des armes nucléaires, il serait difficile de ne pas être contraint d'accepter une certaine atteinte à la vie privée et peut-être même que l'introduction de la biométrie n'affectera pas substantiellement les libertés tout en apportant plus de sécurité. Dans le cas contraire, où la biométrie ne renforce pas substantiellement la sécurité, il n'y aurait aucune raison de diminuer d'un iota le droit à la vie privée.

Finalement, c'est un travail essentiellement normatif, autour d'une thématique qui oriente la réflexion sur le sujet de la vie privée, la sécurité et de la démocratie. C'est donc la question des droits de l'individu et du droit à la vie privée qui sous-tend ce travail.

Sphère privée et sphère publique

La sphère privée existe d'abord parce qu'elle est une norme sociétale où certains endroits sont considérés comme inaccessibles par tous sauf une infime minorité de gens. C'est un genre de sanctuaire où ne rentre pas qui veut. Pour que cette norme existe, il doit y avoir un nombre d'agents assez important ou un minimum d'agents d'une importance assez grande pour avoir une sphère privée étant donné que les sphères peuvent changer d'importance avec le temps[53].

Qu'est-ce qui est inclus dans cette sphère ? Du moment où il est reconnu que certaines choses appartiennent au citoyen en propre, il y a une sphère privée et des codes de politesse, d'étiquette, sociales ou autres normes sociales qui vont stipuler, implicitement, quels renseignements peuvent ou ne peuvent pas être demandés, quand et où une personne peut ou ne peut pas en aborder une autre, lui parler, la regarder ou interagir avec elle (par exemple, la salle de bain n'est pas accessible si la porte est fermée)[54].

La sphère privée inclut aussi certaines associations[55], par exemple ce qui se passe dans une réunion de bureau est privé en ce sens que seuls ceux qui y sont invités peuvent y prendre part et qu'il y a une attente que les discussions ne sortiront pas du bureau

Les sphères privées et publiques sont deux concepts contrastés qui, ensemble, englobent la totalité de la société et de ses phénomènes[56]. Malgré

---

[53] Weinstein, W. L.. « 2 : The Private and the Free : A Conceptual Inquiry » , In Pennock J. Roland et John W. Chapman (sous la dir.), *loc. cit.,* pp 27-28.
[54] *Ibid.*, pp. 29-30.
[55] *Ibid.*, pp. 32-33.
[56] *Ibid.*, p. 33.

le fait qu'il s'agisse de concepts contrastés, Hannah Arendt affirme que sans sphère privée, il n'y a pas de sphère publique, car plus quelqu'un en sait sur un individu, plus il devient unique et personnel, donc non public[57].

Aussi, les sphères privées comme publiques sont variables étant donné qu'elles sont basées sur des concepts normatifs et servent de fonctions dans les discours politiques et moraux. Si la sphère publique peut s'immiscer dans la sphère privée au nom du bien commun de la communauté (un crime, même dans une propriété privée, reste un crime), il est important de comprendre que la sphère privée dépasse le seul individu[58]. Les deux sphères se côtoient : par exemple, la vie personnelle (opinions, goûts, amitiés, état matrimonial, etc.) d'un citoyen relève exclusivement de sa sphère privée même lorsqu'il se trouve dans la sphère publique. Même ses amitiés de bureau ne relèvent pas, du moins en grande partie, de la sphère publique. Par contre, ses agissements au bureau sont en partie privés et en partie publics (par exemple, les rapports de performance d'un employé restent en général à l'intérieur de la compagnie, mais leurs contenus sont connus par plusieurs). Mais ses engagements politiques (manifestations, discours publics, etc.) sont totalement et exclusivement dans la sphère publique. Quelqu'un peut aussi décider de rendre public quelque chose relevant de la sphère privée.

Mais les gens agissent différemment s'ils sont observés ou croient l'être. Leurs paroles, leurs actions et même leur personnalité vont changer. C'est pour cela que la sphère privée existe[59]. En fait, les gens ne vont se confier qu'à leurs proches, formant un genre de société secrète selon Sidney

---

[57] Regan, Priscilla M.., *Legislating privacy : Technologie, Social Values, and Public Policy*, University of North Carolina Press, 1995, pp. 226-227.
[58] Weinstein, *loc. cit.*, p. 33.
[59] Benn, *loc. cit.*, p. 24.

M. Jourard et c'est pour cela que beaucoup d'institutions et de gouvernements découragent ces notions de vie privée qui les empêchent d'exercer un contrôle sur leurs citoyens et préfèrent donc l'ouverture à la fermeture[60]. Les totalitarismes ne peuvent concevoir qu'une action ou une parole ne puissent pas relever du domaine public, car la sphère publique englobe tout et c'est normal parce que l'État, étant le gestionnaire du bien commun, doit tout diriger[61].

Mais la sphère privée est une sphère de liberté : la liberté étant un principe fondamental, toute dérogation ou tout empiètement nécessite une justification. Il ne faut pas demander pourquoi tel droit existe mais bien pourquoi il n'existe pas, puisqu'il faut toujours justifier les limitations de liberté. Ainsi, il faut justifier les empiètements dans la sphère privée[62]. Du fait que l'individu doit, pour être libre, avoir le choix de ses actions, de ses associations et de ses prises de position entre autres, bien que ses actions puissent avoir des conséquences négatives. Il y a des limites qui font en sorte que certaines parties de la sphère privée peuvent devenir publiques, notamment la perpétration d'actes criminels[63].

Finalement, il est possible de résumer la sphère privée en citant Julie Inness : « Privacy is the state of the agent having control over a realm of intimacy, which contains her decisions about intimate access to herself (including intimate informational access) and her decisions about her own intimate actions »[64].

---

[60] McLean, *op. cit.*, pp. 53-54.
[61] Benn, *loc. cit.*, p. 22.
[62] Weinstein, *loc. cit.* p. 35.
[63] *Ibid.*, pp.35-39.
[64] Rössler, *loc. cit.*, pp. 7-9.

Degrés de vie privée

Il est possible de voir le degré de vie privée de deux façons. Premièrement, c'est la métaphore de l'onion. Le cœur de l'onion, c'est le corps des individus et donc faisant totalement partie de la sphère privée. La deuxième pelure, c'est la famille, puis les amis et les proches, le tout faisant partie de la sphère privée mais quand même moins privée que la première pelure. La troisième pelure, c'est la société. Le citoyen y conserve un aspect privé relativement à l'intervention étatique, mais cela fait aussi partie de la sphère publique car cela touche à la quatrième couche, qui est celle de l'État qui est la dernière et est celle qui est complètement publique[65].

L'autre façon, c'est celle de la dimension : même en public il est possible d'avoir une forte vie privée. Par exemple, les gens vont au cinéma en tant que citoyens privés dans un lieu public. C'est alors une sphère d'action et de responsabilité individuelle (*individual action and responsability*) qui suit les individus peu importe où ils sont et qui leur permet d'agir sans intrusion de la part des autres ou des institutions[66].

Cependant, il y a plusieurs degrés de vie privée. Par exemple, les personnages publics, que ce soit des politiciens, des juges ou des criminels (du fait qu'ils commettent un geste illégal à l'encontre de la société), abandonnent une part de leur droit à la vie privée. Mais même en privé il est possible de perdre un peu de vie privée. Par exemple, un homme et sa femme renoncent l'un envers l'autre à une bonne partie de leur vie privée du fait de leur vie commune[67]. Donc l'attente de vie privée dépend du statut de la

---

[65] *Ibid.*, pp. 6-7.
[66] *Idem.*
[67] Van Den Haag, Ernest. « 8 : On Privacy » , In Pennock J. Roland et John W. Chapman (sous la dir.), *loc. cit.* pp. 157-160.

personne (acteur, chanteur, politicien) et du lieu physique (dans la rue ou dans la maison)[68].

En résumé, la sphère privée est une norme sociétale qui permet aux gens d'avoir un genre de sanctuaire où ne rentre pas qui veut, un endroit qui est considéré hors limite pour tous les autres ou presque. Ces deux sphères, la privée et la publique, ont des frontières variables et s'immiscent l'une dans l'autre car elles sont normatives. La sphère privée peut être vue comme les pelures d'un onion où plus la pelure se rapproche du centre (le corps des gens), plus elle relève de la sphère privée et plus elle rapproche de la pelure externe (l'État), plus elle relève de la sphère publique. Ou encore, cela peut être une question de dimension où la sphère privée est une sphère d'action et de responsabilité individuelle qui accompagne chacun partout et qui en résulte que même en public il est possible de vivre sans ingérence d'autrui ou des institutions.

Plan du mémoire

Ce mémoire est divisé en trois chapitres. Les deux premiers sont essentiellement factuels et empiriques : le premier aborde l'histoire de la biométrie tandis que le deuxième présente son aspect technologique et sa fiabilité. Le troisième chapitre, normatif, est le cœur du mémoire, et analyse les conséquences de la biométrie sur la vie privée et donc sur la pratique de la démocratie libérale. Plus précisément, c'est dans ce chapitre que les deux fonctions explicitées dans le cadre analytique seront utilisées. Le contrôle informationnel sera surtout utilisé pour la première section sur les banques de

[68] *Idem.*

données de plus en plus omniprésentes ainsi que pour la quatrième et dernière section portant sur le risque de glissement du fait de son impact négatif et néfaste sur la capacité des gens de contrôler l'information sur eux-mêmes. Cette partie se terminera avec l'étude d'un cas concret, celui de l'expérience américaine de l'implantation du numéro d'assurance sociale. L'autre fonction, le contrôle sensoriel, sera surtout utilisée pour les deuxièmes et troisièmes parties de ce chapitre portant d'abord sur le Panopticon puis sur la lutte contre la criminalité et le terrorisme.

Chapitre 1 : Brève histoire de la biométrie

La biométrie a une longue histoire même si beaucoup ne le réalisent pas. Depuis des temps immémoriaux, l'Homme reconnaît ses semblables en scrutant leurs visages, leurs voix et leur morphologie. Mais ce n'est pas de ce processus naturel qu'il est question ici, mais bien de la technologie biométrique en tant que telle.

Mais même cette biométrie n'est pas nouvelle : les empreintes digitales, la seule forme de biométrie jusqu'au XX^{e} siècle, ont des origines très lointaines, comme en témoigne une fresque murale où des tribus de Nouvelle-Écosse qui y ont dessiné une main avec les empreintes de la paume et des doigts. Ou encore, dans la Babylone antique où les empreintes étaient utilisées pour régler des transactions ou même en Chine où des empreintes sur des sceaux en argile ont été trouvées[69]. Aussi, déjà au 14^{e} siècle les Chinois utilisaient les empreintes digitales et plantaires pour distinguer les jeunes enfants des marchands.[70] Mais les empreintes digitales semblent être tombées dans l'oubli pour plusieurs siècles, voire quelques millénaires.

Ce chapitre traitera en grande partie des empreintes digitales car c'est la technologie biométrique la plus ancienne et donc la mieux documentée. Il sera aussi question de l'utilisation institutionnelle de la biométrie qui ne date

---

[69] Guardware Systems Ltd., *Fingerprint Recognition II : History of Fingerprinting*, [en ligne], http://biometrie.online.fr/dossiers/technique/empreintes/History_of_Fingerprinting.pdf, p. 4, (consulté le 2 septembre 2006).

[70] National Center for State Courts - Court Technology Laboratory, Director of National Intelligence, *A brief history of biometrics*, [en ligne], http://ctl.ncsc.dni.us/biomet%20web/BMHistory.html, (consulté le 2 juin 2006).

que de la fin du 19e siècle (fin 1890) où les policiers parisiens (Alphonse Bertillon) ont commencé à utiliser les mesures des différentes parties du corps pour identifier les criminels. Mais cette méthode est tombée en désuétude lorsqu'il est devenu évident qu'elle n'était pas fiable. Et dès lors, les empreintes digitales ont été utilisées (technique développée par Richard Edward Henry de Scotland Yard). Ensuite, depuis quelques décennies, de nouvelles méthodes ont fait leur apparition et connaissent de plus en plus d'applications à mesure que les systèmes biométriques deviennent abordables[71].

L'histoire d'autres systèmes, plus récents, sera aussi abordée. Pour ce qui est des yeux, l'iris et la rétine sont deux systèmes assez connus bien que cette dernière, la lecture de la rétine, reste marginalement utilisée. L'histoire de la géométrie de la main, technologie très répandue, de la reconnaissance faciale, technologie de plus en plus médiatisée, de la lecture des veines de la main, technologie toute nouvelle, de la reconnaissance vocale, très connue à cause des films d'espionnage, de la reconnaissance par la signature, un peu moins connue, ainsi que celle de l'identification par l'ADN, qui connaît un essor exponentiel depuis quelques années, sera incluse dans ce chapitre. Les brèves histoires des systèmes expérimentaux comme la reconnaissance par l'odeur y seront aussi.

En résumé, c'est dans ce chapitre que seront abordés les grands moments de la biométrie, ces moments qui ont marqué son histoire et qui doivent être compris afin d'entrevoir son évolution.

---

[71] *Idem*

Bertillonnage

Malgré que sa technique ne soit plus en utilisation, Alphonse Bertillon est le premier à inventer un système avec le but avoué d'identifier scientifiquement des gens. Travaillant comme chef de l'identification criminelle à la police parisienne à la fin du XIX^{e} siècle, il a inventé un système qui identifie les criminels en mesurant les différentes parties du corps, leur morphologie et en notant les différentes marques d'un corps, que ce soit des cicatrices, des taches de naissance, etc.[72] Connaître l'identité des criminels est important afin d'empêcher les criminels récidivistes de donner un faux nom lorsqu'ils se font attraper et ainsi cacher leur passé criminel[73] pour obtenir la clémence des cours de justice. En 1884, seulement deux ans après sa mise en œuvre, le « Bertillonnage » avait déjà identifié 241 criminels récidivistes[74]. Son système va s'effondrer à cause d'un manque de rigueur taxinomique et ses lacunes en ce qui touche la qualité et la précision des données anthropomorphiques. Par exemple, certains « mesureurs » mesuraient avec plus ou moins de précision, certains ne mesuraient que certaines parties (car tout mesurer était long), d'autres encore utilisaient des termes subjectifs comme grands ou petits pour décrire certaines parties au lieu de mesures numériques. En plus, la plupart des mesureurs n'avaient pas la lourde formation requise. Dès l'arrivée des empreintes digitales, l'anthropométrie a dû laisser sa place[75]. Et c'est en 1903 que le système

---

[72] Dugelay, Jean-Luc, *Reconnaissance du visage*, [en ligne], http://dept-info.labri.u-bordeaux.fr/~maylis/pari-stic.labri.fr/TUTORIAL/tutorial_BIO_2_PARISTIC_05.pdf, p. 26, (consulté le 7 septembre 2006).

[73] Turner, Alexis, *The Death of Bertillonage*, [en ligne], http://oninformatics.com/?p=7 (consulté le 12 septembre 2006).

[74] Le Douarin, Nicole, *Allocution : Science et justice : Des empreintes digitales aux empreintes génétiques, à la recherche de la preuve indiscutable*, Institut de France, Académie des sciences, mardi le 23 novembre 2004, [en ligne], http://www.academie-sciences.fr/conferences/seances_solennelles/pdf/discours_Le_Douarin_23_11_04.pdf, p. 2, (consulté le 10 septembre 2006).

[75] Turner, *loc. cit.*

connaît son raté le plus spectaculaire et qui allait mettre fin à son utilisation lorsqu'un homme arrive au pénitencier de Leavenworth : son nom et sa photo sont à s'y méprendre identiques à ceux d'un autre criminel. En plus, sa fiche de *bertillonnage* est aussi la même (dans les normes qui tiennent compte des différences engendrées par les « mesureurs » de criminels). C'est lors de la prise d'empreintes digitales que les autorités se rendent compte de l'erreur : cet homme n'est pas le criminel récidiviste tel que décrit par la fiche de bertillonnage, et qui, lui, purgeait une autre peine dans une autre prison[76].

Mais l'histoire de la biométrie est surtout celle des empreintes digitales qui ont été utilisées pendant des millénaires tandis que les autres technologies ne sont vieilles que de quelques décennies au maximum.

Empreintes digitales et des paumes des mains

C'est en 1686 que le médecin italien Marcello Malpighi a été le premier occidental à remarquer certaines distinctions entre les empreintes digitales. Il a écrit un traité sur le sujet qui décrivait les trois motifs qu'il avait remarqués. Aujourd'hui une couche de l'épiderme porte son nom : la couche de Malpighi, du fait de sa contribution à ce sujet avec ses études sur la peau[77].

Puis, un physiologiste tchécoslovaque, Johannes Evangelista Purkinje (1787 – 1869), est le premier, en 1823, à avoir caractérisé les différences dans les empreintes digitales. Il les classe en 9 catégories de motifs. Il est donc le premier à avoir utilisé un système de classification pour les

---

[76] Sagem Morpho, Inc., *The History of Fingerprinting*, [en ligne], http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/biometria/Fingerprinting.htm, (consulté le 3 septembre 2006).

[77] Mauck, Melissa Jeanne, *Fingerprints: Are They Your Own?*, [en ligne], http://www.shsu.edu/~mth_jaj/math470/papers_s06/Melissa.pdf, p. 2 et 3, (consulté le 7 septembre 2006).

empreintes digitales bien qu'il n'ait jamais pensé l'utiliser à des fins d'identification[78].

Ensuite, William Herschel a commencé à utiliser les empreintes digitales dans ses fonctions de magistrat en chef du district de Hooghly aux Indes britanniques en 1858. Il demandait, pour conclure des contrats avec la population locale, que ceux-ci apposent l'empreinte de la paume de leur main (plus tard, l'empreinte de leurs index et majeur de la main droite) à l'arrière du contrat. Le but était de faire peur, car avec l'apposition de la main le contrat devenait plus « engageant » et l'idée de le répudier devenait moins probable qu'avec une simple signature. Il a utilisé cette méthode à grande échelle pour la première fois dans l'humanité et avec les années a accumulé une vaste collection d'empreintes digitales. Il s'est rendu compte que, non seulement les empreintes digitales étaient utiles pour exploiter les superstitions des populations coloniales, mais elles pouvaient aussi être utilisées pour identifier les gens, afin de prouver si quelqu'un est qui il prétend être. Il a aussi acquis la conviction de la permanence des empreintes digitales au cours de la vie d'une personne[79].

En 1877, il a imposé, sous sa propre autorité, les empreintes digitales comme moyens d'authentification auprès des autorités[80]. De 1877 à 1878, les pensionnaires de l'État (les prestataires d'assistance sociale de l'époque) devaient utiliser leurs empreintes digitales sur un document mensuel pour obtenir leur aide mensuelle[81]. Même principe pour les transactions aux

---

[78] Ashbaugh, David R., *Ridgeology : Modern evaluative friction ridge identification*, Forensic identification support section, Gendarmerie royale du Canada, [en ligne], http://onin.com/fp/ridgeology.pdf, pp. 8 et 12, (consulté le 30 août 2006).
[79] Guardware Systems Ltd., *loc. cit.*, p. 4.
[80] Beavan, Colin, *Fingerprints: The Origins of Crime Detection and the Murder Case That Launched Forensic Science*, 2001, p. 133.
[81] *Ibid.*, p. 45.

registres fonciers[82]. Et c'est lui qui a obligé les condamnés à fournir leurs empreintes digitales, bien que dans ce cas, c'était moins une question policière qu'une façon d'empêcher les criminels d'engager un substitut pour faire leur temps de prison à leur place[83]. Herschel écrit même un article dans *Nature* en 1880, *Skin Furrow of the Hand*, où il sanctionne l'utilisation des empreintes digitales comme méthode de signature et d'identification[84].

Puis il y a eu Francis Galton qui a réussi à obtenir plus de 8 000 ensembles d'empreintes digitales et c'est en les étudiant qu'il a pu établir les bases scientifiques qui servent à comparer deux empreintes digitales. Il aurait de plus démontré que, statistiquement, chaque empreinte était unique. Il a aussi publié un livre clé en matière d'empreintes digitales : *Fingerprints*[85].

C'est Galton, qui dresse le premier système de classification qui a par la suite été modifié par Edward Henry pour être utilisé pour l'identification des criminels. Il a aussi été un fervent militant qui croyait en l'infaillibilité des empreintes digitales aux fins d'identification et il a tout fait pour en convaincre la population[86].

Une autre figure importante est Edward Henry (1850-1931) qui était l'inspecteur général pour la province du Bengale aux Indes britanniques. Si, auparavant, les criminels avaient leurs sentences tatouées sur le front et, dans certains cas, leur nom avec la date de condamnation, les pressions provenant du public britannique face à ce genre de punitions révoltantes ont forcé l'Angleterre à changer le traitement de ces criminels, ce qui a culminé

---

[82] *Idem.*
[83] *Idem.*
[84] *Ibid.*, p. 74.
[85] Tredoux, Gavan, *Francis Galton and Fingerprints*, Archives de Francis Galton, [en ligne], http://galton.org/fingerprinter.html, (consulté le 4 septembre 2006).
[86] *Idem.*

avec la « *Criminal Tribes Act* » de 1871. Radicale, cette loi a criminalisé des tribus et des communautés entières et les a confinées, légalement, à certains endroits. Tous les individus de ces communautés devaient s'enregistrer auprès de la police, demander une permission à la police pour quitter leur communauté avec un trajet et un horaire précis ainsi qu'une liste de stations de police que le demandeur devait visiter sur son chemin. Toute infraction entraînait de graves punitions. Mais Henry s'inquiétait du fait que les communautés ne respectaient pas cette loi, car les gens n'utilisaient pas le nom que le registre de la police leur avait assigné. Ces « criminels professionnels », comme les qualifiait Henry, devaient être maîtrisés le plus rapidement possible. Au début, il a utilisé le bertillonnage, puis une combinaison de bertillonnage et d'empreintes du pouce. Après avoir consulté Francis Galton, il a décidé de donner la tâche à deux officiers (Azizul Haque et Chandra Bose) de régler la problématique du système de classification des empreintes digitales pour le rendre plus utilisable et d'en finir avec les énormes problèmes d'interprétation inhérents au système de Galton. Finalement, en 1897, le système de Henry est officiellement adopté par les Indes britanniques pour l'identification des criminels. Puis il a fait ses recommandations au comité du *Home Office* présidé par Henry Belper, comité qui a recommandé en 1900 l'utilisation des empreintes digitales en Grande-Bretagne[87]. Aussi, Henry publie un livre qui servira de référence au XX^{e} siècle : *The Classification and uses of Finger Printing*[88]. Ce système a permis aux empreintes digitales d'entrer dans l'ère moderne et a même été utilisé dans la 1re mouture de l'AFIS (*Automated Fingerprint Identification*

[87] Breckenridge, Keith, *Towards the theory of the Biometric State*, [en ligne], http://www.history.und.ac.za/Sempapers/Breckenridge2005.pdf, pp. 9 à 11, (consulté le 8 septembre 2006).
[88] *Idem.*

System), car jusqu'à tout récemment, il était encore largement utilisé et il l'est encore aujourd'hui bien que dans une moindre mesure[89].

Ensuite, il y a aussi eu Juan Vucetich (1858-1925) qui, travaillant au bureau d'identification et de statistiques de La Plata d'Argentine, a instauré la pratique de ficher toutes les personnes arrêtées avec leurs 10 empreintes digitales et leurs mesures anthropométriques, après avoir lu un article sur les travaux de Galton. Il a aussi inventé un système de classification et vu l'efficacité des empreintes digitales, Vucetich a ainsi pu se passer des mesures anthropométriques qui étaient inutiles selon lui. Son système de classification permettait de regrouper les fichiers d'empreintes par catégories, rendant leur consultation plus facile[90]. Encore aujourd'hui, son système est utilisé dans la plupart des pays hispanophones[91].

Les empreintes digitales ont eu de plus en plus la cote, mais c'est en 1975 que leur analyse a connu une petite révolution : le FBI finance le développement de capteurs permettant d'extraire les minuties (caractéristiques d'une empreinte digitale) d'une fiche d'empreintes digitales. Cependant, seules les minuties elles-mêmes étaient gardées, du fait que le coût d'entreposage numérique était prohibitif[92].

---

[89] International Biometric Group, *The Henry Classification System*, Research Consulting Integration, 2003, [en ligne], http://www.biometricgroup.com/Henry%20Fingerprint%20Classification.pdf, p. 3, (consulté le 5 septembre 2006).

[90] National institutes of health, *Visible proofs: Forensic Views of the Body: Biographies: Juan Vucetich (1858-1925)*, National library of medecine, [en ligne], http://www.nlm.nih.gov/visibleproofs/galleries/biographies/vucetich_image_3.html, (consulté le 7 septembre 2006).

[91] Guardware Systems Ltd., *loc.. cit.*, p. 6.

[92] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Fingerprint Recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Fingerprint%20Recognition.pdf, pp. 1-2, (consulté le 2 septembre 2006).

Plus tard, le NIST (*National Institute of Standards and Technology*) a développé l'algorithme M-40 qui permettait de soumettre une empreinte digitale à l'ordinateur et celui-ci choisissait toutes celles qui lui ressemblaient. Cela permettait de réduire considérablement le temps de recherche dans les banques de données et aussi permettait aux spécialistes des empreintes digitales de n'avoir qu'à travailler que sur une petite sélection d'empreintes digitales en écartant les millions d'empreintes qui n'étaient assurément pas celles qu'ils cherchent[93].

Mais c'est en 1994 que le FBI entreprend une contribution majeure à la reconnaissance des empreintes digitales. C'est le commencement de l'IAFIS (*Integrated Automated Fingerprint Identification System*) qui est basé sur trois aspects, d'abord l'acquisition d'une empreinte digitale, l'extraction de ses caractéristiques puis leur comparaison. C'est *Lockheed Martin* qui allait construire le système. Cependant, il faudra attendre cinq ans, soit en 1999, pour que les composantes majeures du IAFIS deviennent opérationnelles[94]. Dès lors, tous les systèmes d'empreintes digitales sont inter-opérationnels : le FBI peut chercher dans toutes les bases de données car elles sont compatibles. De plus, un réseau national d'empreintes digitales est développé et un service policier peut soumettre électroniquement des empreintes au FBI. Donc une empreinte latente trouvée sur une scène de crime à New York peut être comparée à une banque de données sur les criminels de Dallas dans un temps record. Non seulement l'IAFIS est utilisé pour les enquêtes criminelles, il est aussi utilisé pour les vérifications d'antécédents criminels lors d'embauches pour certains emplois. L'IAFIS procure ainsi une recherche automatisée des empreintes, entrepose des images électroniques de celles-ci et du criminel qui lui est associé (si le

---

[93] *Ibid.*, p. 2.
[94] *Idem.*

propriétaire de l'empreinte a été identifié bien sûr) et permet l'échange d'empreintes digitales[95].

La prochaine version de l'IAFIS va comprendre l'intégration des empreintes provenant des paumes de la main. Il y aura même un « National Palm Print Service » intégré. La raison de tout cela c'est qu'environ 30% des empreintes trouvées sur les lieux de crimes sont des empreintes de paumes, par exemple pour les manches des couteaux ou les volants de voitures.[96]

Géométrie de la main

La reconnaissance par géométrie de la main est un des systèmes biométriques commerciaux les plus anciens. C'est en effet en 1974 que le premier système est commercialisé. Ce système était conçu pour être polyvalent, et était fait pour contrôler l'accès à certains lieux, pour identifier les gens et finalement pour contrôler la présence et le temps passé par les employés au travail[97]. Mais c'est David Sidlauskas qui en 1985 développe plus en profondeur et brevète[98] ce concept technologique et c'est en 1986

---

[95] Federal Bureau of Investigation - CJIS Division, *Integrated Automated Fingerprint Identification System or IAFIS*, [En ligne], http://www.fbi.gov/hq/cjisd/iafis.htm, (consulté le 9 septembre 2006).

[96] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Palm Print Recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Palm%20Print%20Recognition.pdf, pp. 1-3, (consulté le 2 septembre 2006).

[97] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Biometrics History*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Biometrics%20History.pdf, (consulté le 15 septembre 2006).

[98] United States Patent and Trademark Office, *Patent 4,736,203: 3D hand profile identification apparatus*, 5 avril 1988, [en ligne], http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1=4,736,203.WKU.&OS=PN/4,736,203&RS=PN/4,736,203, (consulté le 15 septembre 2006).

que le 1er système biométrique à géométrie de la main brevetée est commercialement en vente[99].

Reconnaissance faciale

L'arrivée de la reconnaissance faciale comme outil biométrique est aussi assez récente. Elle a commencé dans les années 1960 où des techniciens devaient établir manuellement sur une photo les points clés (nez, bouche, mentons, etc.) et le système calculait ainsi par rapport à une référence commune les distances et les ratios entre les points. Ensuite, il restait à comparer les données obtenues avec celles gardées dans une banque de données faciales. Cependant, le caractère manuel de la technique implique donc la possibilité d'une forte dose d'erreurs humaines. Il faut attendre 1988 pour avoir une percée importante où L. Sirovich et M. Kirby ont appliqué une technique algébrique linéaire qui a montré que moins de cent données pouvaient être utilisées pour coder une image faciale normalisée. C'est la technique Eigenfaces. Trois ans plus tard, en 1991, M. Turk et A. Pentland ont trouvé qu'ils pouvaient détecter des visages dans une image en utilisant l'erreur résiduelle de la technique Eigenfaces. Cela va mener à la reconnaissance faciale automatique et en temps réel malgré les obstacles environnementaux (par exemple la luminosité et l'angle de vue) qui restaient importants[100].

---

[99] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Hand geometry*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Hand%20Geometry.pdf, (consulté le 2 septembre 2006).

[100] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Face recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Face%20Recognition.pdf, pp. 1 et 2, (consulté le 2 septembre 2006).

En 1993, le *Counterdrug Technology Development Program Office* du département de la défense des États-Unis, implante le programme FERET (FacE REcogniTion) qui durera cinq ans et engloutira plus de 6,5 millions de dollars. Ce programme avait trois objectifs : d'abord celui de financer les chercheurs en biométrie faciale, que ce soit en matière de théorie ou d'algorithmes, dont beaucoup sont encore utilisés aujourd'hui. Ensuite, FERET se voulait une importante banque de données faciales : aujourd'hui, elle contient 12 126 photos de visages de 1199 personnes et a été distribuée à plus de 100 groupes ne faisant pas partie du programme FERET. Finalement, FERET se voulait un évaluateur capable de tester les différents algorithmes (car tout le monde utilise la même banque de données)[101].

Aussi, c'est lors de son utilisation pendant le « *Superbowl* » de 2001 que la reconnaissance faciale a fait son entrée dans l'esprit du citoyen moyen. Chaque personne qui entrait au stade avait, à son insu et sans son consentement, son visage comparé à ceux compris dans une banque de données de criminels et de terroristes[102].

Iris

Pour l'iris, l'histoire commence en 1936 où l'ophtalmologiste Frank Burch décrit pour la première fois le concept d'iris comme moyen d'identification. Cependant, ce concept est resté sans suites jusqu'en 1985, où les ophtalmologistes Léonard Flom et Aran Safir ont affirmé que chaque iris était unique et pouvait ainsi servir à l'identification des individus. Deux

---

[101] Face Recognition Vendor Test (FRVT), *FacE REcognition Technology (FERET)*, [en ligne], http://www.frvt.org/FERET/default.htm, (consulté le 14 septembre 2006).

[102] Woodward, John D. Jr., *Super Bowl Surveillance : Facing Up to Biometrics*, RAND, Arroyo center, [en ligne], http://www.rand.org/pubs/issue_papers/2005/IP209.pdf, p. 3 (consulté le 10 septembre 2006).

années plus tard, en 1987, ils reçoivent un brevet pour ce concept. Le docteur John Daugman est contacté par le Dr Flom afin de trouver un algorithme de reconnaissance de l'iris. C'est en 1995 que les trois scientifiques de la *Defense Nuclear Agency* complètent et testent avec succès l'algorithme de reconnaissance automatique de l'iris et c'est la même année que le produit de ces recherches est commercialisé avec l'apparition sur le marché du premier lecteur d'iris. Et c'est le Dr Daugman qui possède le brevet. Le brevet de l'unicité de l'iris ayant expiré en 2005, d'autres compagnies vont donc entrer dans le marché pour cette technologie biométrique. Mais le brevet sur l'algorithme du Dr Daugman ne va expirer qu'en 2011[103].

Rétine

La biométrie rétinienne a commencé en 1935 où, dans un article du *New York State Journal of Medicine*, la question de l'identification par l'utilisation des vaisseaux sanguins sur la rétine était soulevée. Plus les recherches ont été poussées, plus la conclusion s'est avérée que chaque rétine serait unique et ne changerait pas au cours de la vie sauf par certains traumatismes ou maladies (surtout oculaires)[104].

Malgré tout, il faut attendre 1984 pour que la compagnie, nouvellement formée en 1976, EyeDentify développe le premier lecteur de rétine commercial (le Eyedentification 7,5). Cette compagnie reste la plus

---

[103] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Iris recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Iris%20Recognition.pdf, pp. 1-2, (consulté le 2 septembre 2006).

[104] Grgic, Marin, *Biometrics and Retina Scan Technology*, [en ligne], https://olt.qut.edu.au/it/itn584/gen/static/resources/01p-grgic.pdf, (consulté le 29 août 2006).

importante, sinon la seule, à produire ce type d'équipement biométrique[105]. Cependant, cette même compagnie a cessé sa production en 2001. Le pourquoi reste très spéculatif, mais une chose est sûre, la compagnie stagnait depuis longtemps[106].

Veines

L'histoire de la reconnaissance par les veines de la main n'en est pas vraiment une tellement cette technologie est récente. C'est le docteur K. Shimizu qui a commencé le tout en publiant un article sur l'imagerie trans-corporelle en 1992. Et c'est en 1996 que Yamamoto K et K. Shimizu font le suivi du premier article. Mais c'est en 2000 que l'aspect biométrique apparaît clairement avec une communication qui démontre comment ils ont inventé un système qui utilise les vaisseaux sanguins sous-cutanés du revers de la main aux fins d'identification d'un individu. La même année, le système est commercialisé[107].

Par la voix

Ensuite, si la biométrie par l'analyse de la voix est très populaire au cinéma, elle existe aussi dans la vraie vie. C'est en 1960 que le professeur suédois Gunnar Fant a pu, avec les rayons X, montrer la physionomie de la

---

[105] National Center for State Courts - Court Technology Laboratory, Director of National Intelligence, *Retinal scan*, [en ligne], http://ctl.ncsc.dni.us/biomet%20web/BMRetinal.html, (consulté le 28 septembre 2006).

[106] Chopra, Prianka, *The EyeDentify Metamorphosis*, Frost & Sullivan Market Insight, 1er août 2001, [en ligne], http://www.frost.com/prod/servlet/market-insight-top.pag?docid=RKUR-4ZMW3G, (consulté le 14 septembre 2006).

[107] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Vascular pattern recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Vascular%20Pattern%20Recognition.pdf, pp. 1 et 2, (consulté le 3 septembre 2006).

production des sons et de la voix. Le Dr Joseph Perkell qui a aussi utilisé les rayons X a bâti sur le modèle de Fant en y incluant aussi la langue et la mâchoire. Au début, des filtres analogues permettaient, la plupart du temps et avec l'aide d'humains, la reconnaissance de la voix. L'entreprise *Texas Instruments* a inventé un prototype pour l'armée de l'air des États-Unis, en 1976. Dans les années 1980, le NIST a sérieusement entrepris de développer un système de reconnaissance vocale avec son « Speech group » et depuis 1996 ce groupe tient des évaluations annuelles et reçoit un financement de la NSA (*National Security Agency*)[108].

Par la signature

La reconnaissance scientifique par la signature a véritablement commencé en 1965 et pendant les années 1970, mais s'est surtout concentrée sur les caractéristiques géométriques et statiques d'une signature : sa forme physique. C'est l'apparition de technologies sensibles au touché qui a permis de passer de ce que la signature a l'air vers comment la signature a été faite, c'est-à-dire les éléments dynamiques d'une signature (pression du crayon, vitesse et autres caractéristiques). Et c'est finalement en 1977 qu'un premier brevet est accordé pour la reconnaissance par signature avec caractéristiques dynamiques[109]. Les systèmes subséquents ont continué d'évoluer, mais moins radicalement.

---

[108] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Speaker Recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Speaker%20Recognition.pdf, p. 1, (consulté le 10 septembre 2006).

[109] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Dynamic Signature*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/dynamic%20signature.pdf, p. 1, (consulté le 12 septembre 2006).

L'ADN

L'ADN (acide désoxyribonucléique) est étudié depuis plus d'un siècle, que ce soit à travers la théorie de l'évolution de Charles Darwin (1859) ou encore le concept d'hérédité de Gregor Mendel (1866). Mais c'est seulement récemment que l'ADN a été conceptualisé et instrumentalisé aux fins d'identification[110]. Après la publication, en 1953, d'un article de James Watson et Francis Crick sur la structure de l'ADN, il faut attendre 1980 pour que des généticiens trouve une région de l'ADN qui varie beaucoup entre les individus mais sans contenir d'information génétique. Ensuite, c'est Alec Jeffreys qui est le premier à trouver un moyen d'identifier les gens avec leur ADN, c'est la méthode de « Restriction Fragment Length Polymorphism » (RFLP) qu'il découvre en 1984 et la police britannique utilise le profilage par ADN un an plus tard. Et c'est en 1986 que le fameux procédé d'amplification en chaîne par polymérase (*Polymerase Chain Reaction* [PCR]) est inventé par Kary Mullis. Cette découverte permet de multiplier une région de l'ADN, ce qui rend son analyse incommensurablement plus facile. C'est en 1987 que la police britannique a réussi à véritablement introduire l'ADN dans le système judiciaire. D'abord en innocentant un jeune homme de 17 ans et, en faisant des prélèvements de masse semi-volontaires (si quelqu'un ne donne pas son ADN, il devient un suspect) sur 5000 hommes, de trouver le coupable d'un double viol-meurtre. Aussi, aux États-Unis, Gary Doston a réussi à prouver qu'il avait été faussement condamné en utilisant l'ADN. Cela

---

[110] The national health museum – access excellence, *History if genetics timeline*, [en ligne], http://www.accessexcellence.org/AE/AEPC/WWC/1994/geneticstln.html, (consulté le 9 septembre 2006).

lui a permis d'être libéré après avoir purgé huit ans d'une peine pour viol de 25 à 50 ans[111].

Et c'est en 1995 et en Grande-Bretagne que la première banque d'ADN au monde est créée et commence à recueillir des échantillons d'ADN. Les États-Unis vont suivre en 1998 avec le *National DNA Index System* du FBI qui permet à tous les corps de police de comparer électroniquement des profils génétiques. Au tournant du millénaire, en 2000, la banque d'ADN de la Grande-Bretagne compte un million de profils génétiques[112]. Par contre, l'analyse de l'ADN est trop lente à donner des résultats pour être utilisée comme moyen d'identification et d'authentification en temps réel.

Systèmes expérimentaux

Les systèmes expérimentaux sont ces systèmes dont les preuves restent à faire pour même être considérés comme des technologies biométriques sérieuses. D'abord, pour la démarche, il y a eu H. K. Ramakrishnan et M. P. Kadaba qui ont significativement contribué à l'analyse de la démarche d'une personne[113]. Ensuite, H. Lakany et G. Hayes sont sans doute les premiers à avoir réalisé un algorithme pour cette technologie biométrique[114]. Cependant, les piètres performances[115] et la nouveauté de cette technologie la rendent plutôt marginale. Aussi d'autres sont encore plus

---

[111] CrimTrac Agency - Commonwealth of Australia, *Key Dates in the History of DNA Profiling*, [en ligne], http://www.crimtrac.gov.au/dnahistory.htm, (consulté le 14 septembre 2006).
[112] *Idem*.
[113] Ramakrishnan, H. K. et M. P. Kadaba, « On the Estimation of Joint Kinematics During Gait », *J. Biomechanics*, 1991, 24 (10): pp. 969 – 977.
[114] Lakany, H. et G. Hayes, « An Algorithm for Recognising Walkers », In *Audio- and Video-based Biometric Person Authentication*, The International Association for Pattern Recognition, 1997, pp. 112 à 118.
[115] Boyd, Jeffrey E. et James J. Little, *Biometric Gait Recognition*, Universités de Calgary et de Colombie-Britannique : département des sciences informatiques, [en ligne], http://pages.cpsc.ucalgary.ca/~boyd/papers/biometric-summerschool.pdf, (consulté le 4 septembre 2006).

exotiques, comme la biométrie par odeur qui est encore très expérimentale et n'a pas encore véritablement d'« histoire »[116].

Comme cela a été démontré, les technologies biométriques ont une histoire plutôt récente si les empreintes digitales sont exclues, elles qui ont une histoire plusieurs fois centenaires. Mais une chose est sûre, elles continuent d'évoluer et les scientifiques de cette discipline ne cessent de trouver des nouvelles idées pour mesurer (*métrie*) les caractéristiques physiques (bio). Il y a à peine un siècle, la biométrie se limitait aux empreintes digitales, aujourd'hui, la biométrie comprend une dizaine de technologies et une demi-douzaine de technologies encore expérimentales. Alors, le secteur biométrique continuera probablement pour plusieurs décennies sa croissance et les systèmes biométriques pourraient être de plus en plus présents. Mais pour répondre à la problématique, il faut savoir si ces technologies fonctionnent comme elles le devraient et c'est ce thème qui sera abordé dans le prochain chapitre.

---

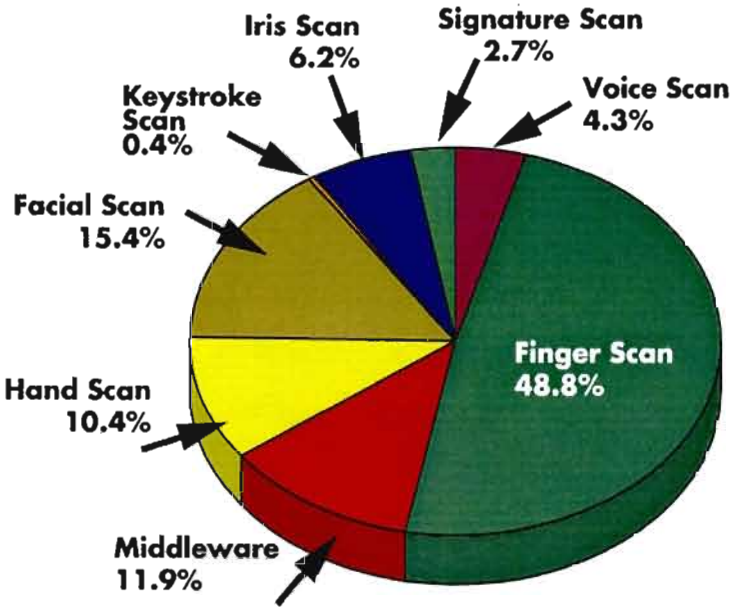
[116] Korotkaya, Zhanna, *Biometric Person Authentication: Odor*, Lappeenranta University of Technology : Department of Information Technology : Laboratory of Applied Mathematics, [en ligne], http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf, (consulté le 14 septembre 2006).

Chapitre 2 : Les diverses technologies biométriques modernes

C'est dans ce chapitre que la biométrie en tant que technologie sera abordée. Puisqu'avant de discourir davantage sur la biométrie et d'en caractériser les impacts qu'elle peut avoir sur la démocratie et la vie privée, il faut montrer ce qu'est la biométrie en tant que telle, c'est-à-dire le fonctionnement de ces technologies, puis leur fiabilité. Celles-ci peuvent être regroupées selon ce qu'elles analysent : la main (empreintes digitales, géométrie de la main et analyse des veines), le visage (reconnaissance faciale, analyse de l'iris et de la rétine), la bio-dynamique (analyse de la voix, analyse de la signature), l'ADN qui a sa propre catégorie à lui seul et les caractéristiques imposées/implantées (par exemple le (malheureusement ?) célèbre VERIchip qui est une puce implantée sous peau servant à l'identification par émission d'onde radio à très courte portée), mais qui ne seront pas abordées dans ce travail[117]. Finalement, il sera question de la fiabilité des différentes technologies biométriques, car il est essentiel de savoir si elles fonctionnent ou non pour répondre à la problématique qui consistait à savoir si l'implantation de la biométrie en vaut la peine.

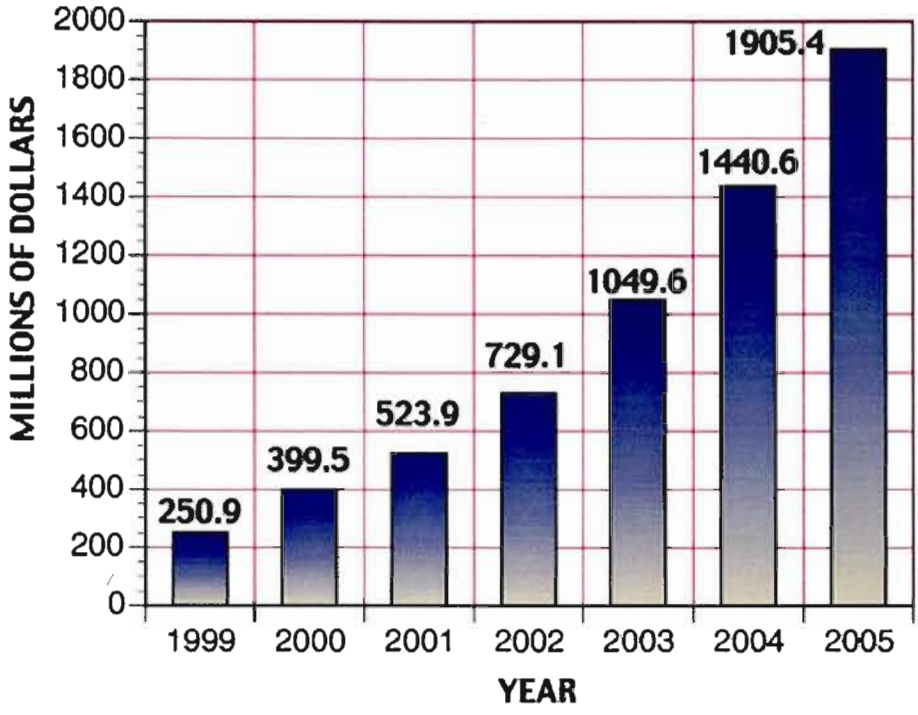
---

[117] Clarke, Roger, *Biometrics and Privacy*, Xamax Consultancy Pty Ltd, Canberra, Department of Computer Science, Australian National University, Notes du 15 avril 2001, [en ligne], http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html, (consulté le 3 juin 2006).



Graphique 1A : Parts des marchés mondiaux en 2001[118]

[118] International Biometric Group, New York, NY; 1.212.809.9491



Graphique 1B : Revenus totaux et mondiaux provenant de la vente de technologies biométriques de 1999 à 2005[119]

[119] International Biometric Group, New York, NY; 1.212.809.9491

Tableau synthèse sur les données biométriques

Biométrie[37]	Robustesse[38]	Unicité[39]	Fiabilité[40]	Potentiel[41]	Acceptabilité[42]	Coût	Applications
Empreintes digitales	Moyenne-Haute	Haute	Très haute	Haut	Basse-Moyenne	Très faible-Moyen	Voyageur, permis de conduire, services sociaux
Géométrie de la main	Moyenne-Haute	Haute	Haute	Moyen-Haut	Moyenne-Haute	Moyen	Contrôles d'accès, voyageurs, « day care »
Géométrie des doigts	Moyenne-Haute	nd	Moyenne-Haute	nd	Moyenne-Haute	Moyen	Contrôles d'accès, détenteurs de billets dans les parcs d'amusement
Reconnaissance faciale	Moyenne	Haute	Basse	Moyen	Haute	Moyen	Casinos, voyageurs
Iris	Haute	Très haute	Haute	Haut-Très haut	Moyenne-Haute	Très élevé	Prisons, contrôles d'accès, voyageurs
Rétine	Haute	Très haute	Haute	nd	Basse	Élevé	Contrôles d'accès, voyageurs
Signature	Basse-Moyenne	Moyenne	Basse	Bas-Moyen	Moyenne-Haute	Faible	Applications à faible niveau de sécurité, applications comportant déjà une signature
Voix	Moyenne	Moyenne-Haute	Moyenne-Haute	Moyen-Haut	Haute	Faible	Applications à faible niveau de sécurité, authentification téléphonique
Odeur	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu	nd	nd	nd
Oreille	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu	nd	nd	nd
Imagerie thermique	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu	nd	nd	nd
Frappe sur clavier	Niveau inconnu	Niveau inconnu	Bas	Niveau inconnu	nd	nd	nd

Sources : Office parlementaire d'évaluation des choix scientifiques et technologiques (France)[43] et OCDE[44]

Tableau 1 : Tableau synthèse sur les données biométriques[120]

[120] Commission de l'éthique de la science et de la technologie, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques – Documents*

ADN

Bien que vraiment récente, l'analyse par ADN ou empreinte génétique a été très médiatisée. Son principe est simple : même si plus de 99% du bagage génétique des êtres humains est identique et donc inutile pour n'importe quelle forme d'identification ou d'authentification, il reste que 0,1% des nucléotides contiennent des variations connues sous le nom de polymorphisme. Ce sont ces variations que les différentes méthodes analysent[121]. Ce polymorphisme plus scientifiquement appelé *Number of Tandem Repeats loci* (VNTRs)[122].

L'analyse par PCR est la base de toutes les autres technologies utilisées aujourd'hui. Elle vise l'amplification de certaines régions de l'ADN qui sont connues pour leur haut taux de polymorphisme[123]. Contrairement à la RFLP (*Restriction Fragment Length Polymorphism*) qui précédait la PCR, cette dernière n'a plus besoin d'une grande quantité de sang (taille qui était de la grosseur d'un 25 sous) pour faire cette analyse et est plus efficace[124].

---

de Réflexion, p. 10, [en ligne], http://www.ethique.gouv.qc.ca/fr/ftp/Biometrie-reflexion.pdf, (consulté le 30 mars 2006).

[121] The Academy for the Advancement of Science and Technology, *DNA Fingerprinting*, [en ligne], http://www.bergen.org/AAST/Projects/Gel/fingprint1.htm, (consulté le 15 janvier 2007).

[122] Rascati, Ralph J., *An Overview of Forensic DNA Typing Systems*, Kennesaw State University, [en ligne], http://science.kennesaw.edu/~rrascati/forensicpolymorphs.html, (consulté le 13 janvier 2007).

[123] *Idem.*

[124] Human Genome Project (HGP), *DNA Forensics*, [en ligne], http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml, (consulté le 14 janvier 2007).

Mais la technologie la plus répandue aujourd'hui est la STR *(short tandem repeats*) qui analyse des régions à très haut degré de polymorphisme mais avec de petites séquences d'ADN qui sont répétées[125].

Chaque VNTRs n'est pas unique, loin de là : en fait, chaque VNTRs sera présent chez 1 à 10 % de la population. C'est pourquoi il faut en tester plusieurs (le système CODIS aux États-Unis en teste treize) afin de s'assurer d'avoir une combinaison qui ne se retrouvera pas chez personne d'autre. Étant donné que chaque VNTRs est indépendant des autres, il suffit de multiplier toutes les fréquences pour obtenir la possibilité que quelqu'un ait le même profil génétique : un chiffre qui est souvent précédé de 15 zéros[126].

Mais il faut faire attention avec l'ADN en ce qui concerne la criminalité. Car il peut y avoir contamination de la scène de crime ou du prélèvement par une autre source d'ADN (par exemple un technicien qui ne porterait pas de gants). Et même si l'ADN correspond, ce n'est en aucun cas une preuve de culpabilité, au mieux cela veut dire qu'à un moment donné (avant ou pendant ou après le crime en question) ce suspect se trouvait sur le lieu où le crime a été commis, et au pire, que le suspect a été en contact avec une personne qui, elle, s'est trouvée à un moment donné sur le lieu où le crime s'est finalement produit.

Il y a aussi le risque de fabrication de preuve comme l'a montré le docteur John Schneeberger qui, en 1992, avait violé certaines de ses

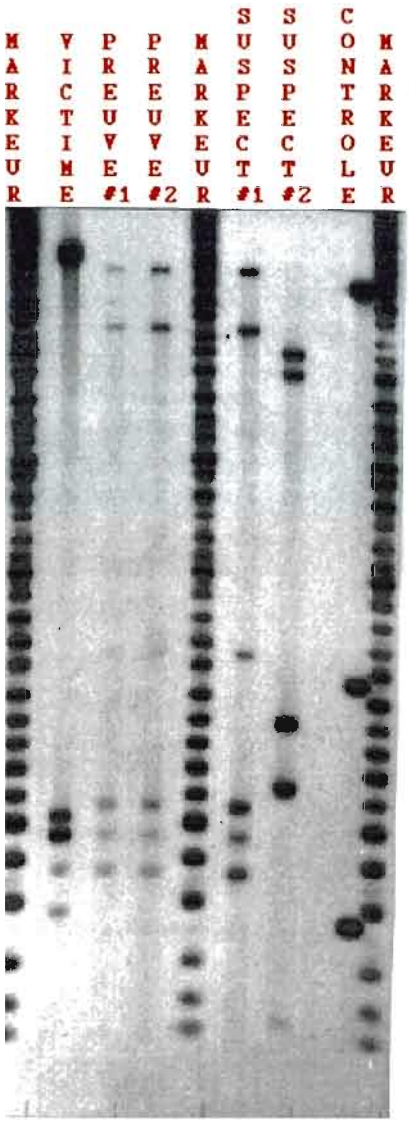
---

[125] The Biology Project, *What is a Short Tandem Repeat Polymorphism (STR)?,* Université d'Arizona, [en ligne], http://www.biology.arizona.edu/Human_Bio/activities/blackett2/str_description.html, (consulté le 11 janvier 2007).

[126] The Biology Project, *What are the 13 core CODIS loci?*, Université d'Arizona, États-Unis, [en ligne], http://www.biology.arizona.edu/Human_Bio/activities/blackett2/str_codis.html, (consulté le 11 janvier 2007).

patientes, dont au moins une qui était sous sédation. Lorsque les policiers ont voulu tester son ADN, il a inséré un tube en plastique rempli de sang dans son bras, sous la peau, et il s'est arrangé pour que le prélèvement sanguin se fasse dans le tube qui passait donc pour une veine. Il a ainsi déjoué les policiers à 3 reprises.[127] D'ailleurs, un film a été fait à ce sujet, *I accuse*[128].

[127] CBC News, *Sask. doctor sentenced for rape*, 10 novembre 2000, [en ligne], http://www.cbc.ca/story/news/?/news/1999/11/26/saskdr991126, (consulté le 14 janvier 2007).
[128] DeJong, Matthew, Matt De Jong, Charles Wilkinson et John Ketcham, *I Accuse*, 2003.



Légende

Preuve 1 : ADN du sperme retrouvé sur les vêtements de la victime du viol

Preuve 2 : ADN du sperme retrouvé suite à un prélèvement vaginal de la victime du viol

Victime : ADN de la victime, car il faut pouvoir distinguer les différents ADN trouvés sur le lieu du crime

Suspect : ADN des deux suspects

Controle : les résultats de fragments d'ADN d'une personne déjà testée

Markeurs . Un ensemble de fragments d'ADN de longueurs connues qui permet de servir de règle à mesurer pour les autres fragments

Photo 1 : Autoradiographie d'ADN[129]

[129] Kimball, John W., *Restriction Fragment Length Polymorphisms (RFLPs)*, [en ligne], http://users.rcn.com/jkimball.ma.ultranet/BiologyPages/R/RFLPs.html, (consulté le 17 janvier 2007).

Main (empreintes digitales, géométrie de la main et analyse des veines)

L'analyse de la main est très utilisée en biométrie pour des raisons évidentes : elle est le principal lien avec le monde physique qui entoure l'homme (prendre des choses, appuyer sur des touches, ouvrir et fermer des portes) et laisse sa trace un peu partout (ce qui a amené la police scientifique à développer les techniques concernant les empreintes digitales), elle n'est pas de nature privée comme l'ADN. C'est donc une des technologies les plus développées.

Empreintes digitales et des paumes

Les empreintes digitales sont une série de lignes, de vallées (en blanc), de pointes (représentées en noires) qui forment des motifs. Les empreintes digitales sont analysées en utilisant leurs minuties qui sont la localisation, la direction et les bifurcations des motifs des empreintes digitales[130].

[130] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Fingerprint Recognition*, *loc. cit.*, pp. 2 et 3.

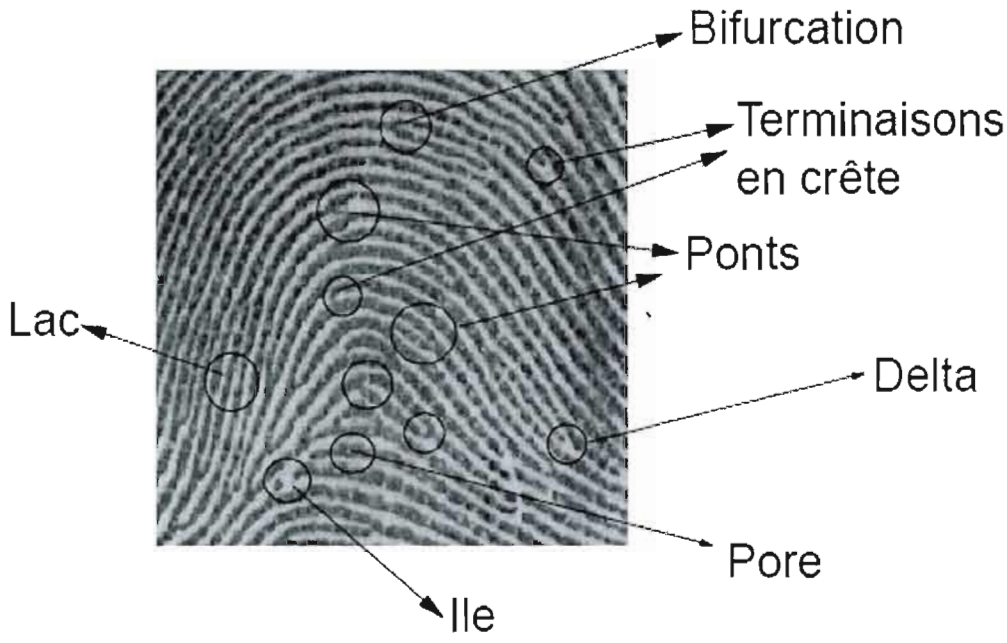


Schéma 1 : Caractéristiques des minuties[131]

En plus des services policiers et de l'IAFIS (*Integrated Automated Fingerprint Identification System*) du FBI, l'utilisation la plus récemment médiatisée de l'utilisation de la biométrie des empreintes digitales est celle du programme US-VISIT où chaque visiteur (avec des exceptions pour les Canadiens et les Mexicains) doit fournir ses empreintes digitales qui seront vérifiées à son entrée et à sa sortie des États-Unis[132].

---

[131] Club de la Sécurité des Systèmes d'Information Régional, *Gestion des identités : Biométrie – RFID – Moyens d'authentification – contrôles d'accès au SI – gestion des droits*, [en ligne], www.clusir-rha.fr/download.php?id=106, (consulté le 7 mai 2007).

[132] Department of homeland security, *US-VISIT Program*, [en ligne], http://www.dhs.gov/dhspublic/interapp/content_multi_image/content_multi_image_0006.xml, (consulté le 30 septembre 2006).

Géométrie de la main

Simple, en prenant une photo de la silhouette d'une main sur un guide, cette technologie mesure la longueur, la largeur, l'épaisseur, la surface de la main, etc. En fait, cette technologie prend deux photos, une du dessus de la main, l'autre du côté de la main en utilisant un miroir à angle. En tout, il y a 31 000 points qui sont analysés et le système prend 90 mesures (par exemple la distance entre les noues des doigts). Le tout est comparé avec un échantillon fourni par l'utilisateur antérieurement[133].

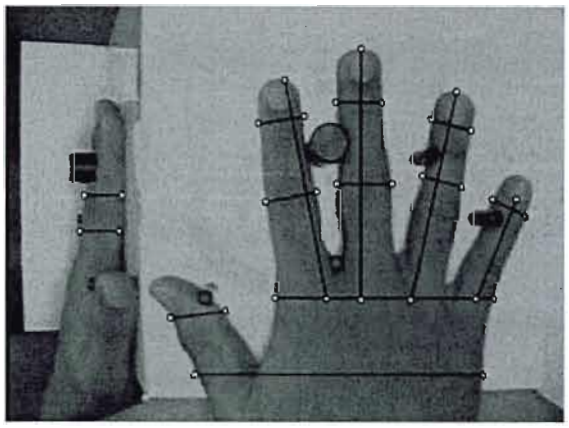


Photo 2 : Géométrie de la main[134]

La géométrie de la main est une technologie très utilisée. Par exemple, Hydro-Québec l'utilise pour quiconque veut accéder à sa centrale nucléaire Gentilly-2. C'est aussi la norme pour les centrales nucléaires aux États-Unis[135].

---

[133] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Hand geometry*, *loc. cit.*, pp. 1 et 2.

[134] *Idem.*

[135] Avery, Keith, *Utilizing Technology*, [en ligne], http://www.stevenspublishing.com/Stevens/SecProdPub.nsf/frame?open&redirect=http://www.stevenspublishing.com/stevens/secprodpub.nsf/d3d5b4f938b22b6e8625670c006dbc58/2a9e1688dd432ca88625711f0062b8c7?OpenDocument, (consulté le 22 septembre 2006).

Veines

La biométrie par la reconnaissance des veines fonctionne assez simplement. Des diodes émettent une lumière proche de l'infrarouge (IR) qui pénètre soit le revers de la main ou les doigts (ce sont les deux endroits les plus couramment utilisés pour la reconnaissance par les veines). Cette lumière est absorbée par les tissus de la peau et les vaisseaux sanguins : certains tissus vont en absorber plus que d'autres et certains tissus vont refléter la lumière IR plus que d'autres. Pour la reconnaissance par les veines du revers de la main, c'est la lumière réfléchie qui est captée par les capteurs tandis que pour les doigts, c'est la lumière absorbée qui l'est (les tissus qui absorbent cette lumière apparaîtront comme noirs). L'image résultante est numérisée et traitée pour en extraire le motif des veines, mais aussi leurs épaisseurs, leurs branchements, leurs interconnexions et autres caractéristiques pertinentes.[136]

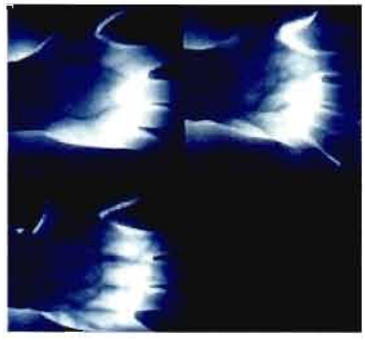


Photo 3 : Veines de la main[137]

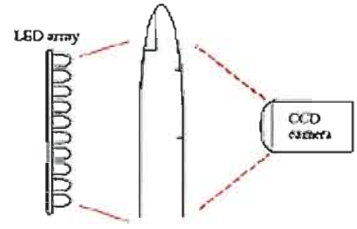


Schéma 2 : Veines du doigt[138]

La seule utilisation connue de cette technologie est par les banques japonaises qui offrent à leurs clients la possibilité d'avoir une carte de guichet

---

[136] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Vascular pattern recognition*, *loc. cit.*, p. 2.
[137] *Idem*.
[138] *Idem*.

bancaire qui utilise la reconnaissance par les veines. Récemment, il y a eu des tentatives pour rendre compatibles les deux technologies (car certains guichets utilisent les veines des mains et d'autres utilisent les veines du doigt)[139].

Visage (reconnaissance faciale, analyse de l'iris et de la rétine)

Les technologies biométriques qui se concentrent sur le visage sont plus récentes, mais ce sont celles qui connaissent l'essor le plus grand.

Visage

La reconnaissance faciale est divisée en deux grandes catégories : les *géométriques* qui se basent sur les caractéristiques du visage et les *photométriques* qui sont basées sur la vue. De ces catégories, trois algorithmes sont dominants, soit l'analyse en composantes principales (*Principal Components Analysis* [PCA]), l'analyse linéaire discriminante (*Linear Discriminant Analysis* [LDA]), et finalement, le troisième algorithme est le *Elastic Bunch Graph Matching* (EBGM)[140]. Avec la PCA, les images captées et les images sources sont d'abord normalisées afin qu'elles soient de mêmes grosseurs et que les principales caractéristiques du visage (yeux et bouche) soient alignées. Cette technique permet de défaire la structure du visage en composantes orthogonales (*eigenfaces*) et lorsqu'un visage est soumis à cette technique, chacun de ses vecteurs caractéristiques sera comparé aux vecteurs caractéristiques des autres visages en mesurant la

---

[139] AFX News Limited, *Mizuho, SMBC to share finger-vein biometric ATMs with Japan Post – report*, [en ligne], http://www.forbes.com/business/feeds/afx/2006/08/20/afx2960839.html, (consulté le 25 septembre 2006).

[140] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Face recognition*, *loc. cit.*, p. 2.

distance entre ces vecteurs pour trouver le bon visage. Cette technique est surtout utile pour réduire la taille des données utilisées[141].

L'autre technique, l'analyse linéaire discriminante (LDA), est une analyse statistique pour classer les échantillons de classes inconnues en s'appuyant sur des classes connues disponibles. Dans cette analyse, chaque classe est la plus dissemblable possible des autres, mais avec le moins de différences possible à l'intérieur de la classe en elle-même.[142].

La dernière méthode, la EBGM, est basée sur le fait que les visages ont beaucoup d'aspects non linéaires. Par exemple, la luminosité pose un grand problème pour les approches linéaires, car la lumière n'éclaire pas un visage homogénéiquement. Aussi, il y a la position du visage et les expressions faciales qui changent de beaucoup le visage. L'ondelette de Gabor (*Gabor wavelet*) projette sur le visage une toile élastique qui permet de voir celui-ci en trois dimensions. En fait, cette méthode se rapproche beaucoup de la façon dont le cortex visuel des mammifères supérieurs agit pour identifier un visage[143].

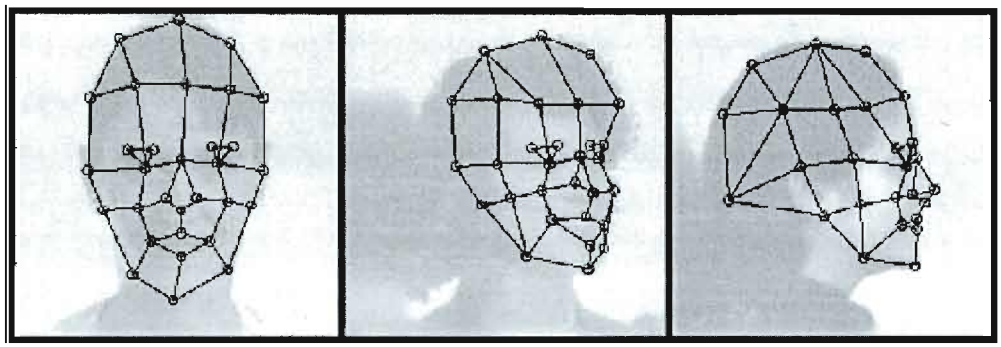


Schéma 3 : Ondelette de Gabor[144]

---

[141] *Idem.*
[142] *Ibid.*, p. 3.
[143] *Ibid.*, p. 4.
[144] *Idem.*

Les casinos sont probablement les plus grands utilisateurs de reconnaissance faciale afin de repérer les tricheurs ou les compteurs de cartes. C'était une évolution naturelle dans un milieu comme les casinos qui comptent énormément de caméras (le *Sands Hotel* d'Atlantic City au New Jersey en a plus de 1000) et ont les moyens et les intérêts financiers pour le faire[145].

Iris

Pour la technologie de la biométrie pour l'iris, il faut d'abord trouver l'iris en utilisant des points de repère. L'iris est ensuite éclairé avec une lumière infrarouge pour la prise de photo. Puis, un filtre de Gabor en deux dimensions est appliqué où l'iris est décomposé en vecteurs et chaque vecteur est analysé pour en arriver à un code de l'iris. Lorsque deux iris sont comparés, c'est leurs codes qui sont comparés et c'est la distance de Hammer qui est utilisée pour savoir si deux codes proviennent du même iris. Ce test d'indépendance statistique est simple : si le résultat du test est que moins du tiers des bites du code de l'iris est différent, ce code échoue au test de signifiance statistique et les deux codes sont considérés comme venant du même iris[146].

Avant même le 11 septembre, les aéroports considéraient l'utilisation de la reconnaissance par l'iris pour augmenter leurs mesures de sécurité[147]. Encore aujourd'hui, cette utilisation reste liée aux aéroports.

---

[145] Stellitano, Corrina, « Face Value », *Access control & security systems*, [en ligne], http://securitysolutions.com/mag/security_face_value/, (consulté le 28 septembre 2006).
[146] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Iris recognition*, *loc. cit.*, pp. 2 et 3.
[147] Meehan, Michael, *Iris scans take off at airports*, Computerworld, [en ligne], http://archives.cnn.com/2000/TECH/computing/07/19/iris.scan.idg/index.html, (consulté le 28 septembre 2006).

Rétine

Pour l'analyse de la rétine, une lumière de faible intensité illumine le fond de l'œil, là où se trouve la rétine, afin de montrer les motifs de la couche de vaisseaux sanguins. Un appareil photographie le tout et un algorithme l'analyse[148].

Les technologies rétiniennes n'ont jamais vraiment été publiquement utilisées, mais il y a quelques cas. D'abord à Fallujah, en Irak, où, après avoir assiégé la ville, les autorités états-uniennes ont imposé une carte obligatoire à tous les résidents, qui doit être portée en tout temps et qui inclut les empreintes digitales et l'empreinte de la rétine[149]. Cette technologie est aussi utilisée pour certaines installations militaires et gouvernementales[150].

Bio-dynamique (analyse de la voix, analyse de la signature)

La biométrie bio-dynamique comporte une composante statique (par exemple la forme de la signature), mais aussi dynamique (force utilisée lors de la signature) afin d'identifier ou d'authentifier quelqu'un.

Signature dynamique

L'analyse de la signature se fait à l'aide d'un matériel sensible au toucher qui permet d'enregistrer plusieurs caractéristiques comme la vélocité,

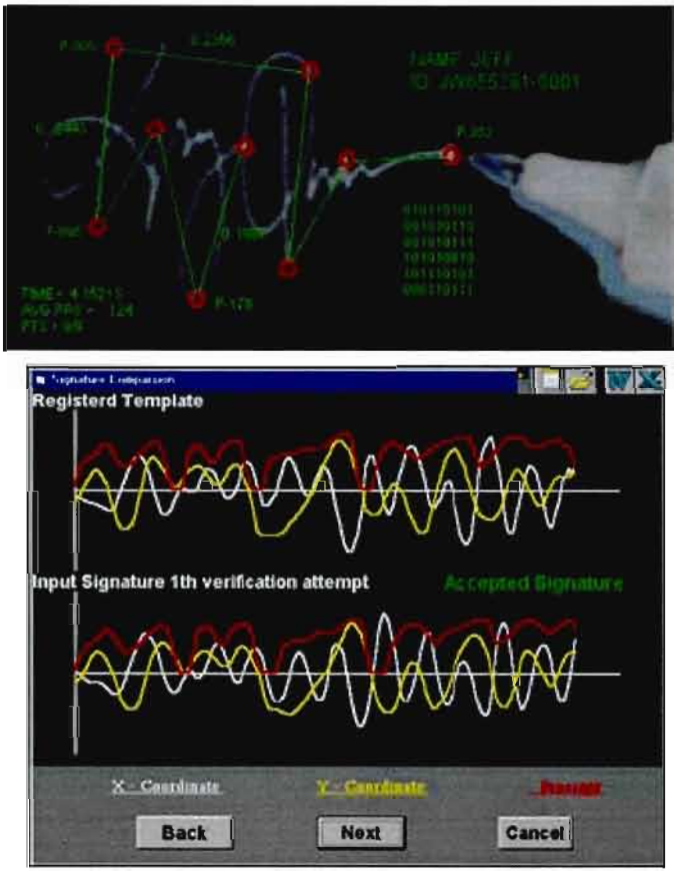
---

[148] National Center for State Courts - Court Technology Laboratory, Director of National Intelligence, *Retinal scan*, [en ligne], http://ctl.ncsc.dni.us/biomet%20web/BMRetinal.html, (consulté le 28 septembre 2006).

[149] Jones, Alex, *Fallujah Residents Face Choice: Retina Scan and Take ID Card....Or Die*, [en ligne], http://www.prisonplanet.com/articles/december2004/021204facechoice.htm, (consulté le 27 septembre 2006).

[150] Technovelgy.com, *Biometric authentication: what method works best?*, [en ligne], http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=16, (consulté le 29 septembre 2006).

l'accélération, la pression, les coups de crayon et leurs directions. Le tout est analysé dans un graphique à trois axes : les axes X et Y (lignes blanches et lignes jaunes) indiquant la vélocité et Z (lignes rouges) indique les changements de pression eu égard au temps. Aussi, il y a utilisation d'éléments statiques comme la forme et la géographie de la signature[151].



Schémas 4 et 5 : Exemples d'analyse de signature dynamique[152]

L'utilisation la plus connue de cette technologie est celle faite par l'IRS (*Internal Revenue Service* : ministère du Revenu aux États-Unis). Lorsqu'une

[151] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Dynamic Signature*, *loc. cit.*, pp. 1 à 3.
[152] *Idem.*

déclaration fiscale est faite par un tiers (H&R Block, par exemple) et est transmise électroniquement, le contribuable signe en utilisant cette technologie de signature dynamique[153].

Voix

Il y a deux formes de biométrie vocale, celle qui nécessite la lecture d'un texte et celle qui est indépendante de cette lecture. Dans la première forme, l'individu doit lire des phrases ou une série de chiffres qui, si le système se veut plus sécuritaire, sont aléatoires. Sa voix est ensuite comparée avec l'échantillon qu'il a fourni lors de son entrée dans le système et dont un modèle a été créé. Les modèles utilisés peuvent varier, que ce soit le « Hidden Markov Models » ou encore le « Gaussian Mixture Model », mais ils sont tous basés sur la construction statistique d'un modèle vocal auquel d'autres voix peuvent être comparées. Car il faut comprendre que la voix constitue une onde qui varie en temps (l'axe horizontal) et en intensité (l'axe vertical). Le système compare donc les caractéristiques de cette onde, que ce soit l'intensité dynamique, ses caractéristiques graves ou aiguës, etc. Aussi, les techniques n'étant pas dépendantes de la lecture d'un texte sont basées sur l'utilisation de caractéristiques comme le rythme, la vitesse, les intonations ou les prononciations. Bref, des caractéristiques relevant entre autres du type de personnalité, de l'éducation reçue, de l'origine linguistique, sociale.[154]

---

[153] Wright, Benjamin, *Signing tax returns with a digital pen*, Electronic Frontiers Georgie, [en ligne], http://www.efga.org/digsig/penop02.txt, (consulté le 17 septembre 2006).

[154] National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Speaker Recognition*, *loc. cit.*, pp. 2 à 5.

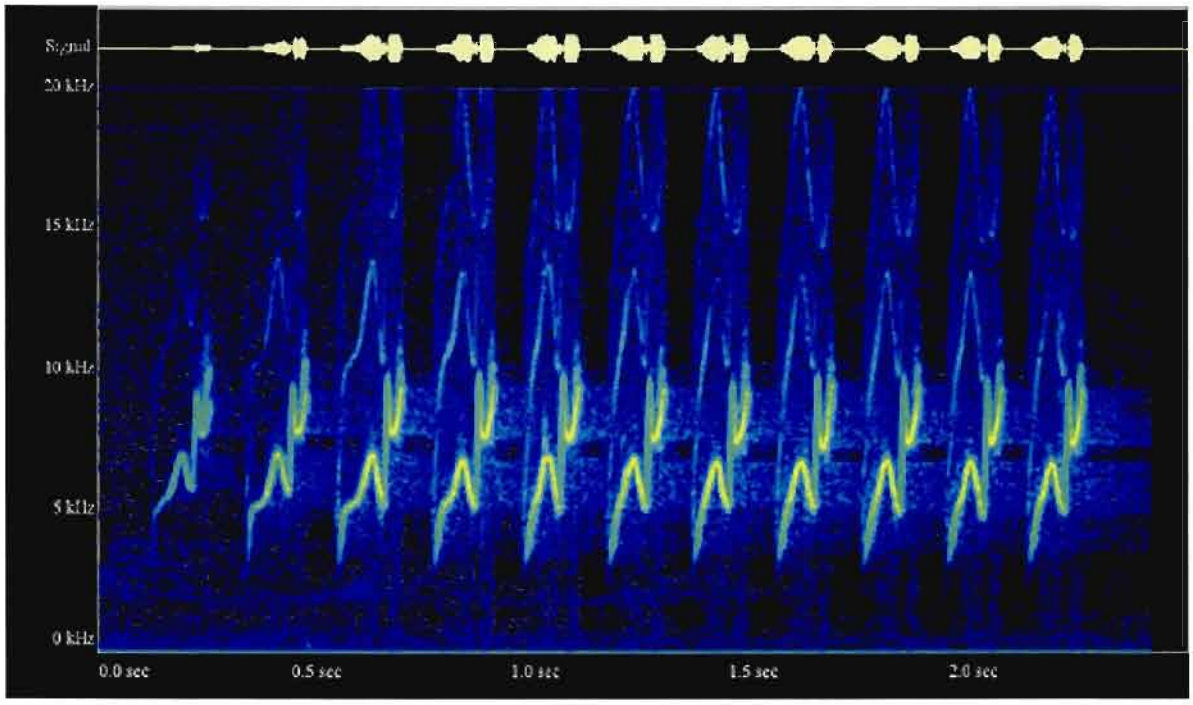


Schéma 6 : Analyse spectrale de la voix (les grands pics montrent l'intensité, la partie plus basse montre la nature spectrale de la voix)[155]

L'analyse de la voix a déjà été utilisée par une banque des Pays-Bas, la ABN AMRO, pour authentifier ses clients qui font des transactions par téléphone[156].

Fonctionnement des systèmes biométriques

D'abord, ces systèmes fonctionnent sur une base de probabilité et non d'une simple comparaison. Plus précisément, même si deux vecteurs sont identiques il en résultera quand même que deux lectures biométriques du même doigt (pour les scanographes d'empreintes digitales par exemple) ne

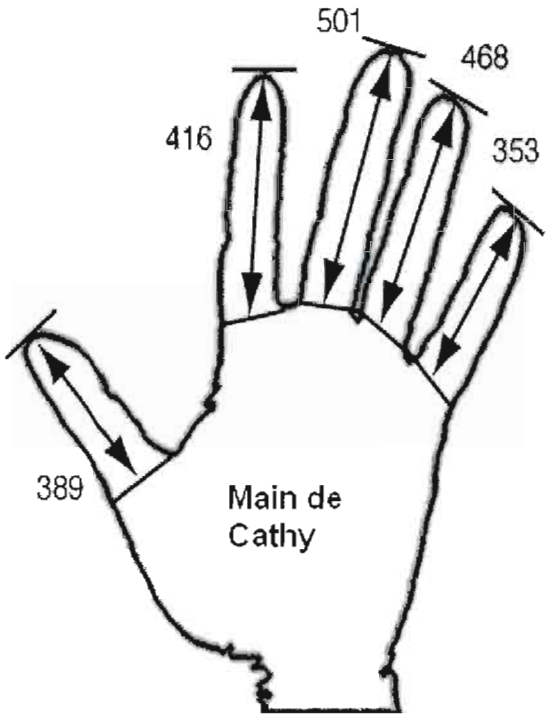
[155] *Ibid.*, p. 2.
[156] ABN AMRO, *ABN AMRO launches biometric voice verification in telephone banking*, [en ligne], http://www.abnamro.com/pressroom/releases/2006/2006-07-20-en.jsp, (consulté le 30 septembre 2006).

donneront jamais exactement le même résultat. Cela à cause des conditions environnementales, des changements de température, des légers changements sur les vecteurs biométriques (doigt enflé suite à un coup par exemple), des changements dans la façon dont la personne présente son doigt au lecteur et beaucoup d'autres imprévus.

Ainsi la machine quantifie la probabilité que deux vecteurs proviennent de la même personne[157]. Les personnes en autorité déterminent le seuil de tolérance, c'est-à-dire le niveau d'erreurs que la machine acceptera (car deux lectures d'un même vecteur, même provenant du même doigt et de la même personne, ne donneront jamais le même résultat), donc le seuil qui détermine le niveau de similitude minimum entre le vecteur emmagasiné et celui qui est présenté au lecteur afin de déterminer si une personne sera ou non reconnue comme légitime.

---

[157] Prabhakar Salil, Sharath Pankanti et Anil K. Jain, *loc. cit.*, pp. 33-35.



Signature biométrique de Cathy pour aujourd'hui	Signature entreposée de Cathy	Signature entreposée de Tim
389	390	284
416	418	570
501	502	534
468	471	501
353	355	399
	Distance de 4 par rapport à cette signature	**Distance de 19 par rapport à cette signature**

Tableau 2 : Comparaison entre deux lectures du même vecteur et un autre vecteur contenu dans la base de données[158]

Ce faisant, il y a deux types d'erreur que les lecteurs peuvent engendrer : les fausses acceptations, le système accepte ceux qui ne le devraient pas ; les faux rejets, le système rejette des gens dont la signature biométrique devrait être acceptée[159].

Il y a deux utilisations des systèmes biométriques, soit l'identification et l'authentification. La première constitue la recherche d'une personne parmi

[158] Smith, Rick, *The Biometric Dilemma*, secure computing, diapositive # 10, [en ligne], http://www.smat.us/crypto/docs/bh-us-02-smith-biometric.ppt, (consulté le 3 juin 2006).
[159] Prabhakar, Salil, Sharath Pankanti et Anil K. Jain, *loc. cit.*, pp. 33-35.

tant d'autres, il y a donc une banque de données et il y a utilisation d'un vecteur pour trouver si et à quel fichier la personne correspond, il faut ainsi trouver qui elle est. L'authentification est la comparaison entre un fichier précis et le vecteur que la personne présente, il ne s'agit plus de trouver qui est la personne comme avec l'identification, mais bien de savoir si elle est qui elle prétend être[160].

Une nouvelle tendance en biométrie est l'approche multi-modes (*Multimodals*) où plusieurs capteurs différents sont intégrés. C'est ce que tente *Accenture Technology Labs* qui déploie un cadre bayésien (*Bayesian framework*) pour intégrer de nombreux capteurs pour la surveillance complexe et plus globale. Cette approche intègre 30 caméras, des capteurs IR (infra-rouge) et un lecteur d'empreintes digitales. Le tout pour surveiller 18 000 pieds carrés (1 672 m^2) de superficie d'un édifice à bureaux. Tout le monde est surveillé en permanence, mais en plus l'ordinateur calcule la probabilité qu'une personne se trouve à un endroit précis en utilisant des « a priori » (quelqu'un se trouve plus souvent à un endroit que ses autres collègues) et des probabilités transitionnelles (personne ne peut être à deux endroits au même moment par exemple)[161].

Finalement, comme démontré précédemment, la biométrie connaît un vaste secteur d'application. Que ce soit l'identification à des fins judiciaires (criminalité, terrorisme, etc.) ou le contrôle des documents officiels (afin de renforcer leur sécurité et ainsi leur valeur dans les processus d'identification et d'authentification). Aussi, la biométrie permettrait d'assurer une meilleure

---

[160] Clarke, *loc. cit.*

[161] Gang Wei et Dongge Li « 8 : Biometrics : Applications, Challenges and the Future », In J. Strandburg, Katherine et Daniela Stan Raicu (sous la dir.), *loc. cit.*, pp. 144-145.

sécurité par rapport à l'accès à des zones et de l'équipement à accès restreint ou encore à des documents sécurisés[162].

Fiabilité de ces technologies

L'aspect de la sécurité reste la question centrale qui doit être posée afin de savoir si les technologies biométriques rehaussent la sécurité ou non, donc si elles doivent être implantées ou non. Le terme sécurité pourrait se définir comme étant une absence de menaces réelles ou appréhendées, tant à l'intérieur qu'à l'extérieur du territoire national, à la survie d'une personne. L'implantation de mesures sécuritaires est la réponse à l'identification d'une menace[163]. Il faut ainsi savoir si ces mesures sécuritaires, dans ce cas les technologies biométriques, sont efficaces face aux menaces. Bref, est-ce que la technologie fait ce qu'elle est censée faire ?

L'ADN

L'ADN est réputé pour être extrêmement fiable et capable de mettre les coupables en prison, mais aussi de libérer les innocents injustement condamnés. Le doute sur la fiabilité de l'ADN ne provient pas de son analyse en tant que telle, mais bien des risques réels de contaminations volontaires ou non.

---

[162] Commission de l'éthique de la science et de la technologie, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques – Documents de Réflexion*, pp. 5-6, [en ligne], http://www.ethique.gouv.qc.ca/fr/ftp/Biometrie-reflexion.pdf, (consulté le 30 mars 2006).

[163] *Ibid.*, pp. 1 à 3.

Les risques de contaminations involontaires sont nombreux et arrivent en fait assez souvent. Par exemple, lors du procès de Robert Pickon, qui est accusé d'avoir tué 6 femmes et suspecté d'en avoir tué beaucoup plus, au moins une demi-douzaine de preuves ont été contaminées par l'ADN des techniciens judiciaires. Dans un cas, l'ADN d'une technicienne s'est retrouvé sur deux preuves qu'elle n'avait même jamais manipulées directement. Le seul fait qu'elle se trouvait dans la même pièce a suffi à contaminer ces preuves. L'avocat de la défense a tout à fait raison de mentionner que ces contaminations sont arrivées en dépit des procédures et protocoles du laboratoire judiciaire[164]. Alors dans des conditions normales, il est naturel de déduire que les risques de contaminations sont encore plus grands.

Ce qui fait le plus mal à la fiabilité de l'analyse d'ADN est qu'actuellement, une simple technique pourrait mettre hors d'état l'analyse d'ADN pour un bon bout de temps. Il suffit de vaporiser le lieu d'un crime avec un autre ADN, par exemple à l'aide d'une bouteille de parfum remplie d'ADN (parce que les bouteilles de parfum comprennent déjà un mécanisme de vaporisation). Pour cela il faut d'abord mettre la main sur de l'ADN, ce qui est assez simple : il peut s'agir de la salive sur une bouteille d'eau ou sur un mégot de cigarette, ou encore un cheveu, etc. Ensuite avec cette salive ou ce cheveu, des milliards de copies peuvent être fabriquées avec grâce à un équipement servant à l'amplification en chaîne par polymérase (PCR). Ce qui est ironique, c'est que la meilleure façon pour un criminel de contrecarrer l'analyse d'ADN est d'en utiliser les mêmes techniques. Ce procédé est si efficace à produire de l'ADN que la bouteille de parfum sera pleine en quelques heures seulement. En quelques coups de vaporisateur, l'ADN va

---

[164] Matt Kieltyka, Sun Media C-News, *DNA contamination in Pickton trial*, [en ligne], http://cnews.canoe.ca/CNEWS/Canada/PicktonTrial/News/2007/03/28/3853028-sun.html, (consulté le 10 juin 2007).

prévaloir sur n'importe quel autre ADN trouvé sur le lieu du crime. D'ailleurs, un criminel qui laisserait tomber une goutte de sang n'aurait qu'à la vaporiser à quelques reprises d'un autre ADN et c'est ce dernier qui serait découvert lorsque la goutte de sang serait analysée, puisque celle-ci sera littéralement immergée par les milliards de molécules d'ADN du nouvel ADN[165].

Une machine PCR permet de faire des milliards de copies de l'ADN facilement, mais coûte beaucoup d'argent. Cependant, ce n'est pas nécessaire. Ces machines ne sont qu'un système de chauffage et de refroidissement... la même chose peut être faite avec des casseroles remplies d'eau chaude et un thermomètre. Essentiellement en utilisant des produits chimiques facilement disponibles et en plongeant et replongeant l'échantillon d'ADN dans des casseroles avec de l'eau à différentes températures. Tout ceci peut être fait à la maison et il est déjà facile de trouver des sites internet qui montrent comment changer les divers ustensiles, accessoires et articles de cuisine en les équipements scientifiques requis pour fabriquer des machines PCR artisanales. En fait, ce n'est pas beaucoup plus dur que de constituer un laboratoire artisanal pour fabriquer des amphétamines, ce que font déjà nombre de criminels, car ces plans tout comme ceux des machines PCR artisanales sont facilement accessibles sur internet[166].

Le scénario est donc le suivant : un criminel commet un délit, il se blesse légèrement et laisse tomber une goutte de sang, il la vaporise avec une mystérieuse bouteille contenant l'ADN de son patron. Les policiers

---

[165] Catalyst - Australian Broadcasting Corporation (ABC), *DNA Doubt*, émission du 16 septembre 2004, transcription, [en ligne], http://www.abc.net.au/catalyst/stories/s1199805.htm, (consulté le 30 janvier 2007).
[166] *Idem.*

arrivent sur les lieux, prélèvent le sang et en font une analyse d'ADN qui révèle le profil génétique... du patron ! Car un criminel avec quelques notions de base de bio-chimie peut facilement non seulement effacer « ses traces » du lieu d'un crime, mais aussi piéger n'importe qui en y laissant leur ADN[167].

Reconnaissance faciale

D'abord, le *National Institute of Standards and Technology* aux États-Unis a conclu que la technologie de reconnaissance faciale est inefficace et faillible et c'est la raison pour laquelle le gouvernement états-unien n'est pas allé plus loin dans l'implantation de cette technologie. D'autres rapports indiquent notamment que 18 mois après avoir inséré les mesures d'un visage dans une banque de données, il y avait 43% de chance d'avoir un faux-négatif (la vraie personne n'obtient plus l'accès avec son vecteur, dufait que le visage a trop changé en 18 mois)[168].

Ce constat est soutenu par la multitude des échecs de la reconnaissance faciale dans les aéroports (par exemple, deux Japonais qui ont inter-changé leurs passeports ont facilement déjoué le dernier cri en matière d'authentification faciale à l'aéroport de Sydney[169]), avec des probabilités de faux rejets et de fausses acceptations qualifiées d'excessives[170]. Les prétentions des compagnies biométriques sont

---

[167] *Idem.*

[168] Berkowitz, Bill, *Surveillance cameras are watching you in the name of the 'war on terrorism'*, WorkingForChange, 05.03.02, [en ligne], http://www.workingforchange.com/article.cfm?ItemID=13257, (consulté le 3 juin 2006).

[169] Dearne, Karen, *Face recognition fails test*, 27 février 2003, [en ligne], http://www.notbored.org/face-misrecognition.html, (consulté le 2 juin 2006).

[170] Willing, Richard, « Airport anti-terror systems flub tests », In *USA Today*, mis à jour le 9/2/2003, [en ligne], http://www.usatoday.com/news/nation/2003-09-01-faces-usat_x.htm, (consulté le 5 juin 2006).

contestables et mises en doute par plusieurs experts[171]. Même le président-directeur général de « Viisage », une des deux plus grandes compagnies en matière de reconnaissance faciale, met en doute l'utilisation de la reconnaissance faciale dans les aéroports en affirmant que la technologie n'en est pas rendue là[172]. D'ailleurs, un rapport de l'armée des États-Unis rapporte un taux de réussite de seulement 81% pour la reconnaissance faciale[173].

Par exemple, les résultats d'une étude sur la reconnaissance faciale de l'aéroport de Palm Beach démontrent que cette technologie ne fonctionne pas (des échecs 53% du temps, malgré des sujets coopératifs et des photos de très bonne qualité) en plus de causer des alarmes très fréquentes (deux à trois fois par heure), ceci en directe continuité des échecs de cette technologie lors des *Superbowl* et sur les rues de Tampa[174]. Imaginez une alerte donnée toutes les 20 minutes. Après quelques mois, les gardiens de sécurité vont tout simplement les ignorer.

Une autre expérience d'identification faciale à Tampa dans le district de Ybor corrobore l'expérience de Palm Beach, mais sur une plus grande échelle. Ce système prévoyait pouvoir reconnaître n'importe quel criminel qui déambulait dans les rues de Tampa, mais comme pour le *Superbowl*, il n'y a

---

[171] Schwartz, John, « New Side to Face-Recognition Technology: Identifying Victims », In *The New York Times*, 15 janvier 2002, [en ligne], http://www.nytimes.com/2002/01/15/science/physical/15FACE.html?ex=1130385600&en=10482ca2addbfbf2&ei=5070, (consulté le 9 juin 2006).

[172] Murphy, Shelley et Bray Hiawatha, « Face recognition devices failed in test at Logan », In *Boston Globe*, 9/3/2003, [en ligne], http://www.boston.com/news/local/articles/2003/09/03/face_recognition_devices_failed_in_test_at_logan/, (consulté le 1er juin 2006).

[173] King, Steven, *Testing Iris and Face Recognition in a Personnel Identification Application*, Information Systems Directorate, Office of the Deputy Under Secretary of Defense (Science & Technology), Hal Harrelson & George Tran Army Research Lab, 15 février 2002, pp. 7 à 8.

[174] ACLU, *Data on Face-Recognition Test at Palm Beach Airport Further Demonstrates Systems' Fatal Flaws*, 14 mai 2002, [en ligne], http://www.aclu.org/Privacy/Privacy.cfm?ID=10340&c=130, (consulté le 2 juin 2006).

eu aucune arrestation et aucune identification positive, mais plusieurs identifications négatives, certaines complètement loufoques (confondre un homme avec une femme criminelle)[175]. Il est fort peu probable qu'aucun criminel n'ait été à Ybor comme il est improbable qu'aucun criminel ne se soit trouvé parmi les dizaines de milliers de personnes qui se sont rendues au *Superbowl* en 2001 où la reconnaissance faciale a été testée.

Empreintes digitales

Même les empreintes digitales ne seraient pas aussi efficaces que prévu, un rapport du UKPS (*United Kingdom Passport Service*) indiquant un faible succès de 81% pour cette méthode[176]. Ce qui amène même le chef de l'agence des passeports de Grande-Bretagne à admettre que les terroristes et autres criminels très motivés ne seront pas arrêtés avec l'implantation des passeports biométriques[177]. D'ailleurs, la base scientifique affirmant que les empreintes digitales sont uniques ne serait pas si solide selon une enquête du *Newscientist*, car les études sur le sujet sont basées sur des prémisses et des statistiques douteuses[178].

---

[175] ACLU, *"Drawing a Blank: Tampa Police Records Reveal Poor Performance of Face-Recognition Technology."*, 3 janvier 2002, [en ligne], http://www.aclu.org/news/2001/n010302a.html, (consulté le 2 juin 2006).

[176] Rohde, Laura, « U.K.'s biometric trial exposes 'teething problems' », In *Computerworld*, [en ligne], http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,102051,00.html?from=story_picks, (consulté le 7 juin 2006).

[177] Fay, Joe, « Biometrics won't deter passport fraudsters, chief admits », In *The register*, 1er juillet 2005, [en ligne], http://www.theregister.co.uk/2005/07/01/bio_passport_fraud/, (consulté le 3 juin 2006).

[178] Randerson, James et Andy Coghlan, « Forensic evidence stands accused », In *New scientist*, 31 janvier 2004, Magazine issue 2432.

Objectivement, les empreintes digitales n'ont aucune base statistique ferme pour prouver leur fiabilité. Personne ne sait le taux de succès ou d'erreur. Et même si la prémisse, qui n'a jamais été prouvée, selon laquelle chaque empreinte digitale est unique était vraie, il reste toujours le problème de savoir quelle est la probabilité que deux personnes aient des empreintes assez similaires pour qu'un expert conclue qu'elles sont identiques[179].

De plus, il faut considérer qu'il est courant de retrouver des empreintes partielles sur le lieu d'un crime, alors quelle est la probabilité qu'une partie d'une empreinte digitale d'un tel ressemble profondément à une partie de l'empreinte digitale d'un autre[180] ? En réalité, il semble que l'acceptation des empreintes digitales en cour de justice relève davantage de la « tradition » que de la science, les empreintes digitales n'ayant pas eu à prouver leur efficacité au même niveau que l'analyse d'ADN par exemple.

Les autres technologies biométriques

Les autres technologies biométriques sont aussi problématiques. D'abord, la géométrie de la main est si imprécise qu'elle ne peut être utilisée que pour l'authentification et non pour l'identification. En fait, si assez de gens enregistrent le profil de la géométrie de leur main dans le système, il est probable que certains profils provenant de différentes personnes soient pareils[181]. Et c'est sans compter les coûts prohibitifs, qui ont justifié l'abandon

---

[179] Mnookin, Jennifer L., « The Achilles' Heel of Fingerprints », *Washington Post*, samedi 29 mai 2004, p. A27.
[180] *Idem.*
[181] National Center for State Courts - Court Technology Laboratory, Director of National Intelligence, *Hand geometry*, [en ligne], http://ctl.ncsc.dni.us/biomet%20web/BMHand.html, (consulté le 24 juillet 2007).

de l'INSPASS (*Immigration and Naturalization Service Passenger Accelerated Service System*), qui contrôlait la frontière mexicano-américaine par la biométrie de la géométrie de la main[182].

Ensuite, la précision de la reconnaissance par la signature est assez modeste et sa fiabilité plutôt basse. Les chances d'erreur sont d'une sur 50. Cette forme de biométrie ne peut être utilisée que pour l'authentification étant donné son manque de précision[183]. De plus, la signature d'une personne peut changer beaucoup avec le temps. Surtout qu'avec l'informatique, les gens ont de moins en moins d'occasions de développer une signature stable, alors la question est ouverte sur la pertinence même de cette technologie.

De même, la reconnaissance par la voix a aussi une précision plutôt modeste et une basse fiabilité en plus d'avoir aussi un taux d'erreur d'un sur 50. En plus, le bruit environnant, un rhume chez l'usager et plein d'autres facteurs vont diminuer son efficacité. La reconnaissance par la voix, comme la reconnaissance par la signature, ne peut servir que pour l'authentification à cause de sa précision modeste[184].

Une étude de l'armée des États-Unis place l'inefficacité de la biométrie de l'iris autour de 6 à 7% (1 à 2% si un seul œil est testé)[185]. De plus, le *General Accounting Office* (GAO) des États-Unis (équivalent du vérificateur général du Québec) a placé le taux d'échec à l'inscription autour de 0,5% et

---

[182] McMillan, Robert, « The Myth of Airport Biometrics », In *Wired News*, 9 août 2002, [en ligne], http://www.wired.com/news/conflict/0,2100,54418,00.html, (consulté le 2 juin 2006).
[183] National Center for State Courts - Court Technology Laboratory, Director of National Intelligence, *Biometrics comparison chart*, [en ligne], http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html, (consulté le 24 juillet 2007).
[184] *Idem.*
[185] King, Steven, *Testing Iris and Face Recognition in a Personnel Identification Application*, Information Systems Directorate, Office of the Deputy Under Secretary of Defense (Science & Technology), Hal Harrelson & George Tran Army Research Lab, 15 février 2002, pp. 7 à 8.

le taux de faux rejets allant de 1,9% à 6%. Alors, une personne sur 200 ne pourra pas s'inscrire, une sur 18 à une sur 50 subira un faux rejet. Certaines études rapportent des résultats encore pires[186].

Il est assez significatif que les gens avec des problèmes de vision soient souvent exclus des tests sur la reconnaissance par l'iris. Ainsi, les tests ne sont pas nécessairement faits sur une population en général, mais seulement sur ceux qui ont la capacité de les passer. Personne ne sait exactement combien sont ces gens, mais même une compagnie qui vend cette technologie les a estimés à « moins de 2% » (par conséquent, au minimum, c'est un peu moins de 6 millions de personnes aux États-Unis et quelque 153 000 citoyens québécois)[187].

Mais même les gens qui ont des « problèmes » sommes toutes très mineures en ce qui touche leurs yeux rencontreront des difficultés avec les systèmes de reconnaissance par l'iris. Ces « problèmes » incluent les yeux larmoyants, des cils trop longs ou encore des verres de contact durs[188]. En plus, les paupières peuvent causer des problèmes, notamment les paupières tombantes. Et lorsque la pupille se dilate ou se contracte, il y a parfois des déformations non élastiques de l'iris ce qui fait que les pupilles ne sont souvent pas complètement rondes (et donc l'iris aussi). Aussi, moins de la moitié de l'iris est visible chez groupes ethniques[189]. En fait, 7% des balayages de l'iris se sont soldés par des échecs lors d'essais faits par la

---

[186] House of Commons - Home Affairs (Grande-Bretagne), 57. Supplementary memorandum submitted by Privacy International, [en ligne], http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we66.htm, (consulté le 30 juin 2007).

[187] *Idem*.

[188] *Idem*.

[189] Drygajlo, Andrzej, *Biometrics*, [en ligne], http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007/07-Biometrics-Lecture-7-Part1-1-2006-12-04.pdf, pp. 22-27, (consulté le 18 juin 2007).

Grande-Bretagne qui a même dû suspendre ceux-ci à cause de tous ces problèmes[190].

Par contre, certaines technologies sont si expérimentales (reconnaissance par l'odeur, la démarche) ou si nouvelles (reconnaissance des veines) ou si peu répandues (reconnaissance de la rétine) qu'il est impossible de savoir objectivement leur taux d'efficacité, du fait qu'aucune étude indépendante n'a pu être répertoriée.

Problèmes techniques

Mais peu importe la méthode utilisée, le problème reste toujours celui de dresser le seuil de tolérance, c'est-à-dire le seuil qui va déterminer le niveau de similitude minimum entre le vecteur qui est emmagasiné et celui qui est présenté au lecteur pour déterminer si une personne sera ou non reconnue comme légitime (car l'empreinte digitale laissée par une personne n'est jamais la même, donc le système doit accepter une certaine part d'erreurs). À un extrême, plus le système est sécuritaire, plus grandes sont les chances qu'un individu ayant légitimement le droit d'accéder à quelque chose s'y verra refuser l'accès. À l'autre extrême, moins de gens qui sont légitimes seront rejetés, mais plus élevées sont les chances qu'un individu ne devant pas avoir accès à un lieu ou à quelque chose pourra déjouer les systèmes biométriques. Ainsi, il y aura toujours des taux de fausses acceptations et de faux rejets[191]. Et un taux de fausse acceptation de seulement 1,6% ferait en sorte que sur les 80 millions de chèques émis en

[190] House of Commons - Home Affairs (Grande-Bretagne), 57. Supplementary memorandum submitted by Privacy International, *loc. cit.*
[191] Thalheim Lisa, Krissler Jan et Peter-Michael Ziegler, *loc. cit.*

Australie, 1 million serait frauduleusement accepté. En 2001, seulement 12 500 chèques ont été frauduleusement émis avec les méthodes traditionnelles non biométriques. Inversement, le taux de faux rejets rend la biométrie inapplicable pour le système bancaire[192].

Certains vont même jusqu'à prétendre que l'identification et l'authentification de larges populations sont impossibles ou presque, car chaque ajout dans la banque de données centrale doit être comparé aux autres identités déjà en place. Même si un système avait un taux de réussite 99,9999%, cela donnerait une erreur à chaque million de vérifications, mais la capacité à bien identifier ou authentifier est inversement proportionnelle à la grosseur de la banque de données utilisée. Ainsi, pour avoir la véritable capacité d'un système (y), il faut prendre le taux de réussite (x) et le mettre à la puissance « z » qui est le nombre de personnes dans la base de données, soit $y = x^{z}$[193]. Par exemple, il y a 7 125 000 personnes au Québec, ce qui donne : $0{,}999999^{7125000} = 0{,}0008$. Alors, la véritable capacité de ce système, son véritable taux de réussite est de 0,8%. Donc cela n'est bon que pour une petite population de quelques centaines de milliers de personnes au maximum.

Même utiliser des technologies biométriques croisées n'arrange pas la situation, bien au contraire. Si deux vecteurs biométriques sont utilisés (un qui sera automatiquement plus faible que l'autre), il y a deux possibilités, soit l'individu doit « réussir » les deux tests ou réussir seulement un des deux. Dans ce dernier cas, il est évident que la technologie biométrique avec le

---

[192] Dearne, Karen, *Biometric checks must improve*, [en ligne], http://www.argus-solutions.com/austit15oct02.html, (consulté le 6 juin 2006).

[193] SA Mathieson, « Image problem », In *The Guardian*, 20 novembre, 2003, [en ligne], http://technology.guardian.co.uk/online/story/0,3605,1088437,00.html, (consulté le 5 juin 2006).

plus faible rendement va tirer le système vers le bas, du fait que les gens qui veulent déjouer le système ne doivent qu'en déjouer un seul pour passer (puisque pour être refusé, il faut échouer aux deux tests, tandis que pour passer, il ne faut qu'en réussir un seul). Donc, le taux de fausses acceptations sera très élevé et celui de faux rejets très bas[194].

Mais même dans l'autre cas, où il faut réussir les deux tests, ce n'est pas mieux, car pour être refusé, il ne faut qu'échouer un test alors que pour être accepté, il faut passer les deux. Cela va diminuer le nombre de fausses acceptations, mais exagérer le nombre de faux rejets[195]. Seule une similitude d'efficacité entre deux systèmes permet une meilleure performance,[196] mais la problématique caractéristique de la biométrie (faux rejets VS fausses acceptations) reste la même.

Une technologie facilement déjouable

D'ailleurs, ces systèmes sont plus ou moins facilement déjouables. En fait, il y a trois façons de contourner les systèmes[197] :

1- utiliser des vecteurs artificiels (par exemple, de mouler une empreinte digitale avec du latex afin d'en créer une copie conforme) afin d'imiter le vecteur réel,

---

[194] Daugman, John, *Combining Multiple Biometrics*, The Computer Laboratory, Cambridge University, http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html, (consulté le 24 juin 2006).
[195] *Idem.*
[196] *Idem.*
[197] Thalheim Lisa, Krissler Jan et Peter-Michael Ziegler, *loc. cit.*

2- passer outre le lecteur biométrique et envoyer de l'information imitant la lecture du vecteur directement à la cible (attaque qui ressemble à celle dont sont victimes les gens qui se font frauder par carte de débit, où un fil est installé dans le lecteur légitime afin de copier la bande magnétique de la carte).

3- attaquer la base de données directement afin d'échanger les associations entre vecteurs biométriques et privilèges à accéder à certains endroits ou certains documents.

Une équipe de journalistes a essayé de déjouer ces systèmes en utilisant la première façon, et tous les systèmes testés ont échoué bien que les méthodes utilisées fussent pour le moins primitives. Par exemple, souffler sur la matrice à empreintes digitales afin de « ré-activer » la dernière empreinte du fait que la buée due au souffle fait ressortir l'empreinte[198]. Donc, les systèmes avec empreintes digitales sont plus ou moins fiables, car il faut un capteur qui, à moins d'être essuyé après chaque utilisation, peut être compromis du fait qu'il reste une empreinte latente qui peut être prélevée de diverses façons : soit la méthode mentionnée précédemment de souffler sur les capteurs, ou encore utiliser un mince sac de plastique rempli d'eau froide et le coller sur le capteur ou encore utiliser de la poussière de graphite puis du ruban gommé. Cette dernière méthode donne un taux de réussite de presque 100%[199]. De plus, même les nouveaux systèmes qui utilisent des méthodes pour s'assurer que le vecteur est authentiquement vivant (par opposition à un doigt coupé) ont aussi échoué. Pour les lecteurs d'iris, le résultat est tout aussi problématique. Il a suffi que les journalistes fassent une photocopie d'un iris et d'y faire un trou au niveau de la pupille. Le journaliste

---

[198] *Idem.*
[199] Gang Wei et Dongge Li. *loc. cit.*, pp. 142-143.

met la photocopie devant son œil et lorsque le système regarde l'iris photocopié, il ne voit pas la différence entre la photocopie et l'original. Et lorsqu'il regarde la dilatation de la pupille pour s'assurer que ce n'est pas un œil arraché, il voit la dilatation à travers le trou de la photocopie, le système est ainsi déjoué (voir annexe)[200].

Dans la même ligne, Tsutomu Matsumoto[201] a réussi à déjouer 80% des lecteurs d'empreintes digitales en utilisant de la gélatine à bonbon (coûtant seulement 10$) pour mouler des empreintes digitales. Il a même réussi l'expérience en utilisant des empreintes latentes qui sont des empreintes non visibles provenant de résidus comme de la saleté ou de la sueur laissées sur un objet par opposition aux empreintes directes qui laissent une marque visible. Il est à noter que M. Matsumoto est mathématicien et non pas un spécialiste en effets spéciaux[202] (voir annexe). Car un vecteur biométrique ne donne jamais la même valeur deux fois, donc il est possible qu'un criminel fasse une copie assez précise pour que le lecteur biométrique l'accepte[203].

De plus, il est évident que s'il y a système biométrique, il faut inscrire les gens et les terroristes ne vont pas s'inscrire si c'est possible, et même s'il le faut, ils ne vont pas s'enregistrer en tant que terroristes[204].

---

[200] *Idem.*
[201] T. Matsumoto et al., *loc. cit.*
[202] Schneier, Bruce, « Fun with Fingerprint Readers », In *Crypto-Gram Newsletter*, 15 mai 2002, [en ligne], http://www.schneier.com/crypto-gram-0205.html#5, (consulté le 8 février 2006).
[203] Garfinkel, Simson, *Biometrics Slouches Toward the Mainstream : The systems are getting cheaper, but accuracy and acceptance kinks remain*, CSO, [en ligne], http://www.csoonline.com.au/index.php/id;1183366141;fp;8;fpid;8, (consulté le 9 juin 2006).
[204] Ackerman, Linda, *Biometrics And Airport Security*, Privacyactivism.org, 17 février 2003, [en ligne], http://www.privacyactivism.org/Item/64, (consulté le 1er juin 2006).

Après avoir vu le fonctionnement des différentes technologies biométriques, il a été possible de constater que leur fiabilité, c'est-à-dire leur capacité à performer comme elles le devraient, est plutôt douteuse. Car si la biométrie a démontré quelque chose, c'est qu'il faut en être critique. Prenons l'analyse de comparaison de cheveux, c'est-à-dire la « science » qui prétendait être capable de dire si deux cheveux provenaient de la même personne en comparant leurs caractéristiques physiques. Barry Gaudette, de la GRC et pionnier dans cette technique, prétendait, dans une étude faite dans les années 70, que la possibilité que cette méthode se trompe était d'une sur 4500, soit 0,02%[205]. Une technique si précise qu'elle a été utilisée pour condamner des gens à mort[206]. Cependant, l'avocat et scientifique Stafford Smith, avec l'aide d'analystes de l'Université Columbia, a décidé de reprendre les données originales de l'étude de Gaudette et réanalyser le tout. Il a conclu que l'étude était tellement peu rigoureuse que c'était pratiquement du charlatanisme, lui et ses spécialistes ayant établi que la possibilité d'erreur était plutôt d'une sur deux ou 50%[207]. Depuis cette révélation, vingt détenus ont été libérés aux États-Unis[208]. Le Dr Edward Blake résume bien le tout en disant : « There's no scientific basis for hair comparison under virtually any circumstance. »[209] En fait, jouer à pile ou face aurait donné un résultat similaire ! Pensons-y bien, cet avocat a été le premier et le seul à contester cette technique biométrique utilisée depuis plusieurs décennies. S'il n'avait rien fait, cette technique serait encore utilisée. Alors, il faut toujours poser la

---

[205] CBC News Disclosure, *Unreliable evidence*, [en ligne], http://www.cbc.ca/disclosure/archives/031126_evidence/hair.html, (consulté le 3 janvier 2007).

[206] Scheck, Barry et Peter Neufeld, « Junk Science, Junk Evidence », In *The New York Times*, 11 mai 2001, section A, p. 35.

[207] CBC News Disclosure, *loc. cit.*

[208] *Idem.*

[209] Wrolstad, Mark, « Hair-matching flawed as a forensic science: DNA testing reveals dozens of wrongful verdicts nationwide », In *The Dallas Morning News*, [en ligne], http://www.law-forensic.com/cfr_hair_3.htm, (consulté le 3 janvier 2007).

même question de la crédibilité des autres techniques et technologies biométriques et toujours mettre en doute leur supposée fiabilité. Car il est évident que les technologies biométriques ne peuvent apporter une sécurité significativement accrue si elles ne donnent pas les résultats escomptés. Si elles ne peuvent apporter la sécurité voulue, à quoi servent-elles ? Ainsi, il faut poser la question des impacts de ces technologies faillibles sur la démocratie et sur la vie privée afin de pouvoir répondre à la question de recherche de ce mémoire.

Chapitre 3 : Impacts de la biométrie sur la pratique de la démocratie libérale

Après avoir vu l'histoire de la biométrie, et avoir analysé le fonctionnement de ces technologies et leur faillibilité, il est pertinent d'entrer dans le vif du sujet : les impacts de l'implantation de la biométrie sur la pratique de la démocratie libérale et surtout sur une de ses valeurs fondamentales, l'espace privé. Dans ce chapitre, il sera d'abord question de rappeler quelques-unes des caractéristiques de la démocratie libérale qui sont pertinentes pour cette étude. Ensuite, ce mémoire tentera d'évaluer les impacts de la biométrie sur la pratique de la démocratie libérale. Cette section sera divisée en quatre parties, soit les bases de données, le panopticon, la criminalité et le terrorisme puis finalement sur le risque de glissement. Enfin, une étude d'un cas sur ces glissements possibles, portant sur le numéro d'assurance sociale aux États-Unis, sera présentée.

Traditionnellement, la « démocratie libérale » est présentée comme une forme de gouvernement représentatif où le pouvoir de l'État et de ses agents est soumis à des contraintes. Celles-ci prennent la forme de contrepoids législatifs (parlements) et judiciaires (tribunaux), mais aussi par l'existence de constitutions et de chartes qui garantissent des droits aux citoyens. Les membres composant le législatif et de l'exécutif sont choisis par le biais d'élections fréquentes, libres, au suffrage universel et mettant en opposition plusieurs partis politiques.

D'abord, le gouvernement de type démocratique et libéral tire sa légitimité du consentement de ses gouvernés. En effet, ceux-ci n'ont aucune autre obligation que celle de se soumettre aux lois faites par le pouvoir

législatif auquel ils ont consenti leur autorité : c'est la souveraineté populaire[210]. Il en résulte, dans une perspective de démocratie libérale lockienne, que le pouvoir politique doit faire les lois, utiliser les moyens nécessaires pour les faire appliquer, défendre la société des menaces intérieures et extérieures, mais surtout préserver la protection de la propriété privée[211]. Car pour Locke, l'homme est propriétaire de lui-même et de ses actions et en conséquence le droit de propriété est essentiel[212]. Cette conception de la propriété privée est la base de la démocratie libérale, en ce sens que le citoyen possède non seulement sa propre personne et sa propriété foncière, mais aussi sa propre sphère privée (qui elle-même est la base d'une foule de droits dont celui de la liberté de croyance). Cette sphère privée, droit inaliénable, est, dans la conception classique de la démocratie libérale, sa demeure, qui est son sanctuaire où même le gouvernement, c'est-à-dire l'acteur le plus puissant d'une société, ne peut pénétrer sans le consentement de son propriétaire. Puisqu'à moins qu'il n'ait violé la loi, donc la volonté populaire exprimée à travers l'exercice du pouvoir législatif, ce citoyen a la garantie de la quiétude et de l'inviolabilité de son sanctuaire. La propriété privée et la sphère privée sont ainsi intimement liées dans cette conception de la démocratie libérale inspirée par le grand penseur John Locke. Ce lien entre démocratie, propriété privée et sphère privée est important du fait que la biométrie pose de sérieuses questions à propos de la sphère privée, concept clé de ce mémoire, et pourrait en changer la définition en faveur de la sphère publique en rétrécissant l'espace privé avec toutes les conséquences que cela aurait sur la démocratie libérale.

---

[210] Locke, John, *The Second Treatise of Government*, The Library of Liberal Arts, The Bobbs-Merrill Compagny Inc., imprimé aux États-Unis, 1952, p. 15.
[211] *Ibid.*, p. 4.
[212] *Ibid.*, pp. 26-27.

Mais poursuivons dans les autres aspects pertinents de la démocratie libérale dans le contexte de ce mémoire. En ce qui concerne la séparation des pouvoirs, Montesquieu montre qu'il y en a trois qui sont constitutifs d'un État : le législatif, l'exécutif et le judiciaire. Le premier est chargé de faire les lois, de voir si elles sont appliquées et de les abroger si nécessaire, c'est un pouvoir mieux assumé par plusieurs (comme le montre le grand nombre de députés dans les parlements démocratiques). De plus, il doit y avoir possibilité de changer le corps législatif afin de garder la confiance du public et assurer sa représentativité et sa légitimité (ce qui implique des élections fréquentes). Le second est l'exécutif, qui est responsable de la direction de la politique étrangère et assure la sécurité publique. Le dernier, le pouvoir judiciaire, se doit de régler les disputes civiles et de punir les criminels selon les lois en vigueur, bien qu'il doive être séparé des deux autres pouvoirs, sinon l'arbitraire en serait le résultat car le juge appliquerait les lois qu'il décréterait lui-même[213]. C'est le principe même d'une dictature que c'est le juge qui fait ses lois tandis que dans une démocratie le juge applique les lois du législatif[214]. Ces trois pouvoirs doivent être séparés puisque la concentration du pouvoir ne peut mener qu'au pouvoir absolu, à la tyrannie. En fait, chaque pouvoir se doit de contrebalancer les autres[215]. Cela est très important par rapport à la biométrie en tant que telle, du fait qu'il semble bien que l'implantation de la biométrie mène au renforcement de l'exécutif et des diverses agences étatiques (comme les forces policières et les services de sécurité en premier lieu) au détriment du législatif, donc du Parlement réunissant les élus. Le meilleur exemple de cette situation se retrouve en Grande-Bretagne où même après avoir perdu un vote au Parlement en avril

---

[213] Montesquieu, *De l'Esprit des lois, I*, Collection Folio/Essais, Gallimard, La Flèche (Sarthe), France, 1995, pp. 327-342.
[214] *Ibid.*, pp. 200-201.
[215] *Ibid.*, pp. 327-342.

2005 sur la question de la carte d'identité nationale, le gouvernement affirmait qu'il allait utiliser sa prérogative royale pour forcer les futurs détenteurs de passeport à donner leurs empreintes digitales qui seront dans une nouvelle banque de données. Les policiers auront accès à cette banque de données lors de leurs enquêtes courantes et pourront comparer toutes les empreintes trouvées sur le lieu d'un crime à celles qui se trouvent dans cette banque de données. De plus, le gouvernement a l'intention de se servir de la prise d'empreintes digitales pour le passeport comme de « blocs de construction » (*building block*) menant à une carte d'identité biométrique nationale[216]. La biométrie a dans ce cas fait pencher la balance du pouvoir vers le gouvernement et les services policiers de façon excessive, et le débalancement des trois composantes étatiques en faveur d'une seule ne peut qu'être néfaste pour le fonctionnement de la démocratie libérale.

Finalement, une condition cruciale à la liberté est l'assurance de la sécurité,[217] car sans celle-ci il est très difficile de jouir des autres libertés. Cette sécurité est assurée par le gouvernement qui la régule en instaurant la règle de droit (rule of law). Celle-ci fait en sorte que tous doivent obéir à la même loi créée par le législatif, c'est l'égalité de tous devant la loi (« Law should be like death, which spares no one. »[218]). À l'intérieur de ces lois, un homme peut faire ce que bon lui semble sans subir l'arbitraire d'un autre,[219]

---

[216] Travis, Alan, home affairs editor, « Passport applicants must give fingerprints : Preparation for ID cards goes ahead without parliament », *The Guardian*, Mardi 12 avril 2005, [en ligne], http://www.guardian.co.uk/uk_news/story/0,,1457289,00.html, (consulté le 4 mai 2007).

[217] Montesquieu, *op. cit.*, pp. 327-328.

[218] Soliman, Omar, *Political Jurisprudence vs. Judicial Independence : Reflections on the Legal Purpose and Institutional Role of Courts in a Liberal Democracy*, Université de Toronto, [en ligne], http://individual.utoronto.ca/soliman/essays/political_jurisprudence_vs_judicial_independence.pdf, (consulté le 25 janvier 2007).

[219] Locke, *op. cit.* Section 22.

car la liberté face à l'arbitraire est essentielle[220]. C'est dans cette optique que la fiabilité de la biométrie, dans le chapitre deux, a été abordée du fait qu'il était primordial de savoir si la biométrie pouvait apporter un renforcement considérable de la sécurité. C'est important du fait que la démocratie est basée sur la liberté qui, elle-même, ne peut exister sans qu'il y ait un minimum de sécurité.

Mais pour revenir plus en profondeur sur le droit à la vie privée, il faut constater que ce droit est un des droits fondamentaux les plus importants dans les démocraties libérales, un droit que le juge Louis Brandeis a qualifié de « *right to be left alone* ». Ce dernier et son collègue Samuel Warren, deux universitaires qui allaient devenir juges à la Cour suprême des États-Unis, sont parmi les premiers à avoir voulu faire reconnaître le droit à la vie privée. Tout en admettant que les avancées technologiques aient changé la donne, ils sont les premiers à définir la vie privée comme une valeur unifiée et cohérente, une valeur sacrée et inviolable[221]. Leur œuvre clé est un article publié dans la *Havard Law Review* en 1890 intitulé « The Right to Privacy »[222]. Dans cet article, ils se penchent sur les changements technologiques dont l'avènement nécessiterait que la vie privée soit légalement protégée. Ils faisaient plus précisément aux pratiques de la presse qui violaient le droit à la vie privée des gens. Ils dénonçaient en particulier le recours de plus en plus massif à la photographie dans les journaux, et dont la presse de l'époque abusait abondamment. Face à une

---

[220] *Ibid.*, Section 23.
[221] Schoeman, Ferdinand, « 1 : Privacy : philosophical dimensions of the litterature », In Schoeman, Ferdinand David (sous la dir.), *loc. cit.*, pp. 15-16.
[222] Warren, Samuel et Louis D. Brandeis, « The Right to Privacy », *Harvard Law Review*, IV, décembre, 1890.

presse qui invoquait le premier amendement de la Constitution[223], qui affirmait la liberté d'expression, il fallait avoir un contrepoids protégeant la vie privée des gens. C'est de là que le fameux « *right to be left alone* » a été utilisé pour décrire la vie privée en ses termes les plus simples. Mais il n'y avait pas que la photographie et son abus par la presse qui inquiétaient ces deux juristes. Les télégraphes et les téléphones représentaient aussi des technologies qui pouvaient diminuer la vie privée des gens[224]. Ce n'était pas encore de la haute technologie, mais pour ces deux universitaires, la Constitution protégeait déjà insuffisamment la vie privée à une époque où les banques de données et la surveillance étaient quasi non existantes. L'influence de ces deux futurs juges sur le droit et les législations sur la vie privée est aujourd'hui encore pertinente et d'actualité.

D'ailleurs, la Constitution australienne est très intéressante à ce sujet :

> A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organizations to intrude on that autonomy [...] Privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech [...] Privacy is a basic human right and the reasonable expectation of every person.[225].

Donc le droit à la vie privée ferait partie intégrale de la conception libérale de démocratie.

---

[223] Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.
[224] Warren, Samuel et Louis D. Brandeis, *loc. cit.*
[225] Privacy International, *Privacy and Human Rights, 2003: Overview*, [en ligne], http://www.privacyinternational.org/survey/phr2003/overview.htm, (consulté le 5 juin 2006).

Finalement, l'importance du droit à la vie privée est reconnue dans l'article 12 de la Charte des droits de l'Homme ainsi que dans l'engagement (*Covenant*) international sur les droits civils et politiques. Et aussi bien en Europe qu'en Amérique du Nord, le droit à la vie privée est reconnu dans des conventions régionales ou nationales. Ces droits sont exécutoires, que ce soit sous la Cour inter-américaine, la Cour européenne des droits de l'Homme ou encore la Commission européenne. Il y a aussi des lignes directrices minimales faites par l'Assemblée générale de l'ONU, l'OCDE et d'autres organisations concernant la protection des renseignements sur support informatique. Les données doivent être obtenues légalement, gardées en sécurité, être exactes et mises à jour et ne doivent être utilisées que dans le but originalement prévu[226].

Biométrie et la pratique de la démocratie libérale

Il sera question de l'impact de l'implantation de la biométrie sur la pratique de la démocratie libérale, plus précisément sur le contrôle de l'accès aux frontières personnelles qui en est constitutif (concept double qui inclut le contrôle informationnel et le contrôle sensoriel ou l'accès et le non-accès physiques et mentaux aux autres). La partie sur les bases de données est évidemment reliée exclusivement à la première fonction du contrôle de l'accès, c'est-à-dire le contrôle informationnel. Tandis que les autres parties que ce soit le panopticon, le risque de glissement ou encore la criminalité et le terrorisme traitent des deux fonctions du contrôle de l'accès : les fonctions du contrôle informationnel et du contrôle sensoriel.

---

[226] Thomas, Rebekah, *Biometrics, Migrants, and Human Rights*, Global Commission on International Migration, 1er mars 2005, [en ligne], http://www.migrationinformation.org/Feature/display.cfm?id=289, (consulté le 6 juin 2006).

Bases de données

Pour que le « Big Brother » de George Orwell puisse exister, il faudrait trois éléments : des systèmes qui accumulent des données personnelles dans des buts précis ; ces systèmes doivent être inter-reliés en réseaux ; ces informations doivent être constamment reliées à une personne (les personnes doivent être constamment et correctement identifiées). La biométrie est la réponse à la troisième condition, les deux autres ayant été satisfaites depuis longtemps. La biométrie menace donc de réaliser le cauchemar dont le célèbre livre d'Orwell, *1984*, brossait le tableau[227]. Mais regardons d'abord du côté des bases de données.

Étant donné le coût de la biométrie, les gouvernements auront tendance à lui accorder de multiples buts afin d'en réduire la cherté (par exemple, au lieu d'avoir à la fois une carte d'assurance maladie, un permis de conduire et une pièce d'identité, il pourrait n'y avoir qu'une seule carte). Cela ferait en sorte que les frontières entre agences s'effaceraient et que les données seraient de plus en plus croisées, concentrant ainsi un pouvoir inacceptable entre les mains du gouvernement[228]. Mais, c'est surtout l'établissement d'un registre central qui cause un problème majeur, car la séparation et la compartimentalisation de l'information constituent une assurance pour la protection de la vie privée. En outre, le fait d'avoir plusieurs banques de données permet de mieux faire face à une erreur de système

---

[227] Clarke, Roger, *Biometrics and Privacy*, Xamax Consultancy Pty Ltd, Canberra, Department of Computer Science, Australian National University, Notes du 15 avril 2001, [en ligne], http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html, (consulté le 3 juin 2006).

[228] *Idem.*

que s'il n'y a qu'une seule banque centrale de données[229]. Enfin, il ne faut pas oublier que plus un système est complexe, plus grandes sont les probabilités et plus graves sont les conséquences de son effondrement. Par exemple, dans les années 80, la moitié du réseau téléphonique d'AT&T est tombée à cause d'un virus informatique[230].

Il vient d'être question des risques pour la démocratie libérale et son fonctionnement, mais il y a aussi des dangers pour les libertés individuelles. D'abord, la biométrie amène un faux sentiment de sécurité : les gens se pensent en sécurité, mais la sécurité est déficiente du fait que les bases de données sont toutes vulnérables. Ainsi en 2002, un employé de *Teledata Communications* a vendu 30 000 mots de passe qui donnent accès aux dossiers de crédit... Quel cauchemar avec la biométrie[231]!

D'ailleurs, considérons que des méga-bases de données ont été créées par l'industrie du crédit pour les aider à mieux identifier et à cibler plus efficacement leurs clients (par exemple, Equifax), ces bases ont été de plus en plus inter-connectées et mises en ligne sur internet. Peu après, le vol d'identité devenait le crime en plus haute progression (il a triplé entre 1995 et 2000). Une autre technologie qui a amené un nouveau type de crime[232]. Et c'est sans compter le risque que des membres du crime organisé s'y infiltrent pour obtenir des données comme il y a quelques années à la SAAQ (ce qui avait mené à la tentative de meurtre sur le journaliste d'enquête Michel

---

[229] Davies, Simon G., « Touching Big Brother : How biometric technology will fuse flesh and machine », In *Information Technology & People*, Vol 7, No. 4 1994, [en ligne], http://www.privacy.org/pi/reports/biometric.html, (consulté le 27 février 2006).
[230] *Idem*.
[231] Ackerman, *loc. cit.*
[232] Mann, Charles C. « Homeland Insecurity », In *The Atlantic Monthly*, septembre 2002, p. 1.

Auger)[233]. Ensuite, il est évident et déjà visible que les compagnies privées voudraient avoir accès aux données biométriques avec les conséquences facilement imaginables. Il y aurait déjà, semble-t-il, des discussions pour partager ce genre d'informations avec les compagnies aériennes[234]. Ainsi, le comté de Pinellas en Floride partage ses bases de données de visages avec les autres autorités policières de la Floride et d'autres États gardent la photo du visage de tous les détenteurs de permis de conduite[235].

Les données biométriques pourraient permettre de faire aussi intrusion dans la vie privée des gens du fait que certaines caractéristiques indiquent la présence de maladies, ce qui pourrait compromettre la capacité de ces gens de contracter une assurance vie par exemple[236].

Le citoyen perd donc de plus en plus le contrôle informationnel sur les données relatives à sa personne et la biométrie n'aide en rien au rétablissement de ce contrôle de l'accès.

Panopticon

Le philosophe anglais, Jeremy Bentham, proposait, en 1787, un modèle de prison où les détenus pourraient être surveillés par un très petit nombre de gardes, et qu'il appelait le *Panopticon*. La vigie se trouverait au

---

[233] LCN, *La SAAQ infiltrée par deux taupes reliées aux motards*, [en ligne], http://lcn.canoe.com/infos/national/archives/2000/12/20001208-062657.html, (consulté le 7 juin 2006).

[234] Privacy International, *An Open Letter to the ICAO : PI creates global coalition calling on UN agency to stop its biometric database standard, A second report on 'Towards an International Infrastructure for Surveillance of Movement'*, 30/03/2004, p. 2, [en ligne], http://www.privacyinternational.org/issues/terrorism/rpt/icaoletter.pdf, (consulté le 15 mars 2006).

[235] Gallagher, Sean, *The New Face of Surveillance*, [en ligne], http://www.baselinemag.com/article2/0,1540,1725643,00.asp, (consulté le 3 juin 2006).

[236] Prabhakar Salil, Sharath Pankanti et Anil K. Jain, *loc. cit.*, p. 41.

milieu de cellules construites en cercle et la lumière passerait par les barreaux extérieurs et le détenu produirait une ombre[237]. Le Panopticon fonctionnerait même si le garde n'est pas présent, car la visibilité générale et permanente engendrait la conformité et le contrôle social.

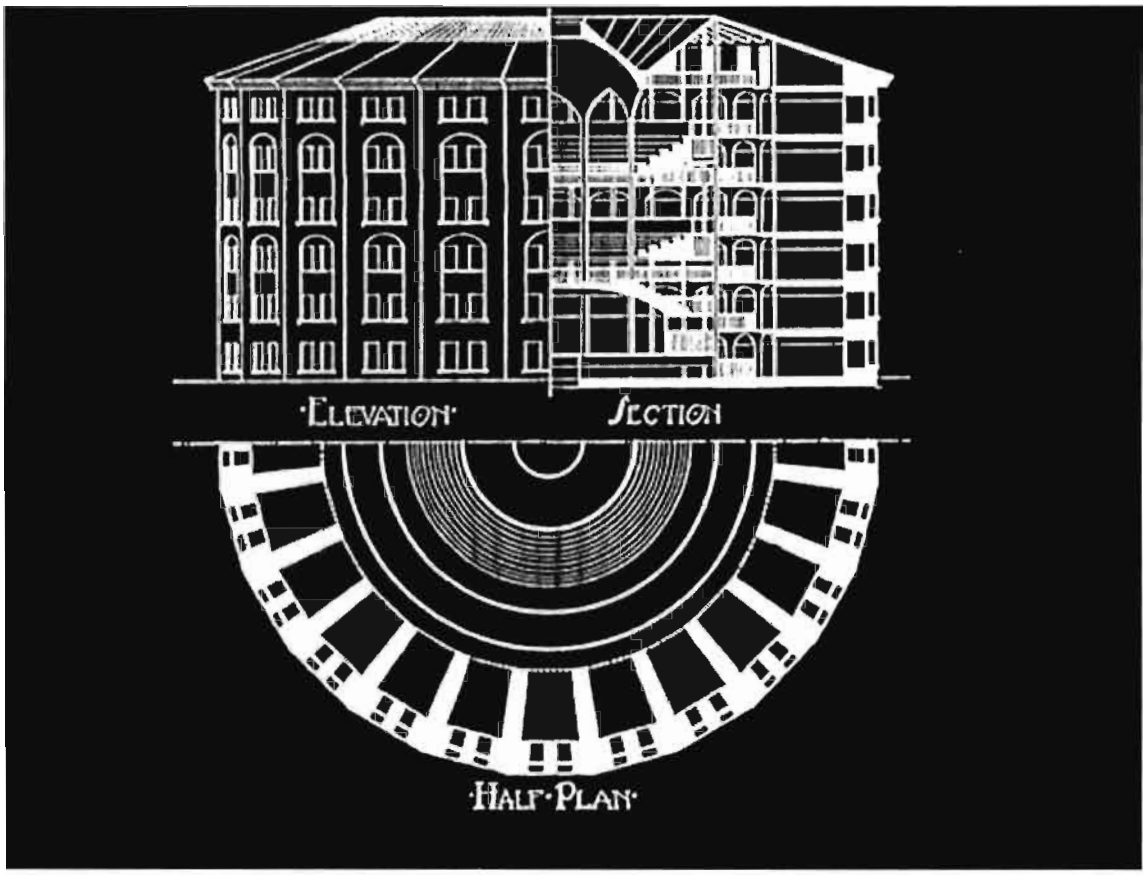


Schéma 7 : Élevation, section et plan de coupe du Panopticon de Jeremy Bentham[238]

[237] Reiman, *loc. cit.*, pp. 195-196.
[238] Columbia University Graduate School of Architecture, planning and preservation, *Panopticon*, [en ligne], http://www.arch.columbia.edu/DDL/cad/IP_SP99/students/Trent/imaps/panopticon.jpg, (consulté le 25 août 2006).

En se référant à ce modèle, Michel Foucault fait remarquer que celui « qui est soumis à un champ de visibilité et qui le sait reprend à son compte les contraintes du pouvoir ; il les fait jouer spontanément sur lui-même ; il inscrit en soi le rapport de pouvoir dans lequel il joue simultanément les deux rôles. »[239] Par conséquent, les gens deviennent les agents de leur propre soumission, du fait même que celui qui est soumis à la visibilité, et le sait, assume les contraintes du pouvoir et s'auto-surveille[240]. Foucault rajoute que dans un tel système le but est de faire en sorte « que la surveillance soit permanente dans ses effets, même si elle est discontinue dans son action ».[241] De là la conséquence ultime du Panopticon, celle « d'induire chez le prisonnier un état conscient et permanent de visibilité qui assure le fonctionnement automatique du pouvoir. »[242] Car si quelqu'un ne peut jamais être certain s'il est observé ou non, il va donc se comporter différemment que s'il était certain d'être seul (par exemple, les manières à table sont plus recherchées dans un restaurant que chez soi)[243]. Non seulement c'est une forme d'intrusion dans sa vie personnelle, mais en plus elle modifie la perception de ses propres actions[244] puisque ce système normalise les gens, comme s'ils étaient tous un risque potentiel. Chaque individu est ainsi constamment analysé selon un profil de risque[245].

D'ailleurs, il faut toujours garder à l'esprit que le panopticon est un modèle de prison, fait pour interner des criminels dangereux pour la société.

---

[239] Foucault, Michel. *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, 1975, p. 204.
[240] Reiman, *loc. cit.*, pp. 195-196.
[241] Foucault, *op. cit.* p. 202.
[242] *Idem.*
[243] Reiman, *loc. cit.*, p. 194.
[244] Benn, *loc. cit.*, pp. 4-6.
[245] Lyon, David. « 2 : Surveillance after September 11, 2001 ». In Webster, Frank et Kirstie Ball (sous la dir.), *The Intensification of Surveillance : Crime, Terrorism and Warfare in the Information Age*, Pluto Press, 2003, pp. 20-21.

Il ne peut être un modèle pour cette même société[246], puisque, selon cette logique, aucune liberté ne pourrait exister. Comme l'affirment Erin Shaw, John Westwood and Russell Wodell :

> Law enforcement... would be wonderfully efficient if there were no rights to privacy --- if all of the information about every citizen which is possessed by the state were centrally stored and easily accessible, if the agents of the state could at will search any person or home and seize any evidence which might relate to a crime, and bug any telephone or office. This is the description of a totalitarian state. Such sweeping powers of search and surveillance are not tolerated in a democratic society[247].

La surveillance technologique est basée sur un rêve que la technologie permettra, un jour, de tout savoir, d'être omniscient, car tout pourra être vu et su, rien ne pourra plus être caché et tout sera donc anticipé. Il doit ainsi y avoir toujours plus de surveillance[248]. C'est la sacralisation de la technologie que constatait Jacques Ellul il y a une trentaine d'années : « Ce n'est pas la technique qui nous asservit mais le sacré transféré à la technique ».[249]

Mais aussi, il y a déshumanisation. Traiter les êtres humains comme de la marchandise (avec le fameux code à barres qui est lu par un lecteur optique) ne peut être accepté en démocratie. Sans compter que les gouvernements autoritaires (la Chine et le Pakistan viennent à l'esprit) ne vont pas se gêner pour obliger les gens légalement, ou par la force si

---

[246] Reiman, *loc. cit.*, pp. 205-206.
[247] Tapscott, Don et Ann Cavoukian, *op. cit.*, pp. 17-18.
[248] Nellis, Mike, « 5 : 'They Don't Even Know We're There' : The Electronic Monitoring of Offenders in England and Wales ». In ». In Webster, Frank et Kirstie Ball (sous la dir.), *loc. cit.*, pp. 76-77.
[249] Ellul, Jacques, *Les nouveaux possédés*, Librairie Arthème Fayard, Paris, 1973, p. 259.

nécessaire, de donner leurs informations biométriques au nom de l'intérêt sécuritaire national. En Occident, certains gouvernements vont aussi dans le même sens[250]. Par exemple, en Grande-Bretagne, des pénalités financières seront exercées contre quiconque refuse de se soumettre au processus biométrique[251]. Et que se passe-t-il après ? Si les gens continuent de refuser de se soumettre ? Le gouvernement va-t-il les forcer ? Les emprisonner ?

Ayant abordé les dangers que représente le panopticon comme modèle général pour le fonctionnement de la société en général venant d'être abordés, l'analyse se poursuit en examinant les dangers qu'il pose plus précisément pour les droits individuels. Sur ce point, il faut commencer par la sphère publique. Beaucoup de gens disent que les endroits publics sont justement des endroits publics où il ne peut y avoir aucune forme d'atteinte de vie privée. Mais la notion de vie privée s'étend au-delà de la sphère privée à cause de l'omniprésence de la technologie. C'est parce que le sens même du concept de sphère publique a été modifié par les nouvelles technologies de l'information qui permettent beaucoup plus facilement de surveiller, d'obtenir, d'entreposer et d'analyser de l'information sur les gens ainsi que de faire du profilage que l'idée d'étendre, au moins partiellement, le droit à la vie privée dans l'espace public est justifié[252].

La technologie change aussi la sphère publique en enlevant par exemple l'anonymat public qui était la norme avant la technologisation de l'information. N'importe qui qui se promène dans les rues d'une ville est vu par des centaines, voire des milliers de personnes, sans perdre son droit à l'anonymat. Non seulement les gens n'ont vu qu'une partie du trajet de la

---

[250] Clarke, *loc. cit.*
[251] SA Mathieson, « Image problem », In *The Guardian*, 20 novembre, 2003, [en ligne], http://technology.guardian.co.uk/online/story/0,3605,1088437,00.html, (consulté le 5 juin 2006).
[252] Nissenbaum, *loc. cit.*, pp. 559-596.

personne en question et s'en souviendront subjectivement (par exemple, il sera vu comme une personne qui marchait bizarrement par l'un, ou plutôt comme un homme corpulent par un autre), mais la plupart du temps personne ne le remarquera réellement et même ceux qui le remarqueront finiront par l'oublier du fait que le cerveau humain a ses limites. Par contre, la technologie permet d'emmagasiner de l'information à un coût de plus en plus dérisoire, de créer des bases de données de plus en plus grandes et complexes, de traiter et de partager l'information de plus en plus rapidement avec une technologie qui permet théoriquement d'enregistrer un nombre d'informations illimitées et de l'analyser selon la portée voulue et d'emmagasiner le tout pour l'éternité[253].

Sur ce point, Helen Nissenbaum rejoint Peter Hope-Tindall, qui a travaillé sur les concepts de sphère publique et sphère privée qui sont, selon lui, souvent mal formulés. Comme Nissenbaum, il conteste la notion qu'il ne peut pas y avoir de vie privée dans des endroits qui relèvent de prime abord de la sphère publique[254]. Il a innové en écrivant qu'il faut garder en tête les notions d'observabilité (une personne doit s'attendre à être vue dans un lieu public), de capacité de lier (*linkability*) (Est-il possible de faire des liens entre les actions et l'identité d'un individu ? Non, car même s'il est possible de voir tout ce qu'il fait, il n'y a aucun nom auquel rattacher ses actions) et finalement, la notion d'anonymat ou pseudonymité (Il est peu probable qu'une personne qui en rencontre une autre sur la rue sache son nom et de toute façon, chacun pourrait prétendre être n'importe qui.). Donc, il reste une base d'attente de vie privée même dans les lieux publics[255]. De plus, les gens rencontrent des milliers de personnes dans la rue, ils les oublient tous, ce qui

---

[253] *Idem.*
[254] Hope-Tindall, *loc. cit.*
[255] *Ibid.*, diapositives #7 à 14.

n'est pas le cas d'une machine biométrique qui peut accumuler des milliards de données.

Et si la biométrie prend le dessus, alors il n'y a plus d'anonymat, il n'y a plus d'étrangers, les commerçants pourraient savoir tout de leur futur client avant même d'entrer dans le magasin, quelle est sa cote de crédit, etc. (notamment si les transactions se font biométriquement ou encore que les commerçants aient accès légalement ou illégalement aux bases de données)[256]. Ensuite, il y a une négation de l'anonymat mais aussi de la possibilité d'utiliser des pseudonymes. Ceci est important puisque le pseudonyme sert, entre autres, à protéger les gens contre les atteintes à leur vie privée et même dans certains cas de leur épargner des atteintes à leur intégrité physique (Si Salman Rushdie avait publié ses *Versets sataniques* sous un pseudonyme, il n'aurait pas à craindre pour le restant de ses jours de se faire tuer à cause de la fatwa de l'ayatollah Khomeyni.). En peu de mots, c'est une façon d'étendre la sphère privée, du moins en partie, dans la sphère publique. Car le pseudonyme est aussi nécessaire pour éviter la méfiance qu'engendre l'utilisation de l'anonymat afin de protéger la vie privée : il est souvent plus simple d'utiliser un faux nom plutôt que d'expliquer et justifier un refus de s'identifier.

De plus en plus, les organisations privées et publiques enregistrent et maintiennent des archives des transactions/interactions effectuées avec qui, quand et comment ces transactions ont eu lieu. Avec la biométrie, notamment avec la reconnaissance faciale, le seul fait de marcher dans la rue pourrait être enregistré dans une banque de données, à cause du coût toujours plus

---

[256] Agre, Phil, *Your face is not a bar code: arguments against automatic face recognition in public places*, Whole Earth, Hiver, 2001, [en ligne], http://www.findarticles.com/p/articles/mi_m0GER/is_2001_Winter/ai_81790171, (consulté le 29 mai 2006).

bas de cet entreposage de données[257]. Il y a à peine 20 ans, lorsque les données étaient écrites uniquement sur papier, cela aurait été impossible.

De plus, la violation de l'intimité des données personnelles va loin du fait que la biométrie est toujours envisagée comme une clé pour relier une personne à des banques de données et ne constitue pas seulement une forme d'identification ou d'authentification. Cela permet donc, à partir d'une seule empreinte digitale, d'accéder à toute la vie d'une personne[258].

Si la fonction sensorielle du contrôle de l'accès est plus évidente à cause de l'aspect de surveillance par caméras, il n'en reste pas moins que l'aspect du contrôle informationnel est très présent.

La biométrie et la lutte contre la criminalité et le terrorisme

Lorsque l'impact de la biométrie sur la pratique de la démocratie libérale doit être évalué, il faut toujours recourir au principe de la prudence, et se demander « pourquoi faudrait-il adopter cette technologie ? » et non pas « pourquoi pas ? ».

Commençons par les dangers que ce raisonnement fait peser sur la démocratie et sur la société en général. Certains affirment que seuls les criminels ou les gens qui ont quelque chose à cacher doivent craindre la biométrie, car seules les photos des criminels recherchés seront dans les bases de données. Cependant, il faut se demander si seuls les criminels seront dans ces bases de données, ou si, risque de glissement oblige, les catégories admissibles ratisseront de plus en plus large. Pourquoi les criminels ordinaires ne seraient-ils pas aussi inclus, puis ceux accusés mais

---

[257] *Idem.*
[258] Clarke, *loc. cit*

relâchés pour manque de preuve, ou encore ceux simplement suspectés d'un crime, ou tout simplement toute personne qui pourrait peut-être être un trouble-fête[259]. Certains pourraient même dire que c'est déjà le cas en se fiant aux séries policières américaines.

De plus, certains affirment « si vous n'avez rien à cacher... » pour justifier une diminution des libertés, mais si cela était mis en pratique systématiquement, la conséquence serait de donner le pouvoir aux policiers de lire les courriels et d'écouter les lignes téléphoniques de n'importe qui sans mandat, de fouiller leurs maisons de tous et chacun, etc. Ce raisonnement est l'argument de base de tous ceux qui veulent s'immiscer dans la vie privée des gens. La démocratie libérale ne voudrait plus rien dire si toute personne se promenant sur la voie publique pour aller à une rencontre privée devait divulguer son identité (ce qui est le cas si une identification à distance est possible). Si c'était le cas, comment les groupes de pression et les partis politiques d'opposition pourraient-ils s'organiser ou s'opposer au gouvernement[260]? D'ailleurs, n'importe qui a des choses qu'il préfère garder pour soi, ne serait-ce que la sexualité. Est-ce que les gens accepteraient des caméras dans leurs chambres à coucher ? Pourtant, rien d'illégal n'y est généralement fait. Même chose pour les salles de bains.

Même l'argument qui veut que de telles pratiques soient nécessaires pour combattre le crime ne tient pas, car une société libre doit placer des limites sur le travail des policiers. Si les policiers peuvent quand même traquer un individu en le faisant suivre par des policiers en civil, la capacité de répression sera exponentiellement plus grande avec des systèmes automatisés, avec toutes les dérives anti-démocratiques que cela

---

[259] Agre, *loc. cit.*
[260] *Idem.*

comporte[261]. Puisque dans un monde sans biométrie ou technologies de pistage sophistiquées (comme les caméras avec reconnaissance faciale), si une organisation comme le gouvernement voulait faire suivre chaque Québécois, il faudrait engager 7 millions de policiers, ce qui est impossible, cependant avec une implantation massive de la biométrie et des technologies de pistage, cela devient un scénario possible et faisable.

De plus, une autre affirmation sans fondement est qu'il faille trouver, à cause du terrorisme, un nouvel équilibre entre liberté et sécurité. Personne ne peut ignorer que la sécurité des individus est essentielle pour le bon fonctionnement de la démocratie et la jouissance des libertés. Cependant, une meilleure sécurité n'implique pas nécessairement moins de libertés[262]. Par exemple, en installant des portes plus résistantes dans les cockpits des avions il y aura une sécurité accrue sans nullement compromettre les libertés de personne.

Ensuite, plusieurs technologies biométriques sont associées à la criminalité (les empreintes digitales surtout, mais aussi pour plusieurs la prise de photos). De plus, les gens refusant de se soumettre à la biométrie pourraient être marginalisés par l'État[263], car beaucoup de gens et certains groupes pourraient refuser de se soumettre au système d'identification et d'authentification biométrique (pour des raisons idéologiques, religieuses, sociales ou autres) et formeraient donc un groupe d'exclus en dehors du système étant incapable d'accéder aux services de base (acte de naissance, santé, éducation et autres) offerts par l'État[264]. Dans la même lignée, les liens officiels et officieux entre les diverses organisations pourraient avoir comme

---

[261] *Idem.*
[262] *Idem.*
[263] Davies, *loc. cit.*
[264] *Idem.*

résultat que d'être en brouille avec une de ces organisations aurait pour conséquence d'avoir des problèmes avec toutes les autres organisations.

Ainsi, les autorités chinoises se sont servies des systèmes utilisés officiellement pour contrôler la circulation urbaine pour identifier et arrêter les étudiants ayant participé à la manifestation de la place Tienanmen en 1989, et que le régime a considérée comme criminelle[265].

Pour ce qui est des libertés individuelles, les dangers sont nombreux. Il y a d'abord le danger du vol d'identité puisque plus il y a de données biométriques dans des banques de données, plus les criminels pourront en faire des copies[266]. Comme l'ont démontré T. Matsumoto et al.[267] il est très facile, avec peu de moyens, de copier une empreinte digitale. Dans une vingtaine d'années, quand la technologie sera plus répandue, les criminels auront plus d'incitatifs à perfectionner les techniques de copiage biométrique. Car plus la biométrie sera utilisée, plus la valeur d'un vecteur biométrique augmentera et par le fait même la volonté des criminels et du crime organisé (ainsi que des terroristes) d'imiter, répliquer et voler ces vecteurs.

D'ailleurs, tout le monde laisse des traces biométriques partout et donc facilement visibles et vulnérables. À moins de porter des gants, les gens laissent des empreintes sur tout ce qui est touché. À moins de porter des lunettes miroitées, l'iris est facilement photographiable. Les gens laissent de l'ADN un peu partout, des cellules de peau, des cheveux, etc. La voix est enregistrable pour qui veut l'entendre. Le visage est visible pour tous. S'il est

---

[265] Coelle, Christopher, « Using and abusing iris recognition », In *Information Age*, 04/12/2003, [en ligne], http://www.infoage.idg.com.au/index.php/id;749011882;fp;4;fpid;866209206, (consulté le 9 juin 2006).
[266] Clarke, *loc. cit.*
[267] T. Matsumoto et al., *op. cit.*

facile de s'immuniser contre le vol d'identité en ne divulguant pas des renseignements personnels, en protégeant le NIP (Numéro d'Identification Personnel) utilisé dans les transactions électroniques et en payant comptant si nécessaire, il est beaucoup plus dur d'empêcher ce genre de vol avec la biométrie... À moins de se promener en burka, avec des gants et en refusant de parler à quiconque !

Ensuite, il y a le vol d'identité permanente, si une personne en personnifie une autre à plusieurs reprises, leurs deux « identités » vont fusionner puisqu'il y aura incapacité de faire la différence entre les deux. Et si aujourd'hui quelqu'un peut toujours se défendre en prétendant qu'un autre a pris des informations sur lui à son insu, il lui serait très difficile de prétendre que son doigt lui a été volé ! Toutes les compagnies clament haut et fort que la biométrie est sans faille. Donc si elle est vraiment sans faille, il n'est pas possible qu'une identité soit volée. De plus, si, aujourd'hui, il est toujours possible, au pire, de changer de compte de banque ou de NIP, il n'en sera plus de même pour un vol d'identité biométrique[268].

Surtout, ne pas maîtriser le contrôle de l'accès sensoriel (dans ce cas-ci, que les gens soient en mesure de priver, à tout de moins partiellement, les technologies biométriques (notamment les caméras) d'avoir accès à eux-mêmes afin de garder un certain anonymat ou pseudonymité) peut être lourd de conséquences, notamment parce que seulement être vu dans un quartier chaud ou en présence d'une personne peu recommandable pourrait porter préjudice. De plus, les conséquences d'un faux-positif peuvent être très sérieuses (par exemple, une caméra couplée avec un logiciel de reconnaissance faciale a faussement identifié un homme qui se promenait dans un quartier chaud comme M. Untel, mais ce n'était pas lui), surtout que

[268] *Idem.*

les faux-positifs sont très fréquents en biométrie (ombrage et luminosité entre autres)[269]. Il peut aussi y avoir le risque de stigmatisation. Par exemple, un homme de Tampa aux États-Unis a vu trois policiers débarquer à son lieu de travail pour l'accuser de négligence criminelle envers un enfant, malgré le fait qu'il n'avait rien à se reprocher (il n'était jamais même allé dans la ville où le crime a eu lieu). Cela est arrivé tout simplement parce que les policiers ont fait une démonstration d'un système biométrique aux médias locaux en utilisant cet homme comme cobaye involontaire (car il ne savait pas qu'il était filmé) et une femme pensait avoir reconnu son ex-mari qui avait criminellement négligé leurs enfants (l'homme de Tampa, en fin de compte, ne s'était jamais marié et n'avait jamais eu d'enfant non plus). Les policiers ont même abandonné le programme[270]. Et dans un cas beaucoup plus grave, Brandon Mayfield, avocat en droit familial dans le comté de Washington en Oregon, a été arrêté et détenu pendant des semaines après que trois experts du FBI (Federal Bureau of Investigation) ont conclu que ses empreintes digitales correspondaient à celle trouvée sur un sac contenant des détonateurs découvert le jour même des attentats de Madrid de 2004. Les trois experts étaient si certains de la concordance entre les empreintes digitales de M. Mayfield et celle du sac qu'ils l'ont qualifiée d'« absolument incontestable »[271]. En fait, un affidavit demandant l'arrestation de M. Mayfield et signé par enquêteur du FBI montre que les trois experts étaient certains de

---

[269] Agre, *loc. cit.*

[270] Dennis, Brady, « Ybor cameras won't seek what they never found », In *St. Petersburg Times*, 20 août 2003, [en ligne], http://www.sptimes.com/2003/08/20/Hillsborough/Ybor_cameras_won_t_se.shtml, (consulté le 15 mars 2006).

[271] Mnookin, Jennifer L., « The Achilles' Heel of Fingerprints », *Washington Post*, samedi 29 mai 2004, p. A27.

cette concordance à 100%[272]. Cela a pris plusieurs semaines avant qu'il ne soit innocenté de toute implication dans cette affaire[273].

Il est facile de voir que la vie privée est menacée tant dans ses fonctions de contrôle de l'accès informationnel que sensoriel.

Risque de glissement

Avant d'aller plus loin, il faut rappeler que le risque de glissement constitue le passage d'une situation donnée vers une situation non initialement prévue ou annoncée, et ce de façon insidieuse, dissimulée et progressivement.

Pour commencer, les gouvernements et les organismes privés ont toujours voulu pouvoir identifier correctement leurs citoyens/clients afin de permettre une meilleure efficacité (administrative, bureaucratique, contre les fraudes par exemple) et continuent à améliorer ces techniques. Il s'agit d'un processus conflictuel, puisque des contrôles souples amènent notamment des dédoublements et de la fraude tandis que des contrôles trop stricts sont impopulaires et certaines personnes peuvent chercher à les éviter. Ces contrôles peuvent concerner ce qu'une personne a en sa possession (permis de conduire), ce qu'elle sait (NIP) ou ce qu'elle est ou fait (biométrie). Mais ils mettent tous en péril l'individualité des gens, car les organisations publiques et privées exercent de plus en plus de contrôles. Cette situation porte le risque de glissement, dont l'histoire de l'identification et de l'authentification est remplie. Par exemple, la carte d'assurance sociale est officiellement aux

---

[272] The Smoking Gun, *FBI Admits Fingering Wrong Man*, [en ligne], http://www.thesmokinggun.com/archive/0525041mayfield3.html, (consulté le 17 mars 2007).
[273] Mnookin, Jennifer L., « The Achilles' Heel of Fingerprints », *Washington Post*, samedi 29 mai 2004, p. A27.

seules fins d'interactions avec le ministère du Revenu, mais une foule d'autres organismes et d'entreprises demandent ce numéro. Ce n'était pas, du moins officiellement, l'idée de départ mais cela a évolué en ce sens. Cela s'est produit aussi dans le cas de la carte d'assurance-maladie et du permis de conduire. Il serait surprenant que la biométrie, un moyen jugé plus sûr pour l'identification et l'authentification que les cartes, ne suive pas la même tendance[274].

La banque d'ADN en Grande-Bretagne offre un bon exemple de ce danger de glissement que comporte le recours à la biométrie. En 1984, il y avait deux types de prélèvement d'ADN, ceux qui étaient considérés comme intimes (les prises de sang, les échantillons de sperme, d'urine, de salive, etc.) et qui devaient obligatoirement se faire avec le consentement du suspect, et les prélèvements non intimes, par exemple, ceux des cheveux, et qui pouvaient être faits sans consentement. Dans ce dernier cas, seul un commissaire de police était autorisé à les faire, et seulement sur des individus soupçonnés d'avoir commis des crimes graves (*serious arrestable offence* - meurtre, viol et autres crimes graves). De plus, ces prélèvements ne pouvaient se faire que s'ils étaient pertinents à l'enquête et l'information génétique ne pouvait être utilisée qu'aux seules fins de cette enquête. Si l'individu en question n'était pas reconnu coupable, ses empreintes digitales, son empreinte génétique et les prélèvements étaient détruits[275]. Mais en une décennie, les choses ont changé avec l'adoption de la *Criminal Justice and Public Order Act* de 1994. D'abord, la catégorie « non intime » a pris beaucoup plus d'ampleur du fait que des prélèvements considérés comme intimes sont maintenant classés comme non intimes, c'est le cas de la salive

---

[274] Davies, *loc. cit.*

[275] Privacy International, *UK Early Beginnings of the DNA Database*, [en ligne], http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-508123, (consulté le 1er février 2007).

par exemple. En outre, l'ADN, même celle qui relève de l'intimité, peut être prélevée sans consentement si quelqu'un est accusé de presque n'importe quel crime et non seulement pour les crimes graves (*recordable offence* au lieu de *serious arrestable offence*).

Ensuite l'information ainsi obtenue peut être utilisée de façon spéculative (et non aux seules fins de l'enquête) et le profil d'un accusé peut être comparé à d'autres profils passés, présents ou futurs dans la banque d'ADN. En cas d'acquittement, les policiers n'ont plus l'obligation de détruire les prélèvements, les empreintes génétiques et digitales, mais ne peuvent plus utiliser l'information contre la personne dans le futur[276]. En 1997, la *Criminal Evidence (Amendment) Act* rend le prélèvement d'ADN rétroactif pour certains crimes commis par des criminels encore en prison[277]. En 2001, la *Criminal Justice and Police Act* permet aux policiers de garder pour toujours tous les profils génétiques qu'ils ont obtenus, même de ceux qui n'ont jamais été accusés de quoi que ce soit ou qui ont été acquittés. Ces profils font dorénavant partie de la banque de données, qui est consultée chaque fois qu'un échantillon d'ADN est retrouvé sur le lieu d'un crime. Les prélèvements avec consentement n'exigent plus la supervision d'un commissaire de police et dans le cas de ceux sans consentement, un simple inspecteur suffit[278]. Enfin, la *Criminal Justice Act* de 2003 facilite le prélèvement d'ADN de façon plus générale et plus particulièrement chez les

---

[276] Privacy International, *UK Expands DNA Database through the Criminal Justice and Public Order Act 1994*, [en ligne], http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-508126, (consulté le 1er février 2007).

[277] Privacy International, *UK retrospectively applies DNA profiling in the Criminal Evidence (Amendment) Act 1997*, [en ligne], http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-508125, (consulté le 1er février 2007).

[278] Privacy International, *UK DNA Database includes the innocent and wrongly accused under the Criminal Justice and Police Act 2001*, [en ligne], http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-508140, (consulté le 1er février 2007).

moins de 18 ans. Si, autrefois, un suspect devait être accusé d'un crime pour que les autorités obtiennent son ADN, aujourd'hui il suffit que la police arrête quelqu'un pour le forcer à fournir son ADN même si les accusations portées sont abandonnées ou que la personne est acquittée de ces accusations, ce qui alimente les accusations de *Privacy International*, un organisme de défense de la vie privée, qui soutient que le gouvernement britannique veut créer furtivement une banque d'ADN contenant les profils génétiques de tous ses citoyens. Les chiffres tendent à soutenir cette dernière hypothèse, du fait que de l'année 2000-2001 à 2005-2006, le nombre de profils d'ADN est passé de 1 186 000 à 3 596 000, de ce nombre 685 748 sont les profils d'adolescents de 10-17 ans, dont 24 000 qui n'ont jamais été accusés de quoi que ce soit, et 139 463 concernent également des gens contre qui la police n'a jamais porté d'accusation[279].

Plus précisément sur les dangers que cela pose aux droits individuels il faut noter qu'avec l'inter-connexion des banques de données et des contrôles biométriques, le pistage et la capture biométrique clandestine deviennent des possibilités. Pistage en temps réel, par exemple, un individu pourrait être suivi au gré des caméras de surveillance avec reconnaissance faciale. Mais aussi la capture biométrique clandestine, car si quelqu'un assiste à un rassemblement politique, les visages de tous ceux présents pourraient être identifiés puis inscrits sur la liste gouvernementale des personnes à surveiller (*reverse engineer*)[280]. Alors, étant donné que les vecteurs biométriques doivent être visibles pour être analysés (le visage et l'iris par exemple), certains pourraient obtenir ces vecteurs sans le consentement des personnes et ainsi forcer les gens à perdre leur anonymat,

---

[279] Privacy International, *UK DNA Database to grow dramatically under the Criminal Justice Act 2003*, [en ligne], http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-508144, (consulté le 1er février 2007).
[280] Woodward John D. Jr. *op. cit.*, pp. 7 à 9.

car ils pourraient être reconnus par un système sans leur consentement[281]. Il faut prendre en compte que ce genre de choses porte atteinte à la liberté de rassemblement qui est une liberté individuelle et publique si importante.

Une fois le système en place pour trouver des terroristes, comment justifier qu'il ne cherche pas non plus les criminels violents recherchés, ensuite les autres criminels, puis pourquoi pas tous ceux qui ont un dossier criminel (il pourrait y avoir des récidivistes), ensuite ceux qui n'ont pas payé leurs contraventions, etc. ? La présomption que quiconque marche dans la rue est innocent jusqu'à preuve du contraire n'existerait plus[282]. Par conséquent, la présomption d'innocence, la pierre angulaire de la justice occidentale, ne serait plus. Il y a également la possibilité d'une négation automatique de ce droit à la présomption d'innocence, puisqu'une compagnie ou un gouvernement pourrait interdire l'accès à certains endroits (ou certains moyens de transport) à des gens soupçonnés d'être des agitateurs ou de fauteurs de troubles (par exemple, quelqu'un est biométriquement identifié dans une manifestation)[283]. En fait, il est possible de constater que c'est déjà le cas pour certains événements sportifs européens, surtout les matchs de soccer.

Il est devenu impossible de se soustraire à la biométrie. Même si les nombreux projets de surveillance par caméras dans les lieux publics vont avertir les gens qu'ils sont filmés, une affiche ne permet pas d'acquérir le consentement d'une personne du fait que parfois les gens sont obligés de passer par des endroits surveillés, ne serait-ce que les ponts et le métro. Et même les magasins, souvent très concentrés en seulement quelques grandes entreprises commerciales, sont tous très surveillés, donc le

---

[281] Prabhakar Salil, Sharath Pankanti et Anil K. Jain, *loc. cit.*, p. 41.
[282] Ackerman, *loc. cit.*
[283] Clarke, *loc. cit.*

consommateur n'a pas nécessairement le choix d'aller ailleurs. Il s'ensuit que la liberté individuelle de mouvement en est entachée.

Un cas intéressant sur ce point est celui de la ville de Middlesbrough, en Angleterre, qui a commencé à équiper ses 158 caméras de surveillance, sept pour l'instant, avec des haut-parleurs permettant aux préposés aux caméras d'interpeller les gens qui sont surpris à faire des actes considérés comme anti-sociaux, par exemple de jeter un papier par terre. Le but est de dissuader les gens d'avoir certains comportements et ainsi de modifier le comportement des gens. Si l'expérience s'avère positive, elle pourrait s'étendre aux secteurs résidentiels. Étonnant est le peu de résistance rencontrée par ce projet, les autorités affirmant n'avoir reçu aucune demande de retrait des caméras. Ceci en plus des réactions de certains qui se sentent rassurés par la présence de ces caméras de surveillance[284].

Une autre ville, celle de Shoreditch, aussi en Angleterre, a eu comme idée de faire participer ses citoyens à leur propre surveillance. Le projet en question, rapidement baptisé ASBO-TV par la population (*Anti-Social Behaviour Order - TeleVision*), va permettre à ses résidents d'avoir accès, par leur téléviseur, à quelque 400 caméras de surveillance. D'abord restreint à 1000 résidents de Haberdasher et des immeubles Charles Square à titre de projet pilote, il sera ensuite étendu à plus de 20 000 foyers dans toute la ville de Shoreditch[285].

---

[284] Daily Mail, *Big Brother is shouting at you*, 16 septembre 2006, [en ligne], http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=405477&in_page_id=1770, (consulté le 1er mai 2007).

[285] BBC News, *Rights group criticises 'Asbo TV'*, [en ligne], http://news.bbc.co.uk/1/hi/england/london/4597990.stm, (consulté le 1er mai 2007).

L'originalité du projet réside dans son interactivité : les téléspectateurs pourront épier les rues de leur ville à la recherche de « voyous » dont les photos défileront à la télévision. Les téléspectateurs pourront dénoncer par courriel et de façon tout à fait anonyme les actes anti-sociaux, les infractions aux ordonnances ASBO ou les crimes dont ils sont témoins depuis leur sofa. C'est une question d'assurer la sécurité de tous clament les autorités, malgré que certains pensent qu'au contraire cela va aider les criminels, notamment en leur permettant de pouvoir savoir si les occupants d'une maison sont présents avant d'y commettre un vol[286].

Un simple abonnement au coût de 3,50£ par semaine permet d'avoir accès à tous les services inclus dans ce projet dont un appareil permettant à une télévision de recevoir les 55 canaux de ASBO-TV, un service de téléphonie locale à rabais, ainsi qu'un accès à internet haute vitesse[287].

Et même lorsque les autorités commettent des erreurs, il n'y a pas de scandales ni de réactions vigoureuses de la part de la population. Par exemple, le jour où les autorités annonçaient leur plan d'étendre leur projet de surveillance à 20 autres centres-villes, les autorités de Middlesbrough ont été obligées de s'excuser auprès d'une femme victime des nouvelles caméras de surveillance parlantes. En effet, une jeune mère de famille a été réprimandée par une caméra malgré qu'elle n'avait rien à se reprocher. Le préposé à la caméra pensait qu'elle venait de jeter un déchet par terre et l'a apostrophée en ce sens. De plus, cette scène où elle « salissait » la voie publique a été montrée au journal télévisé. Malgré tout, elle ne remet pas en

---

[286] Swinford, Steven, « Asbo TV helps residents watch out », In *Times Online*, 8 janvier 2006, [en ligne], http://www.timesonline.co.uk/tol/news/uk/article786225.ece, (consulté le 2 mai 2007).
[287] *Idem*.

cause les caméras, car elles sont rassurantes. Même chose pour les autorités qui sont tellement impressionnées qu'ils vont étendre le système aux villes des alentours au coût de 500,000£[288].

En plus, si la biométrie est permise ici, dans les démocraties, il n'est que plus probable que les gouvernements autoritaires vont aussi adopter cette technologie, notamment les Chinois qui ne tolèrent aucune dissidence politique[289].

La biométrie menacerait aussi le fonctionnement même de la démocratie. En premier lieu, il y a danger de violation du caractère privé du comportement des gens puisque l'utilisation de la biométrie, dans la plupart des cas, requiert l'installation de nombreuses caméras qui surveilleront donc les actions des gens, ce qui a pour effet d'instaurer un état prévisibilité des actions des citoyens face à l'État. L'État et ses agences pourraient anticiper dès lors ce que les gens feront et intervenir en conséquence, ou encore partager ces informations avec des partenaires privilégiés comme certaines organisations ou les entreprises privées[290]. Et la prévisibilité des citoyens par rapport à l'État n'est pas compatible avec une démocratie du fait que c'est la négation même du concept de sphère privée qui est un droit individuel crucial dans une démocratie.

De la même façon, le recours à la biométrie peut avoir un effet débilitant sur la démocratie et les libertés. La surveillance par biométrie n'est pas utilisée seule, elle fait partie d'un ensemble de mesures complémentaires

---

[288] Wainwright, Martin, « Talking CCTV cameras accuse wrong person », In *The Guardian*, 12 avril 2007, [en ligne], http://society.guardian.co.uk/crimeandpunishment/story/0,,2055057,00.html, (consulté le 3 mai 2007).
[289] Agre, *loc. cit.*
[290] Clarke, *loc. cit.*

que le gouvernement met ou voudrait mettre en place. Par exemple, le gouvernement canadien lors des consultations sur son projet de loi « accès légal » aurait voulu que les services de sécurité gouvernementaux (les policiers, le SCRS et les autres agences d'application de la loi) puissent exiger des fournisseurs de services internet d'avoir tous les renseignements disponibles sur un client, et ce, sans mandat judiciaire. De plus, le gouvernement aurait voulu créer une « base de données nationale sur les abonnés » aux services de télécommunications tels que l'internet et obliger les compagnies à recueillir des renseignements précis sur les clients afin de faciliter le travail des forces de l'ordre dans la répression de la criminalité qui utilise de plus en plus l'internet dans ses activités[291]. De telles pratiques risquent de créer un monde contrôlé où, par peur de perdre l'accès à un service, de perdre une perspective d'emploi, d'être fichés par le gouvernement ou face à d'autres perspectives peu reluisantes, les gens pourraient exercer de moins en moins leurs droits de manifester, contester ou critiquer. Dans une telle situation, ce serait les bases mêmes de la démocratie, qui fait l'exaltation des libertés et des droits, qui seraient attaquées. L'Occident a décrié l'univers *Big Brotherien* qu'était l'Union soviétique où l'État savait et voulait tout savoir sur tout. Mais la biométrie pourrait donner aux gouvernements la possibilité de faire pire que les Soviétiques[292].

Mais cela ne devrait pas surprendre du fait que le danger de glissement semble, selon plusieurs, inévitable car les gouvernements veulent

---

[291] Commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, *Réponse à la consultation du gouvernement sur l'accès légal : Présentation du Commissariat à la protection de la vie privée du Canada au ministre de la Justice et procureur général du Canada*, 5 mai 2005, Ottawa (Ontario), [en ligne], http://www.privcom.gc.ca/information/pub/sub_la_050505_f.asp, (consulté le 3 octobre 2006).

[292] *Idem.*

de plus en plus d'interopérabilité, c'est-à-dire la capacité de plusieurs systèmes d'être compatibles au point de pouvoir communiquer et travailler ensemble, ne serait-ce que pour échanger des renseignements dans la lutte au terrorisme et à la criminalité internationale[293].

L'île Ayers montre peut-être l'avenir de la biométrie, l'ultime étape du risque de glissement, celle de l'automatisation de l'identification. Une ancienne usine située à Orono dans le Maine aux États-Unis sera saturée de caméras, de capteurs et de détecteurs. Le tout contrôlé par un système d'intelligence artificielle (IA) qui analysera cet univers et inspectera chaque personne qui entre sur île. Si la personne vient souvent, l'IA s'en souviendra. Et si une personne cherche à éviter les caméras, l'IA lui portera une attention particulière. Le but est de démontrer qu'il est possible pour un État, avec les caméras et l'IA, de tout savoir et de tout comprendre au sujet de tous les individus concernés et en tout temps[294]. Et comme les gens ont tendance à modifier leur comportement lorsqu'ils se sentent surveillés, ils risquent de se comporter de façon à refléter ce qu'ils pensent être la norme sociale. Il y aurait donc la possibilité de plus en plus de discriminations envers ceux qui n'acceptent pas de changer leur comportement[295]. Ceux qui pensent à une simple expérimentation devraient savoir que, selon les responsables du projet, cette petite expérience servira de démonstration de ce que sont capables de faire ces technologies pour la *homeland security*[296].

Il y a un risque très réel que les gens faisant partie d'une minorité idéologique ou sociale ou ceux qui expriment simplement des opinions politiquement incorrectes, soient opprimés. Par exemple, une femme en

---

[293] Thomas, *loc. cit.*
[294] Baard, Mark, « Big Brother to Watch Over Island », In *Wired*, [en ligne], http://www.wired.com/news/privacy/0,1848,63316,00.html, (consulté le 6 juin 2006).
[295] *Idem.*
[296] *Idem.*

Corée du Sud, qui a refusé de nettoyer les excréments de son chien dans le métro, a été prise en photo par un homme sur son téléphone portable. Un lynchage populaire médiatique s'en est suivi, et cette femme est devenue bien malgré elle un symbole national très négatif[297].

Mais si la technologie accélère le glissement, il y a aussi ce qui peut être qualifié de montées subites de l'implantation de technologies liberticides qui sont l'introduction très rapide et en très peu de temps de nouvelles technologies à un moment où le public ne peut débattre de ces technologies du fait que des événements traumatisants sont encore trop récents et émotifs. Cependant, il faut noter que ces montées subites ne font que légitimer des tendances qui étaient là avant l'événement déclencheur[298]. Le meilleur exemple de ce phénomène est le 11 septembre aux États-Unis ou encore le meurtre de Jamie Bulger en Grande-Bretagne en 1993, deux événements traumatisants qui ont tous deux permis l'implantation de technologies potentiellement liberticide sans susciter de réels débats[299].

Le risque de glissement est probablement un des aspects les plus inquiétants de l'implantation de la biométrie. Devant un tel risque de glissement, une étude de cas serait de rigueur.

---

[297] Yang Catherine, Kerry Capell et Otis Port, *loc. cit.*

[298] Wood, David, Eli Konvitz et Kirstie Ball, « 8 : The Constant State of Emergency? : Surveillance after 9/11 », In Webster, Frank et Kirstie Ball (sous la dir.), *loc. cit.*, p. 141.

[299] Jamie Bulger est un enfant de 2 ans qui a été enlevé puis tué en février 1993 par deux autres enfants de 10 ans, Jon Venables et Robert Thompson. Pour un dossier sur le sujet, voir : Scott, Shirley Lynn. *The Death of James Bulger*: Tragic Child Abduction Caught on Tape, [en ligne], http://www.crimelibrary.com/classics3/bulger/, (consulté le 20 mars 2007).

Étude de cas : l'utilisation du numéro d'assurance sociale aux États-Unis

Aucun exemple ne pourrait mieux illustrer le phénomène du risque de glissement que l'instauration du numéro d'assurance sociale (NAS) aux États-Unis. Initialement prévu aux seules fins de gestion des pensions de retraite, ce numéro est devenu, en moins de 75 ans, un identifiant universel pour chaque citoyen Américain du berceau jusqu'au tombeau, une carte obligatoire et indispensable dont les usages et les ramifications n'ont de limite que l'imagination des législateurs.

Partant, en 1935, de l'idée que le gouvernement allait prélever une certaine partie du salaire de ses citoyens et faire fructifier ces fonds pour assurer les vieux jours de ses concitoyens, la carte d'assurance sociale (CAS) s'est vite transformée en pièce d'identité par défaut, malgré le fait que, à l'origine, elle devait simplement identifier les citoyens qui voulaient accéder à leur pension[300].

C'est Franklin D. Roosevelt, en 1943, qui fera augmenter de façon considérable le risque de glissement. Il promulgue en novembre 1943 l'ordre exécutif n° 9397 qui stipulait que désormais les départements et les agences fédérales qui voulaient établir un nouveau système permanent et numérique pour l'identification des employés devaient absolument utiliser le NAS[301].

Mais c'est avec l'informatisation que ce décret prend toute son importance. En 1961, la *Civil Service Commission* ordonne l'utilisation du NAS pour identifier ses employés. L'IRS (*Internal Revenue Service*)

---

[300] Twight, Charlotte, « 11 : Systematic Federal Surveillance of Ordinary Americans ». In McElroy, Wendy et Carl Watner (sous la dir.), *National Identification Systems : essays in Opposition*, McFarland & Compagny, Inc., 2004, pp. 151-152.
[301] *Idem.*

commence à se servir du NAS pour l'identification des contribuables en 1962. Et en 1967, c'est le ministère de la Défense qui y a recours pour identifier son personnel militaire[302].

En 1972, le Congrès modifie la *Social Security Act*, de sorte que le NAS sera désormais utilisé pour identifier les bénéficiaires de programmes fédéraux et les immigrants. Plus tard, ce numéro sera appliqué dans le cas du *Medicaid* (qui est le programme gouvernemental d'assurance-maladie pour les gens à faibles revenus), de l'aide aux familles (*Aid to families with Dependent Children*), des coupons contre nourriture (*food stamps*), des prestations pour les programmes à la nutrition scolaire (*school lunch program benefits*), des prêts fédéraux, et d'un grand nombre d'autres programmes sociaux.[303]

En 1970, la loi sur le secret bancaire (*Bank Secrecy Act*) est modifiée pour obliger les institutions financières à identifier leurs clients. Elles choisiront d'utiliser le NAS[304]. Ces mêmes institutions devront aussi conserver et archiver les informations sur les transactions de leurs clients, microfilmer tous les chèques ou autres documents de transaction identifiant toutes les parties aux transactions[305].

---

[302] *Idem.*
[303] *Idem.*
[304] *Idem.*
[305] *Ibid.*, pp. 170-173

Même la « *Privacy Act*[306] » de 1974[307] n'y change rien, car cette loi exempte le gouvernement fédéral de l'interdiction d'exiger le NAS et permet même la divulgation de renseignements obtenus par le gouvernement fédéral si ceux-ci sont obtenus à des fins d'utilisation routinière[308] (« The agency may only disclose such information if it has permission from the individual or if it can meet one of the twelve following conditions : [...] 3. The disclosure is for a "routine use" »[309]).

En 1976, le Congrès donne le feu vert aux États de pouvoir se comporter exactement comme le gouvernement fédéral. Ils peuvent désormais utiliser le NAS pour les permis de conduire, les programmes sociaux et l'enregistrement des véhicules notamment[310].

Le risque de glissement est très bien illustré par l'obligation de donner le NAS pour obtenir un permis de conduire (un champ de compétence qui relève pourtant de chaque État) qui est cachée dans une loi fédérale omnibus de 749 pages, la *Omnibus Consolidated Act of 1997*. Par ailleurs, la section 656(b) de la *Immigration Reform Act* stipule que le gouvernement fédéral n'acceptera pas comme pièce d'identité les permis de conduire ou autres

---

[306] Electronic Privacy Information Center, *The Privacy Act of 1974*, [en ligne], http://www.epic.org/privacy/1974act/, (consulté le 19 mars 2007).

[307] Cette loi a été adoptée par le Congrès suite aux abus de l'administration Nixon. Elle a pour but de protéger la vie privée en créant quatre droits pour le citoyen. D'abord celui de savoir quelles informations le gouvernement et ses agences détiennent sur lui. Ensuite que lors de la collecte et de la gestion de l'information personnelle sur les gens que les agences et le gouvernement appliquent les principes d'une pratique juste eu égard à l'information (*fair information practices*). Puis cette loi impose des contraintes sur la possibilité des agences de transmettre les données personnelles qu'elles ont. Finalement, elle donne la possibilité aux gens de poursuivre en justice le gouvernement s'il viole les protections à la vie privée contenues dans cette loi. Cependant, cette loi contient aussi beaucoup d'exceptions où le respect de la vie privée ne prime plus ou n'est plus aussi important, notamment pour les agences d'application de la loi.

[308] Twight, *loc. cit.* pp. 151-152.

[309] Electronic Privacy Information Center, *loc. cit.*

[310] Twight, *loc. cit.* pp. 151-152.

documents, à moins qu'ils ne satisfassent aux exigences fédérales, c'est-à-dire qu'ils utilisent le fameux numéro d'assurance sociale[311].

Et si, autrefois, une personne n'obtenait un NAS que lors de son premier emploi, de nos jours même les enfants doivent en obtenir un dès la naissance ou peu après. Et c'est encore le risque de glissement qui est très manifeste : en 1986, le Congrès exige que les enfants à charge obtiennent un NAS avant d'atteindre cinq ans. En 1988, cet âge a été abaissé à deux ans. En 1996, le critère de l'âge a été éliminé. Maintenant, le gouvernement a des programmes dans les 50 États où la demande d'acte de naissance se fait en même temps que celle de la carte de NAS[312].

Le même genre de tendance se retrouve à la *Social Security Administration* (SSA) qui est l'agence qui s'occupe du NAS, de l'émission de nouveaux numéros, de la gestion du NAS et des prestations qui y sont reliées et qui est, en principe, la responsable du glissement qui a été effectué avec le NAS. La *Social Security Administration* partage allègrement toutes les informations qu'elle détient avec une multitude d'agences et de ministères. Par exemple, le gouvernement fédéral, les États, les agences locales qui gèrent l'aide aux familles, le *Medicaid*, le département des vétérans, l'agence de l'immigration et de la naturalisation, la commission des retraites du chemin de fer, et, évidemment, l'IRS[313]!

Quelles sont les informations partagées ? La race, le sexe, les autres caractéristiques physiques, l'état matrimonial, le salaire, les données financières, le NAS, les adresses, les numéros de téléphone, l'information

---

[311] *Ibid.*, pp. 153-154.

[312] *Ibid.*, p. 153.

[313] *Ibid.*, pp. 153-154.

médicale, les rapports psychologiques et psychiatriques, les relations familiales et autres.[314]

Donc même à l'intérieur du risque de glissement primaire, il y en a un secondaire et même un tertiaire. Un glissement peut ainsi en engendrer un autre dans son sillage. Par exemple, le *Child Support Enforcement* (CSE, créé en 1974) a pour mission de trouver les parents qui sont en retard sur leurs paiements de pension alimentaire. En 1976, ils reçoivent l'autorisation de fouiller dans toutes les banques de données fédérales et des États avec l'aide du NAS. Puis, ils obtiennent l'accès aux banques de données de l'IRS. Un directeur de la CSE a même avoué : « Some people would say that's Big Brotherism. Well, it is. ». Car toutes les unités de la CSE ont accès au localisateur de parent du gouvernement fédéral (le *Federal Parent Locator Service* est une agence fédérale qui s'occupe des problèmes reliés au non-paiement des pensions alimentaires notamment afin retrouver les « mauvais payeurs », mais aussi, dans le même domaine, pour la coordination et les statistiques entre autres.)[315].

En conclusion sur le NAS, cette étude de cas a montré à quel point une simple mesure peut prendre, en quelques décennies, des proportions inimaginables par rapport à son but d'origine. De là l'importance de tenir compte du risque de glissement.

Dorénavant, il est facile de constater les impacts négatifs que la mise en œuvre de technologies de type biométrique aurait sur l'espace privé, mais aussi sur la démocratie en tant que telle. Que ce soit le danger des banques de données, la panopticonisation de la société, la normalisation des comportements due à l'état de visibilité permanente ou encore la perte de

---

[314] *Idem.*
[315] *Idem.*

l'anonymat. De plus, l'étude de cas sur le numéro d'assurance sociale aux États-Unis démontre parfaitement que les risques de glissement sont énormes et probablement inévitables si la biométrie est implantée. Avec le cadre analytique, il est possible de conclure que l'usage généralisé de la biométrie n'est pas compatible avec une démocratie libérale qui respecte le droit à l'espace privé de chacun de ses citoyens.

Conclusion

En résumé, ce mémoire porte sur la biométrie selon une double perspective : les instruments de cette technologie rehaussent-ils significativement le niveau de sécurité et quels sont leurs impacts sur la démocratie libérale et plus spécifiquement sur la sphère privée. L'outil pour analyser cette question est le contrôle de l'accès qui est duel, c'est-à-dire le contrôle informationnel et le contrôle sensoriel sur les frontières personnelles.

Et en conclusion, il ne fait pas de doute que la biométrie a un impact significativement négatif sur le fonctionnement de la démocratie libérale puisqu'elle restreint de manière flagrante le contrôle de l'accès. La biométrie ne permet pas de rehausser, bien au contraire, la capacité des citoyens à contrôler leur accès informationnel du fait que la biométrie n'est pas et ne pourra vraisemblablement jamais être fiable et ne peut pas mieux protéger, par exemple les banques de données, que ne le feraient des procédures de sécurité plus simples et déjà existantes (anti-virus, anti-logiciel espion, pare-feu, forcer les mots de passe à avoir plus de 10 caractères alpha-numériques, ainsi que d'autres mesures simples mais efficaces). De plus, la possibilité pour le citoyen de contrôler son accès sensoriel s'en trouve sévèrement diminuée, car s'il est possible de cacher son NIP au fond de sa mémoire, il est impossible de cacher toutes les caractéristiques physiques (physiologiques) de ce même citoyen. Après tout, tout le monde laisse leurs empreintes digitales un peu partout (crayons, claviers, bouteilles d'eau, poignées de porte et autres objets de la vie de tous les jours et ces empreintes peuvent être prélevées), le visage est visible pour qui veut le voir (et par conséquent le photographier), des cheveux et des bouts de peau

remplis d'ADN sont laissés partout (et ainsi utilisable par « amplification en chaîne par polymérase »), l'iris est très visible, donc photographiable et ainsi de suite pour tous les aspects biométriques de l'Homme. Si la biométrie est la clé à des banques de données ou pour les transactions quotidiennes, l'assurance que les gens ont de pouvoir contrôler l'accès sensoriel et informationnel à eux-mêmes s'en trouve pratiquement éliminée à moins qu'ils se promènent en burka et encore...

De plus, la démocratie libérale ne peut fonctionner correctement que si les gens peuvent exprimer leurs préférences (idéologie, parti politique, idées) sans craindre de représailles. Mais il a été montré l'effet débilitant de la biométrie qui entraîne l'effet de visibilité permanente, c'est-à-dire que la possibilité d'être surveillé à tout moment entraîne une conformité et un contrôle social inégalé. Puisque lorsque quelqu'un se sent surveillé, il modifie son comportement pour agir selon sa perception de la normalité. Mais si chacun normalise ses comportements comme s'il devait se reprocher quelque chose, est-ce que la démocratie libérale fonctionne toujours, avec les nécessaires dissidences et oppositions qui la caractérisent ? La réponse est non et c'est pour cela que l'extension de la sphère privée, du moins partiellement, dans ce qui était traditionnellement la sphère publique est légitime, car la technologisation de la société rend plus facile la surveillance classique mais aussi de masse, en brouillant les concepts d'observabilité, de capacité de lier (*linkability*) et de pseudonymité qui relève du contrôle de l'accès sensoriel.

Aussi, est-ce qu'une démocratie libérale peut vraiment fonctionner avec le raisonnement fallacieux du « si vous n'avez rien à cacher... » ? D'abord, personne ne veut de caméra dans les chambres à coucher et c'est parfaitement légitime même si c'est caché. Mais plus profondément, c'est un

raisonnement plus compatible avec un État policier puisque l'État libéral garantit à ses citoyens un certain nombre de droits inaliénables dont la sphère privée. Car dans une dictature, tout relève du domaine public du fait qu'il n'y a pas de reconnaissance de l'individu comme ayant une vie propre mais seulement une vie dans les institutions de la dictature. Une démocratie libérale non seulement reconnaît que chacun possède sa propre vie et peut faire ses propres choix mais que c'est l'agrégation de ces préférences qui détermine les actions du gouvernement et c'est du respect des droits et choix des citoyens que l'État libéral tire sa légitimité. L'absence de la sphère privée et donc du contrôle de l'accès informationnel et sensoriel ne peut que diminuer les critiques sociétales et les opinions dissidentes. Cela totalitarise la société du fait que conformité et élections (et par conséquent démocratie) ne vont pas ensemble[316].

Finalement, il y a un risque de glissement très nuisible pour le fonctionnement de la démocratie libérale à cause que la présomption d'innocence et le fardeau de la preuve, principes primordiaux à la démocratie, pourraient être renversés. En comparant, par exemple avec un logiciel de reconnaissance faciale, tous les visages qu'une caméra capte à un registre des criminels recherchés, c'est la présomption d'innocence qui est en jeu. Il y a aussi l'impossibilité de se soustraire à la plupart des contrôles biométriques, par exemple la caméra ne demande pas la permission de la personne qu'elle filme et il est parfois impossible ou très encombrant de faire un détour pour l'éviter. Et si l'univers de l'île Ayers devient une réalité, se soustraire à la biométrie deviendra impossible, surtout que l'IA porte spécifiquement son regard sur ceux qui cherchent à maintenir leur vie privée, ce qui est très troublant étant donné les dangers de normalisation et d'atteinte à la présomption d'innocence que cela comporte. Le meilleur exemple de

[316] Reiman, *loc. cit.*, p. 208.

glissement qui doit pousser à la prudence reste l'étude de cas avec le numéro d'assurance sociale qui est passé en moins d'un siècle d'un simple moyen d'identification pour un régime de retraite à un moyen d'identification universel.

Le fardeau de la preuve pourrait aussi être inversé et la preuve en est le vol d'identité, car la biométrie étant considérée comme pratiquement parfaite, la bonne foi des victimes pourrait ne plus être présumée ce qui n'augure rien de bon pour une démocratie. Quelqu'un qui prétend que son NIP lui a été subtilisé avec une caméra cachée aura probablement le bénéfice du doute de sa banque puisque c'est quelque chose de plausible, mais pas si cette même personne prétend que ses empreintes ou son iris ont été contrefaits. Aussi, le vol d'identité biométrique est troublant car s'il est possible d'annuler une carte de crédit si elle est volée, une fois un vecteur biométrique copié, il n'y a plus rien à faire et il est facile d'imaginer une telle perte similaire de la présomption de la bonne foi dans les relations des citoyens avec l'État.

Mais une des prémisses de ce mémoire était aussi de se demander si la biométrie pouvait apporter la sécurité afin de pouvoir savoir si les pertes de libertés sont compensées par un gain en sécurité. Le schéma qui sera utilisé pour cette analyse sera celui de Bruce Schneier présenté dans l'introduction de ce mémoire. En cinq points précis, il permet d'évaluer si une technologie doit être implantée ou non :

1) Quel problème la « solution » va-t-elle régler ?

2) Dans quelle proportion le problème sera-t-il réglé ?

3) Est-ce que des problèmes nouveaux vont émerger de l'implantation de la solution ?

4) Coût économique et social.

5) Cela en vaut-il la peine ? [317]

Rapidement, il faut rejeter la biométrie, car les technologies s'adressant aux problèmes de sécurité induits par le terrorisme ne seront efficaces que dans une infime proportion de cas (les terroristes ne vont pas s'enregistrer et s'ils le font, ce ne sera pas en tant que terroriste, la différence entre un terroriste et un homme ordinaire, c'est l'intention) et en plus la technologie ne fonctionne pas (par exemple, pour la reconnaissance faciale qui est le fer de lance de la biométrie depuis le 11 septembre 2001[318] : James Wayman qui est directeur à San Jose du « National Biometrics Test Center » affirmait que la reconnaissance faciale n'aurait que 60% de chance d'identifier correctement Oussama ben Laden s'il n'était pas déguisé).

En regardant les choses en perspective, les nouveaux problèmes sont nombreux, notamment les gens qui vont refuser de s'y soumettre, les contestations, le vol d'identité permanent, les fraudes (de toute façon, si un voleur vole une carte de guichet, la victime peut aller à sa banque qui va lui en émettre une autre avec un autre numéro, si quelqu'un réussit à faire une copie de son empreinte digitale, qu'est que la victime peut faire ?[319]), etc. De plus, un nouveau crime sera crée comme en témoigne un fait divers en Malaisie où des voleurs de voiture ont coupé un doigt à leur victime afin de pouvoir voler une voiture munie d'un système anti-vol biométrique[320]. Donc, la conséquence sera-t-elle de pencher vers plus de sécurité ou moins de sécurité, en ce sens qu'une victime d'un vol classique se portera-t-elle mieux

---

[317] Ackerman, *loc. cit.*
[318] *Idem.*
[319] Mann, l*oc. cit.*, p. 12.
[320] Jonathan, Kent, « Malaysia car thieves steal finger », In *BBC News*, [en ligne], http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm, (consulté le 15 février 2006).

qu'une victime d'un crime impliquant la biométrie ? Qui va tirer profit le plus de ces nouvelles protections ? Le propriétaire de la voiture ou la compagnie d'assurance ?

Aussi, Bruce Schneier définit deux types d'échecs, l'échec simple où une mesure de sécurité ne fonctionne tout simplement pas et l'échec substractif (subtractive failure) où le nouvel élément de sécurité rend les gens plus vulnérables. Par exemple, si la biométrie de la reconnaissance faciale de la compagnie IDENTIX est utilisée en se fiant au taux de succès de 99,32% affirmé par la compagnie elle-même (dans des conditions de laboratoire et en admettant que les terroristes soient fichés), cela veut dire que pour l'aéroport de Boston, par année, 170 000 personnes déclencheraient une fausse alerte bien qu'ils n'aient rien à se reprocher, donc près de 500 alertes par jour, ce qui ferait que les employés finiraient par ignorer ces alertes, même celles qui sont légitimes[321]. La biométrie, du moins celle à reconnaissance faciale, fait aisni partie des échecs substractifs.

Aussi, le coût économique (jusqu'à 25 000$ pour un seul système de reconnaissance faciale[322]) et social est inacceptable, ne serait-ce qu'en matière de pertes de libertés (vie privée et anonymat par exemple) et d'affaiblissement de la démocratie.

Finalement, cela n'en vaut pas la peine. Car ajouter une mesure de sécurité ne mène pas nécessairement à plus de sécurité. Le meilleur exemple est celui de Mann qui écrivait que dans les années 90 les fabricants d'automobiles ont systématisé l'implantation dans leurs automobiles de systèmes anti-démarreurs afin d'enrayer le problème des vols d'automobiles.

---

[321] Mann, *loc. cit.*, pp. 10-11.

[322] Maselli, Jennifer, « Airlines are exploring biometrics to improve security, but it won't be cheap--or easy », In *InformationWeek*, [en ligne], http://www.informationweek.com/story/IWK20011109S0003, (consulté le 5 juin 2006).

Le résultat est plus que douteux : les voleurs font maintenant du « carjacking » (le voleur s'empare de la voiture lorsque le propriétaire y est encore puis l'expulse manu militari)[323]. Donc, qu'est-ce qui est le mieux ? Se faire voler sa voiture ou se faire tabasser ET se faire voler sa voiture ? Ou pire, se faire voler sa voiture ET se faire tabasser ET se faire couper la main ?[324] En conséquence, la capacité des systèmes biométriques à bien passer à travers un échec, concept dont parle Schneier[325], est anémique puisque l'échec d'un système a de graves conséquences. En fait, trop graves du fait que les victimes souffrent de plus en plus lors d'un de ces échecs (les voleurs devront couper la main de leur victime au lieu de simplement voler leur voiture...).

Parce qu'en fin de compte, avant d'en arriver à des « solutions » draconiennes aux conséquences potentiellement liberticides, peut-être faudrait-il faire comme Schneier (celui qui s'est battu avec succès pour empêcher toute forme de réglementation gouvernementale sur le cryptage dans les années 90) et revenir aux bases de la sécurité. Quelle est l'utilité d'un système sophistiqué si les portes sont laissées déverrouillées ? Un sondage a déjà montré que la moitié des travailleurs britanniques utilisaient soit leur propre nom, le nom d'un membre de leur famille ou de leur animal domestique ou encore « Homer Simpson » ou « Darth Vader » comme mot de passe[326] ! Ou encore que les gens utilisent toujours le même nom d'utilisateur et le même mot de passe, que ce soit pour l'ordinateur au travail, pour le courriel, pour leur ordinateur personnel, etc. Ce qui fait dire à Schneier qu'il suffirait d'ouvrir un site internet qui offrirait gratuitement de la pornographie, mais qui demanderait une inscription en ligne pour y accéder

---

[323] Mann, *loc. cit.*, p. 1.
[324] Jonathan, *loc. cit.*
[325] Mann, *loc. cit.*, p. 8.
[326] *Ibid.*, p. 2.

(nom d'utilisateur et mot de passe comme pour les services de courriels gratuits à l'instar d'Hotmail) et des millions de cadres et de dirigeants s'inscriraient avec le même nom d'utilisateur et le même mot de passe qu'ils utilisent au bureau.[327] Ce qui donnerait à Schneier des possibilités énormes pour frauder. En conclusion, avant d'installer des portes blindées sur une maison, il faudrait commencer par verrouiller les portes... Et c'est le même principe avec la biométrie.

Il est convenable de terminer par une citation qui devrait permettre au lecteur de réfléchir plus profondément sur les deux idées centrales de ce texte : la liberté et la sécurité.

« Those who desire to give up Freedom in order to gain Security, will not have, nor do they deserve, either one. » — Thomas Jefferson

---

[327] *Idem.*

Annexe

Voici deux diapositives pour une technique simple qui a déjoué les lecteurs d'empreintes digitales[328] :

Photo 4 : Technique de moulage d'une empreinte digitale

[328] Smith Rick, Ph.D., CISSP, « The Biometric Dilemma », secure computing, http://www.smat.us/crypto/docs/bh-us-02-smith-biometric.ppt, diapositive # 33 et 34.

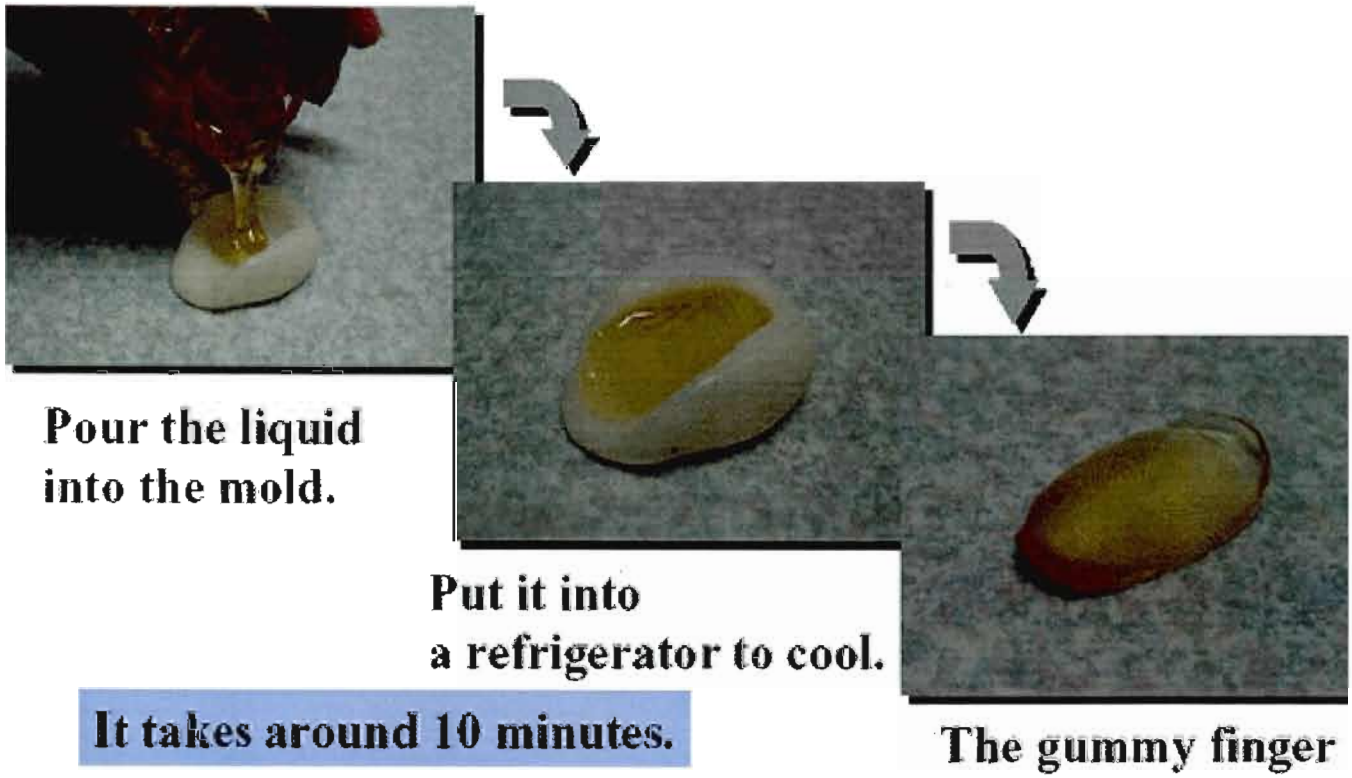


Photo 5 : Technique pour la fabrication d'une empreinte digitale

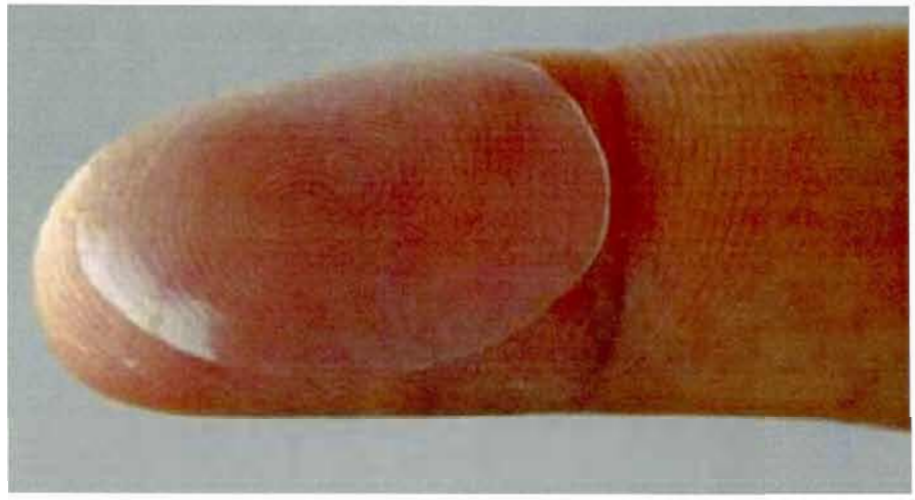


Photo 6 : Voici la version améliorée et très discrète d'une empreinte digitale fabriquée, ce qui déjouerait les lecteurs d'empreintes digitales qui cherchent à savoir si le doigt est vivant (*liveness test*) par le biais de la détection de la chaleur, du pouls ou par électrocardiogramme (ECG)[329].

[329] Drygajlo, Andrzej, *Biometrics for Identity Verification - Attacks on the biometric system*, [en ligne], http://scgwww.epfl.ch/courses/Biometrics-continuingEducation-2007/Andrzej_Drygajlo_Slides.pdf, p. 60, (consulté le 19 août 2007).

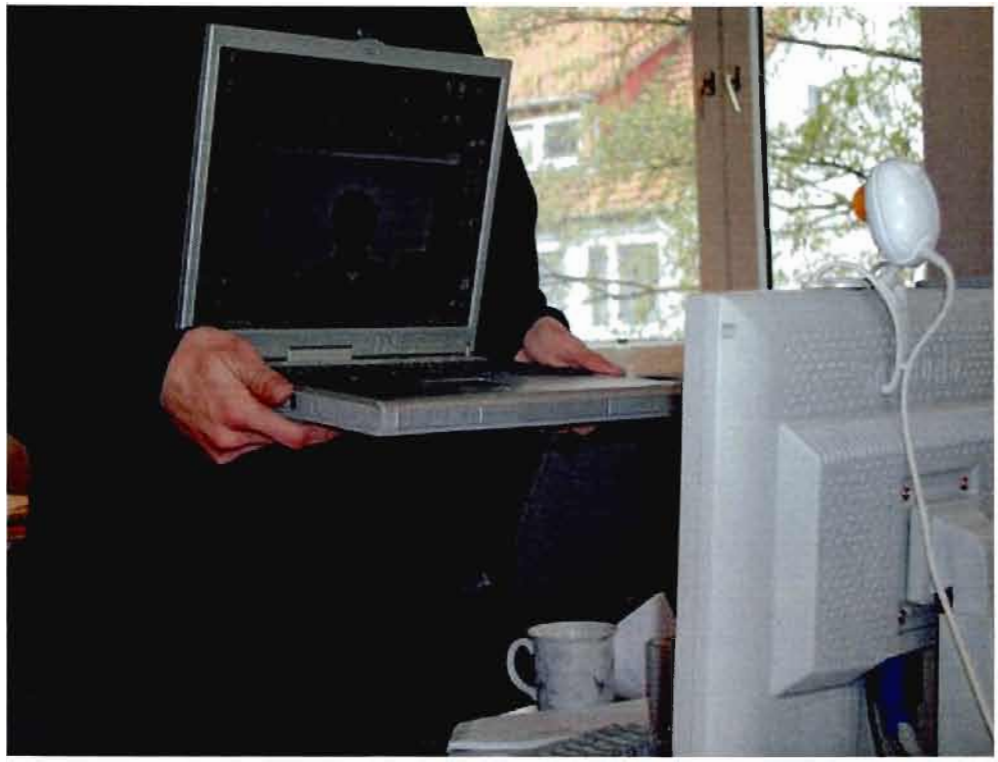


Photo 7 : Déjouer un lecteur facial à l'aide d'un ordinateur portable[330]

[330] Thalheim, Krissler et Ziegler, *loc. cit.*

Photo 8 : Technique pour prélever une empreinte digitale latente à partir d'un lecteur à empreinte digitale[331]

[331] *Idem.*

Photo 9 : Un journaliste met une photo d'iris, avec un trou au milieu, devant son œil afin de déjouer un système à iris (le trou permet à la pupille de se dilater et déjouer le détecteur de dilatation de pupille qui a pour but, ironiquement, d'empêcher qu'une simple photo déjoue le système) [332]

[332] *Idem.*

Bibliographie

ABN AMRO, *ABN AMRO launches biometric voice verification in telephone banking*, [en ligne], http://www.abnamro.com/pressroom/releases/2006/2006-07-20-en.jsp, (consulté le 30 septembre 2006).

Ackerman, Linda, *Biometrics And Airport Security*, Privacyactivism.org, 17 février 2003, [en ligne], http://www.privacyactivism.org/Item/64, (consulté le 1er juin 2006).

ACLU, *American Civil Liberties Union : Feature on Face-Recognition Technology,* [en ligne], http://www.aclu.org/Privacy/Privacy.cfm?ID=12119&c=130, (consulté le 2 juin 2006).

ACLU, *Data on Face-Recognition Test at Palm Beach Airport Further Demonstrates Systems' Fatal Flaws*, 14 mai 2002, [en ligne], http://www.aclu.org/Privacy/Privacy.cfm?ID=10340&c=130, (consulté le 2 juin 2006).

ACLU, *"Drawing a Blank: Tampa Police Records Reveal Poor Performance of Face-Recognition Technology."*, 3 janvier 2002, [en ligne], http://www.aclu.org/news/2001/n010302a.html, (consulté le 2 juin 2006).

AFX News Limited, *Mizuho, SMBC to share finger-vein biometric ATMs with Japan Post – report*, [en ligne], http://www.forbes.com/business/feeds/afx/2006/08/20/afx2960839.html, (consulté le 25 septembre 2006).

Agre, Philip E. et Marc Rotenberg, *Technology and Privacy: The New Landscape*, Cambridge, MIT, 1998.

Agre, Phil, *Your face is not a bar code: arguments against automatic face recognition in public places*, Whole Earth, Hiver 2001, [en ligne], http://www.findarticles.com/p/articles/mi_m0GER/is_2001_Winter/ai_81790171, (consulté le 29 mai 2006).

Alba, Bonnie, *Americans' Illusive Privacy - 'Man No Longer King of His Castle'*, 6 mars 2006, [en ligne], http://www.americanchronicle.com/articles/viewArticle.asp?articleID=6572, (consulté le 13 janvier 2007).

Alderman, Ellen et Caroline Kennedy, *The Right to Privacy*, New York, Vintage Books, 1995.

Ashbaugh, David R., *Ridgeology : Modern evaluative friction ridge identification*, Forensic identification support section, Gendarmerie royale du Canada, [en ligne], http://onin.com/fp/ridgeology.pdf, (consulté le 30 août 2006).

Avery, Keith, *Utilizing Technology*, [en ligne], http://www.stevenspublishing.com/Stevens/SecProdPub.nsf/frame?open&redirect=http://www.stevenspublishing.com/stevens/secprodpub.nsf/d3d5b4f938b22b6e8625670c006dbc58/2a9e1688dd432ca88625711f0062b8c7?OpenDocument, (consulté le 22 septembre 2006).

Baard, Mark, « Big Brother to Watch Over Island », *Wired*, [en ligne], http://www.wired.com/news/privacy/0,1848,63316,00.html, (consulté le 6 juin 2006).

Baker, Stewart A. et Paul R. Hurst, *The Limits of Trust: Cryptography, Governments, and Electronic Commerce*, Boston, Kluwer Law International, 1998.

Barrett, William A., *Iriscan Evaluation*, National Biometric Test Center, San Jose State University, 10 mars, 1999.

BBC News, *Rights group criticises 'Asbo TV'*, [en ligne], http://news.bbc.co.uk/1/hi/england/london/4597990.stm, (consulté le 1er mai 2007).

Beavan, Colin, *Fingerprints: The Origins of Crime Detection and the Murder Case That Launched Forensic Science*, 2001, 256 pages.

Belsie, Laurent, « Tech Trends Coming Soon: ATMs That Recognize Your Eyes » In *Christian Science Monitor,* décembre 2, 1997.

Benn, Stanley I., « 1 : Privacy, Freedom and Respect for Persons », In Pennock J. Roland et John W. Chapman (sous la dir.), *Privacy*, Atherton press, inc., 1971.

Berkowitz, Bill, *Surveillance cameras are watching you in the name of the 'war on terrorism'*, WorkingForChange, 05.03.02, [en ligne], http://www.workingforchange.com/article.cfm?ItemID=13257, (consulté le 3 juin 2006).

Bo, Li, *What Is Rule of Law?* Perspectives, Vol. 1, No. 5, [en ligne], http://www.oycf.org/Perspectives/5_043000/what_is_rule_of_law.htm, (consulté le 28 janvier 2007).

Borking, John, « 3 : The use and value of privacy-enhancing technologies », In Lace, Susanne (sous la dir.), *The Glass Consumer : Life in a surveillance society*, Southampton, Grande-Bretagne, The Policy Press (Bristol), 2005.

Boyd, Jeffrey E. et James J. Little, *Biometric Gait Recognition*, Universités de Calgary et de Colombie-Britannique : département des sciences informatiques, [en ligne], http://pages.cpsc.ucalgary.ca/~boyd/papers/biometric-summerschool.pdf, (consulté le 4 septembre 2006).

Breckenridge, Keith, *Towards the theory of the Biometric State*, [en ligne], http://www.history.und.ac.za/Sempapers/Breckenridge2005.pdf, (consulté le 8 septembre 2006).

Brin, David, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* Perseus Books, 1998.

Catalyst - Australian Broadcasting Corporation (ABC), *DNA Doubt*, émission du 16 septembre 2004, transcription, [en ligne], http://www.abc.net.au/catalyst/stories/s1199805.htm, (consulté le 30 septembre 2007).

Cate, Fred H., *Privacy in the Information Age*, Washington D.C., The Brookings Institution, 1997.

Cavoukian, Ann, « The promise of privacy-enhancing technologies: applications in health information networks. » In *Visions of privacy: policy choices for a digital age*, University of Toronto Press, 1999.

CBC News, *Sask. doctor sentenced for rape*, 10 novembre 2000, [en ligne], http://www.cbc.ca/story/news/?/news/1999/11/26/saskdr991126, (consulté le 14 janvier 2007).

CBC News Disclosure, *Unreliable evidence*, [en ligne], http://www.cbc.ca/disclosure/archives/031126_evidence/hair.html, (consulté le 3 janvier 2007).

Chopra, Prianka, *The EyeDentify Metamorphosis*, Frost & Sullivan Market Insight, 1er août 2001, [en ligne], http://www.frost.com/prod/servlet/market-insight-top.pag?docid=RKUR-4ZMW3G, (consulté le 14 septembre 2006).

Club de la Sécurité des Systèmes d'Information Régional, *Gestion des identités : Biométrie – RFID – Moyens d'authentification – contrôles d'accès au SI – gestion des droits*, [en ligne], www.clusir-rha.fr/download.php?id=106, (consulté le 7 mai 2007).

Clarke, Roger, *Biometrics and Privacy*, Xamax Consultancy Pty Ltd, Canberra, Department of Computer Science, Australian National University, Notes du 15 avril 2001, [en ligne], http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html, (consulté le 3 juin 2006).

Coelle, Christopher, « Using and abusing iris recognition », In *Information Age*, 04/12/2003, [en ligne], http://www.infoage.idg.com.au/index.php/id;749011882;fp;4;fpid;866209206, (consulté le 9 juin 2006).

Columbia University Graduate School of Architecture, planning and preservation, *Panopticon*, [en ligne], http://www.arch.columbia.edu/DDL/cad/IP_SP99/students/Trent/imaps/panopticon.jpg, (consulté le 25 août 2006).

Commissaire à la protection de la vie privée du Canada, Jennifer Stoddart, *Réponse à la consultation du gouvernement sur l'accès légal : Présentation du Commissariat à la protection de la vie privée du Canada au ministre de la Justice et procureur général du Canada*, 5 mai 2005, Ottawa (Ontario), [en ligne], http://www.privcom.gc.ca/information/pub/sub_la_050505_f.asp, (consulté le 3 octobre 2006).

Commission de l'éthique de la science et de la technologie, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques – Documents de Réflexion*, [en ligne], http://www.ethique.gouv.qc.ca/fr/ftp/Biometrie-reflexion.pdf, (consulté le 30 mars 2006).

Commission de l'éthique de la science et de la technologie, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques – Documents de Réflexion*, [en ligne], http://www.ethique.gouv.qc.ca/fr/ftp/Biometrie-reflexion.pdf, (consulté le 30 mars 2006).

Corson B., William, *Brief History of Fingerprint Identification*, [en ligne], http://members.cox.net/bnminalpine/novascot.htm, (consulté le 4 septembre 2006).

CrimTrac Agency - Commonwealth of Australia, *Key Dates in the History of DNA Profiling*, [en ligne], http://www.crimtrac.gov.au/dnahistory.htm, (consulté le 14 septembre 2006).

Daily Mail, *Big Brother is shouting at you*, 16 septembre 2006, [en ligne], http://www.dailymail.co.uk/pages/live/articles/news/news.html?in_article_id=405477&in_page_id=1770, (consulté le 1er mai 2007).

Daugman, John, *Combining Multiple Biometrics*, The Computer Laboratory, Cambridge University, [en ligne], http://www.cl.cam.ac.uk/users/jgd1000/combine/combine.html, (consulté le 24 juin 2006).

Davies, Simon G., « Touching Big Brother : How biometric technology will fuse flesh and machine », In *Information Technology & People*, Vol 7, No. 4, 1994, [en ligne], http://www.privacy.org/pi/reports/biometric.html, (consulté le 27 février 2006).

De Jong, Matthew, Matt De Jong, Charles Wilkinson et John Ketcham, *I Accuse*, 2003.

De Tocqueville, Alexis, *De la démocratie en Amérique, volume 1*, Collection Folio/Histoire, Gallimard, La Flèche (Sarthe), France, 1986, 631 pages.

De Tocqueville, Alexis, *De la démocratie en Amérique, volume 2*, Collection Folio/Histoire, Gallimard, La Flèche (Sarthe), France, 1986, 471 pages.

Dearne, Karen, *Biometric checks must improve*, [en ligne], http://www.argus-solutions.com/austit15oct02.html, (consulté le 6 juin 2006).

Dearne, Karen, *Face recognition fails test*, 27 février 2003, [en ligne], http://www.notbored.org/face-misrecognition.html, (consulté le 2 juin 2006).

Dempsey, James X., *The False Trade-Off Between Freedom and Security*, American Bar Association, [en ligne], http://www.abanet.org/irr/hr/winter02/dempsey.html, (consulté le 23 août 2006).

Dennis, Brady, « Ybor cameras won't seek what they never found », In *St. Petersburg Times*, 20 août 2003, [en ligne], http://www.sptimes.com/2003/08/20/Hillsborough/Ybor_cameras_won_t_se.shtml, (consulté le 15 mars 2006).

Department of homeland security, *US-VISIT Program*, [en ligne], http://www.dhs.gov/dhspublic/interapp/content_multi_image/content_multi_image_0006.xml, (consulté le 30 septembre 2006).

Dick, Philip K., Scott Frank, Jon Cohen et Steven Spielberg, *Minority Report*, 2002.

Drygajlo, Andrzej, *Biometrics*, [en ligne], http://scgwww.epfl.ch/courses/Biometrics-Lectures-2006-2007/07-Biometrics-Lecture-7-Part1-1-2006-12-04.pdf, (consulté le 18 juin 2007).

Drygajlo, Andrzej, *Biometrics for Identity Verification - Attacks on the biometric system*, [en ligne], http://scgwww.epfl.ch/courses/Biometrics-continuingEducation-2007/Andrzej_Drygajlo_Slides.pdf, (consulté le 19 août 2007).

Dugelay, Jean-Luc, *Reconnaissance du visage*, [en ligne], http://dept-info.labri.u-bordeaux.fr/~maylis/pari-stic.labri.fr/TUTORIAL/tutorial_BIO_2_PARISTIC_05.pdf, (consulté le 7 septembre 2006).

Electronic Privacy Information Center, *The Privacy Act of 1974*, [en ligne], http://www.epic.org/privacy/1974act/, (consulté le 19 mars 2007).

Ellul, Jacques, *Les nouveaux possédés*, Librairie Arthème Fayard, Paris, 1973, 286 pages.

European Commission - Directorate-General - Joint Research Centre, *Fact sheet on biometrics*, http://www.jrc.ec.europa.eu/download/press/20050330_biometrics_fact_sheet.pdf, (consulté le 20 août 2007).

Face Recognition Vendor Test (FRVT), *FacE REcognition Technology (FERET)*, [en ligne], http://www.frvt.org/FERET/default.htm, (consulté le 14 septembre 2006).

Fay, Joe, « Biometrics won't deter passport fraudsters, chief admits », In *The register*, 1er juillet 2005, [en ligne], http://www.theregister.co.uk/2005/07/01/bio_passport_fraud/, (consulté le 3 juin 2006).

Federal Bureau of Investigation - CJIS Division. *Integrated Automated Fingerprint Identification System or IAFIS*, [En ligne], http://www.fbi.gov/hq/cjisd/iafis.htm, (consulté le 9 septembre 2006).

Foucault, Michel, *Surveiller et punir. Naissance de la prison*, Paris, Gallimard, 1975, 318 pages.

Fried, Charles, *An Anatomy of Values,* Cambridge, Harvard University Press, 1970.

Gallagher, Sean, *The New Face of Surveillance*, [en ligne], http://www.baselinemag.com/article2/0,1540,1725643,00.asp, (consulté le 3 juin 2006).

Gang Wei et Dongge Li « 8 : Biometrics : Applications, Challenges and the Future », In J. Strandburg, Katherine et Daniela Stan Raicu (sous la dir.), *Privacy and Technologies of Identity – A Cross-Disciplinary Conversation*. Springer Science+Business Media, Inc. 2004.

Garfinkel, Simson, *Biometrics Slouches Toward the Mainstream : The systems are getting cheaper, but accuracy and acceptance kinks remain*, CSO, [en ligne], http://www.csoonline.com.au/index.php/id;1183366141;fp;8;fpid;8, (consulté le 9 juin 2006).

Garfinkel, Simson, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly and Associates, 2000.

Gavison, Ruth, « Privacy and the Limits of Law » In *Yale Law Journal*, volume 89, 1980, pp. 421-471.

GlobalSecurity.org, *Biometrics*, http://www.globalsecurity.org/security/systems/biometrics.htm, (consulté le 20 août 2007).

Grgic, Marin, *Biometrics and Retina Scan Technology*, [en ligne], https://olt.qut.edu.au/it/itn584/gen/static/resources/01p-grgic.pdf, (consulté le 29 août 2006).

Guardware Systems Ltd., *Fingerprint Recognition II : History of Fingerprinting*, [en ligne], http://biometrie.online.fr/dossiers/technique/empreintes/History_of_Fingerprinting.pdf, (consulté le 2 septembre 2006).

Hentoff, Nat, « Our liberties under siege », In *Washington Post*, 7 novembre 2005, [en ligne], http://www.washtimes.com/op-ed/20051106-102157-6451r.htm, (consulté le 23 mai 2006).

Hope-Tindall, Peter, *Public Space, Private Space: Where do we draw the line ?*, Information Rights Salon, 29 octobre 2002, [en ligne], http://www.fis.utoronto.ca/research/inforights/PHT-Presentation.ppt, (consulté le 15 février 2006).

House of Commons - Home Affairs (Grande-Bretagne), 57. Supplementary memorandum submitted by Privacy International, [en ligne], http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130we66.htm, (consulté le 30 juin 2007).

Human Genome Project (HGP), *DNA Forensics*, [en ligne], http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml, (consulté le 14 janvier 2007).

Huysmans, Jef, « Minding Exceptions: The Politics of Insecurity and Liberal Democracy » In *Theory and Practice*, Palgrave Macmillan Ltd, pp. 321 à 341, [en ligne], www.palgrave-journals.com, (consulté le 24 août 2006).

International Biometric Group, *The Henry Classification System*, Research Consulting Integration, 2003, [en ligne], http://www.biometricgroup.com/Henry%20Fingerprint%20Classification.pdf, (consulté le 5 septembre 2006).

J. Strandburg, Katherine et Daniela Stan Raicu (sous la dir.), *Privacy and Technologies of Identity – A Cross-Disciplinary Conversation*, Springer Science+Business Media, Inc., 2004, 383 pages.

Jonathan, Kent, « Malaysia car thieves steal finger », In *BBC News*, [en ligne], http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm, (consulté le 15 février 2006).

Jones, Alex, *Fallujah Residents Face Choice: Retina Scan and Take ID Card....Or Die*, [en ligne], http://www.prisonplanet.com/articles/december2004/021204facechoice.htm, (consulté le 27 septembre 2006).

Kellner, Douglas, *Habermas, the Public Sphere, and Democracy: A Critical Intervention,* [en ligne], http://www.gseis.ucla.edu/faculty/kellner/papers/habermas.htm, (consulté le 13 août 2006).

K Sethi, Ishwar, « 7 : Biometrics : Overview and Applications », In J. Strandburg, Katherine et Daniela Stan Raicu (sous la dir.), *Privacy and*

Technologies of Identity – A Cross-Disciplinary Conversation. Springer Science+Business Media, Inc. 2004.

Kimball, John W., *Restriction Fragment Length Polymorphisms (RFLPs)*, [en ligne], http://users.rcn.com/jkimball.ma.ultranet/BiologyPages/R/RFLPs.html, (consulté le 17 janvier 2007).

King, Steven, *Testing Iris and Face Recognition in a Personnel Identification Application*, Information Systems Directorate, Office of the Deputy Under Secretary of Defense (Science & Technology), Hal Harrelson & George Tran Army Research Lab, 15 février 2002.

Korotkaya, Zhanna, *Biometric Person Authentication: Odor*, Lappeenranta University of Technology : Department of Information Technology : Laboratory of Applied Mathematics, [en ligne], http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Korotkaya.pdf, (consulté le 14 septembre 2006).

Lace, Susanne (sous la dir.), *The Glass Consumer : Life in a surveillance society*, Southampton, Grande-Bretagne, The Policy Press (Bristol), 2005, 259 pages.

Lakany, H. et G. Hayes, « An Algorithm for Recognising Walkers », In *Audio- and Video-based Biometric Person Authentication*, The International Association for Pattern Recognition, 1997, pp. 112 à 118.

Laufer, Berthold, « History of the fingerprint system », In *The print*, Volume 16 (2), mars-avril 2000, pp 1 - 13.

LCN, *La SAAQ infiltrée par deux taupes reliées aux motards*, [en ligne], http://lcn.canoe.com/infos/national/archives/2000/12/20001208-062657.html, (consulté le 7 juin 2006).

Le Douarin, Nicole, *Allocution : Science et justice : Des empreintes digitales aux empreintes génétiques, à la recherche de la preuve indiscutable*, Institut de France, Académie des sciences, mardi le 23 novembre 2004, [en ligne], http://www.academie-sciences.fr/conferences/seances_solennelles/pdf/discours_Le_Douarin_23_11_04.pdf, (consulté le 10 septembre 2006).

Locke, John, *The Second Treatise of Government*, The Library of Liberal Arts, The Bobbs-Merrill Compagny Inc., imprimé aux États-Unis, 1952, 139 pages.

Lyon, David, « 2 : Surveillance after September 11, 2001 ». In Webster, Frank et Kirstie Ball (sous la dir.), *The Intensification of Surveillance : Crime, Terrorism and Warfare in the Information Age*. Pluto Press, 2003.

Mann, Charles C., « Homeland Insecurity », In *The Atlantic Monthly*, septembre 2002.

Marconi, David et Tony Scott, *Enemy of the State*, 1998.

Maselli, Jennifer, « Airlines are exploring biometrics to improve security, but it won't be cheap--or easy », In *InformationWeek*, [en ligne], http://www.informationweek.com/story/IWK20011109S0003, (consulté le 5 juin 2006).

Matsumoto, T., H. Matsumoto, K. Yamada, S. Hoshino, « Impact of Artificial Gummy Fingers on Fingerprint Systems » In *Proceedings of SPIE*, Vol. #4677, Optical Security and Counterfeit Deterrence Techniques IV, 2002.

Matt Kieltyka, Sun Media C-News, *DNA contamination in Pickton trial*, [en ligne], http://cnews.canoe.ca/CNEWS/Canada/PicktonTrial/News/2007/03/28/3853028-sun.html, (consulté le 25 septembre 2007).

Mauck, Melissa Jeanne, *Fingerprints: Are They Your Own?*, [en ligne], http://www.shsu.edu/~mth_jaj/math470/papers_s06/Melissa.pdf, (consulté le 7 septembre 2006).

McElroy, Wendy et Carl Watner (sous la dir.), *National Identification Systems : essays in Opposition*, McFarland & Compagny, Inc., 2004, 308 pages.

McLean, Deckle, *Privacy and it's Invasion*, Westport, Connecticut, Praeger Publishers, 1995, 141 pages.

McMillan, Robert, « The Myth of Airport Biometrics », In *Wired News*, 9 août 2002, [en ligne], http://www.wired.com/news/conflict/0,2100,54418,00.html, (consulté le 2 juin 2006).

Meehan, Michael, *Iris scans take off at airports*, Computerworld, [en ligne], http://archives.cnn.com/2000/TECH/computing/07/19/iris.scan.idg/index.html, (consulté le 28 septembre 2006).

Mill, John Stuart, *On Liberty*, Appleton-Century-Crofts, New York, 1947, 118 pages.

Mnookin, Jennifer L., « The Achilles' Heel of Fingerprints », *Washington Post*, samedi 29 mai 2004, p. A27.

Montesquieu, *De l'Esprit des lois, I*, Collection Folio/Essais, Gallimard, La Flèche (Sarthe), France, 1995, 604 pages.

Montesquieu, *De l'Esprit des lois, II*, Collection Folio/Essais, Gallimard, La Flèche (Sarthe), France, 1995, 1627 pages.

Murphy, Shelley et Bray Hiawatha, « Face recognition devices failed in test at Logan », In *Boston Globe*, 9/3/2003, [en ligne], http://www.boston.com/news/local/articles/2003/09/03/face_recognition_devices_failed_in_test_at_logan/, (consulté le 1er juin 2006).

National Center for State Courts - Court Technology Laboratory, Director of National Intelligence, *A brief history of biometrics*, [en ligne], http://ctl.ncsc.dni.us/biomet%20web/BMHistory.html, (consulté le 2 juin 2006).

National Center for State Courts - Court Technology Laboratory, Director of National Intelligence, *Biometrics comparison chart*, [en ligne], http://ctl.ncsc.dni.us/biomet%20web/BMCompare.html, (consulté le 24 juillet 2007).

National Center for State Courts - Court Technology Laboratory, Director of National Intelligence, *Hand geometry*, [en ligne], http://ctl.ncsc.dni.us/biomet%20web/BMHand.html, (consulté le 24 juillet 2007).

National Center for State Courts - Court Technology Laboratory, Director of National Intelligence, *Retinal scan*, [en ligne], http://ctl.ncsc.dni.us/biomet%20web/BMRetinal.html, (consulté le 28 septembre 2006).

National institutes of health, *Visible proofs: Forensic Views of the Body: Biographies: Juan Vucetich (1858-1925)*, National library of medecine, [en ligne], http://www.nlm.nih.gov/visibleproofs/galleries/biographies/vucetich_image_3.html, (consulté le 7 septembre 2006).

National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Biometrics History*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Biometrics%20History.pdf, (consulté le 15 septembre 2006).

National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Dynamic Signature*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/dynamic%20signature.pdf, (consulté le 12 septembre 2006).

National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Face recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Face%20Recognition.pdf, (consulté le 2 septembre 2006).

National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Fingerprint Recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Fingerprint%20Recognition.pdf, (consulté le 2 septembre 2006).

National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Hand geometry*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Hand%20Geometry.pdf, (consulté le 2 septembre 2006).

National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Iris recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Iris%20Recognition.pdf, (consulté le 2 septembre 2006).

National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Palm Print Recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Palm%20Print%20Recognition.pdf, (consulté le 2 septembre 2006).

National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Speaker Recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Speaker%20Recognition.pdf, (consulté le 10 septembre 2006).

National Science and Technology Council (NSTC), Committee on Technology, Committee on Homeland and National Security, Subcommittee on Biometrics, *Vascular pattern recognition*, [en ligne], http://www.biometricscatalog.org/NSTCSubcommittee/Documents/Vascular%20Pattern%20Recognition.pdf, (consulté le 3 septembre 2006).

Neill, Elizabeth, *Rites of Privacy and the Privacy Trade : On the Limits of Protection for the Self*, McGill-Queen's University Press, 2001, 196 pages.

Nellis, Mike, « 5 : 'They Don't Even Know We're There' : The Electronic Monitoring of Offenders in England and Wales ». In Webster, Frank et Kirstie Ball (sous la dir.), *The Intensification of Surveillance : Crime, Terrorism and Warfare in the Information Age*, Pluto Press, 2003.

Niccol, Andrew, *Gattaca*, 1997.

Nissenbaum, Helen, « Protecting Privacy in an Information Age: The Problem of Privacy in Public », University Center for Human Values, Princeton University, Law and Philosophy, 17: 559-596, 1998.

Orwell, George, *1984*, Signet Classics, ré-édition de juillet 1977, 336 pages.

Parker, Richard B., « A Definition of Privacy » In *Rutgers Law Review,* Vol. 27, 1974.

Pennock J. Roland et John W. Chapman (sous la dir.), *Privacy*, Atherton press, inc., 1971, 255 pages.

Prabhakar Salil, Sharath Pankanti et Anil K. Jain, « Biometric Recognition: Security and Privacy Concerns », In *Security & Privacy Magazine IEEE*, Volume 1, Issue 2, mars-avril 2003.

Privacy International, *An Open Letter to the ICAO : PI creates global coalition calling on UN agency to stop its biometric database standard, A second report on 'Towards an International Infrastructure for Surveillance of Movement'*, 30/03/2004, [en ligne], http://www.privacyinternational.org/issues/terrorism/rpt/icaoletter.pdf, (consulté le 15 mars 2006).

Privacy International, *Privacy and Human Rights, 2003: Overview*, [en ligne], http://www.privacyinternational.org/survey/phr2003/overview.htm, (consulté le 5 juin 2006).

Privacy International, *UK Early Beginnings of the DNA Database*. [en ligne], http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-508123, (consulté le 1er février 2007).

Privacy International, *UK Expands DNA Database through the Criminal Justice and Public Order Act 1994*. [en ligne],

http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-508126, (consulté le 1er février 2007).

Privacy International, *UK DNA Database includes the innocent and wrongly accused under the Criminal Justice and Police Act 2001.* [en ligne], http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-508140, (consulté le 1er février 2007).

Privacy International, *UK DNA Database to grow dramatically under the Criminal Justice Act 2003.* [en ligne], http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-508144, (consulté le 1er février 2007).

Privacy International, *UK retrospectively applies DNA profiling in the Criminal Evidence (Amendment) Act 1997.* [en ligne], http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-508125, (consulté le 1er février 2007).

Ramakrishnan, H. K. et M. P. Kadaba, « On the Estimation of Joint Kinematics During Gait », *J. Biomechanics*, 24 (10): pp. 969 - 977, 1991.

Randerson, James et Andy Coghlan, « Forensic evidence stands accused », In *New scientist*, 31 janvier 2004, Magazine issue 2432.

Rascati, Ralph J., *An Overview of Forensic DNA Typing Systems*, Kennesaw State University, [en ligne], http://science.kennesaw.edu/~rrascati/forensicpolymorphs.html, (consulté le 13 janvier 2007).

Rawls, John, *A Theory of Justice*, Cambridge, Massachusetts, Belknap Press of Harvard, University Press, 1999.

Regan, Priscilla M., *Legislating privacy : Technologie, Social Values, and Public Policy*, University of North Carolina Press, 1995, 310 pages.

Reiman, Jeffrey. « Driving to the Panopticon : A philosophical exploration of the risks to privacy posed by the information technology of the Future ». In Rössler, Beate, (sous la dir.), *Privacies : Philosophical evaluations*, Stanford University Press, 2004.

Rohde, Laura, « U.K.'s biometric trial exposes 'teething problems' », In *Computerworld*, [en ligne], http://www.computerworld.com/governmenttopics/government/policy/story/0,10801,102051,00.html?from=story_picks, (consulté le 7 juin 2006).

Rössler, Beate, « 1 : privacies : an overview ». In Rössler, Beate, (sous la dir.), *Privacies : Philosophical evaluations*, Stanford University Press, 2004.

Rössler, Beate, (sous la dir.), *Privacies : Philosophical evaluations*, Stanford University Press, 2004, 226 pages.

SA Mathieson, « Image problem », In *The Guardian*, 20 novembre, 2003, [en ligne], http://technology.guardian.co.uk/online/story/0,3605,1088437,00.html, (consulté le 5 juin 2006).

Sagem Morpho, Inc., *The History of Fingerprinting*, [en ligne], http://www.dia.unisa.it/~ads/corso-security/www/CORSO-9900/biometria/Fingerprinting.htm, (consulté le 3 septembre 2006).

Scheck, Barry et Peter Neufeld, « Junk Science, Junk Evidence », In *The New York Times*, 11 mai 2001, section A, p. 35.

Schneier, Bruce, *Beyond Fear : Thinking Sensibly About Security in an Uncertain World*, Springer+Business Media, 2003, 296 pages.

Schneier, Bruce, « Fun with Fingerprint Readers », In *Crypto-Gram Newsletter*, 15 mai 2002, [en ligne], http://www.schneier.com/crypto-gram-0205.html#5, (consulté le 8 février 2006).

Schoeman, Ferdinand David. « 1 : Privacy : philosophical dimensions of the literature ». In *Philosophical Dimensions of Privacy*. Cambridge University Press, 1984.

Schoeman, Ferdinand David (sous la dir.), *Philosophical Dimensions of Privacy*, Cambridge University Press, 1984, 426 pages.

Schoeman, Ferdinand David, *Privacy and Social Freedom*, Cambridge, Grande-Bretagne, Cambridge University Press, 1992, 239 pages.

Schwartz, John, « New Side to Face-Recognition Technology: Identifying Victims », In *The New York Times*, 15 janvier 2002, [en ligne], http://www.nytimes.com/2002/01/15/science/physical/15FACE.html?ex=1130385600&en=10482ca2addbfbf2&ei=5070, (consulté le 9 juin 2006).

Smith, Rick, « The Biometric Dilemma », In *secure computing*, [en ligne], http://www.smat.us/crypto/docs/bh-us-02-smith-biometric.ppt, (consulté le 3 juin 2006).

Soliman, Omar, *Political Jurisprudence vs. Judicial Independence : Reflections on the Legal Purpose and Institutional Role of Courts in a Liberal*

Democracy, Université de Toronto, [en ligne], http://individual.utoronto.ca/soliman/essays/political_jurisprudence_vs_judicial_independence.pdf, (consulté le 25 janvier 2007).

Stellitano, Corrina, « Face Value », *Access control & security systems*, [en ligne], http://securitysolutions.com/mag/security_face_value/, (consulté le 28 septembre 2006).

Swinford, Steven, « Asbo TV helps residents watch out », In *Times Online*, 8 janvier 2006, [en ligne], http://www.timesonline.co.uk/tol/news/uk/article786225.ece, (consulté le 2 mai 2007).

Swire, Peter P., et Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive*, Washington, D.C.: Brookings Institution, 1998.

Tapscott, Don, et Ann Cavoukian, *Who knows : safeguarding your privacy in a networked world*, Random House of Canada, 1995, 208 pages.

Technovelgy.com, *Biometric authentication: what method works best?*, [en ligne], http://www.technovelgy.com/ct/Technology-Article.asp?ArtNum=16, (consulté le 29 septembre 2006).

Thalheim Lisa, Krissler Jan et Peter-Michael Ziegler, *Biometric Access Protection Devices and their Programs Put to the Test, Body Check*, [en ligne], http://www.heise.de/ct/english/02/11/114/, (consulté le 8 janvier 2006).

The Academy for the Advancement of Science and Technology, *DNA Fingerprinting*, [en ligne], http://www.bergen.org/AAST/Projects/Gel/fingprint1.htm, (consulté le 15 janvier 2007).

The Biology Project, *What is a Short Tandem Repeat Polymorphism (STR)?*, Université d'Arizona, [en ligne], http://www.biology.arizona.edu/Human_Bio/activities/blackett2/str_description.html, (consulté le 11 janvier 2007).

The Biology Project, *What are the 13 core CODIS loci?*, Université d'Arizona, [en ligne], http://www.biology.arizona.edu/Human_Bio/activities/blackett2/str_codis.html, (consulté le 11 janvier 2007).

The Economist, « New-look passports : High-tech passports are not working », [en ligne], In *The Economist*, http://www.economist.com/science/displaystory.cfm?story_id=3666171, (consulté le 3 novembre 2006).

The national health museum – access excellence, *History if genetics timeline*, [en ligne], http://www.accessexcellence.org/AE/AEPC/WWC/1994/geneticstln.html, (consulté le 9 septembre 2006).

The Smoking Gun, *FBI Admits Fingering Wrong Man*, [en ligne], http://www.thesmokinggun.com/archive/0525041mayfield3.html, (consulté le 17 mars 2007).

Thomas, Rebekah, *Biometrics, Migrants, and Human Rights*, Global Commission on International Migration, 1er mars 2005, [en ligne], http://www.migrationinformation.org/Feature/display.cfm?id=289, (consulté le 6 juin 2006).

Travis, Alan, home affairs editor, « Passport applicants must give fingerprints : Preparation for ID cards goes ahead without parliament », *The Guardian*, Mardi 12 avril 2005, [en ligne], http://www.guardian.co.uk/uk_news/story/0,,1457289,00.html, (consulté le 4 mai 2007).

Tredoux, Gavan, *Francis Galton and Fingerprints*, Archives de Francis Galton, [en ligne], http://galton.org/fingerprinter.html, (consulté le 4 septembre 2006).

Turner, Alexis, *The Death of Bertillonage*, [en ligne], http://oninformatics.com/?p=7, (consulté le 12 septembre 2006).

Twight, Charlotte. « 11 : Systematic Federal Surveillance of Ordinary Americans ». In McElroy, Wendy et Carl Watner (sous la dir.), *National Identification Systems : essays in Opposition*, McFarland & Compagny, Inc., 2004.

Twist, Jo, « Facing a biometric future », In *BBC News Online technology*, 13 janvier 2004, [en ligne], http://news.bbc.co.uk/1/hi/technology/3389209.stm, (consulté le 8 janvier 2007).

United States Patent and Trademark Office, *Patent 4,736,203: 3D hand profile identification apparatus.* 5 avril 1988, [en ligne], http://patft.uspto.gov/netacgi/nph-

Parser?Sect1=PTO1&Sect2=HITOFF&d=PALL&p=1&u=/netahtml/srchnum.htm&r=1&f=G&l=50&s1=4,736,203.WKU.&OS=PN/4,736,203&RS=PN/4,736,203, (consulté le 15 septembre 2006).

Van Den Haag, Ernest. « 8 : On Privacy » , In Pennock J. Roland et John W. Chapman (sous la dir.), Privacy, Atherton press, inc., 1971.

Van Den Nieuwendijk, Hans, *No Fingerprints?*, [en ligne], http://www.xs4all.nl/%7Edacty/noprints.htm, (consulté le 23 septembre 2006).

Wald, Matthew L., « New High-Tech Passports Raise Snooping Concerns », In *New York Times*, [en ligne], http://news.com.com/New+high-tech+passports+raise+snooping+concerns/2100-1039_3-5469533.html, (consulté le 4 janvier 2007).

Warren, Samuel et Louis D. Brandeis, « The Right to Privacy », In *Harvard Law Review*, Vol. IV, 15 décembre 1890.

Wasserstrom, Richard A., « 14 : Privacy : some arguments and assumptions » In Schoeman, Ferdinand David (sous la dir.), *Philosophical Dimensions of Privacy*, Cambridge University Press, 1984.

Watner, Carl. « 17 : Why I oppose Government Enumeration ». In McElroy, Wendy et Carl Watner (sous la dir.), *National Identification Systems : essays in Opposition*, McFarland & Compagny, Inc., 2004.

Webster, Frank et Kirstie Ball (sous la dir.), *The Intensification of Surveillance : Crime, Terrorism and Warfare in the Information Age*, Pluto Press, 2003, 176 pages.

Wainwright, Martin, « Talking CCTV cameras accuse wrong person », In *The Guardian*, 12 avril 2007, [en ligne], http://society.guardian.co.uk/crimeandpunishment/story/0,,2055057,00.html, (consulté le 3 mai 2007).

Weinstein, W. L., « 2 : The private and the Free : A conceptual Inquiry » , In Pennock J. Roland et John W. Chapman (sous la dir.), *Privacy,* Atherton press, inc., 1971.

Westin, Alan F., *Computers, Health Records, and Citizen's Rights*, U.S. Department of Commerce, 1976.

Westin, Alan F. et Michael Baker, *Databanks in a Free Society: Computers, Record-Keeping, and Privacy*, New York : NY Times Book Co., 1972.

Westin, Alan F., *E-commerce and privacy : what net users want*, rapport technique, Louis Harris & Associates, juin 1998.

Westin, Alan F., *Information Technology in a Democracy*, Harvard University Press, Cambridge, Massachusetts, 1971, 499 pages.

Willing, Richard, « Airport anti-terror systems flub tests », In *USA Today*, mis à jour le 9/2/2003, [en ligne], http://www.usatoday.com/news/nation/2003-09-01-faces-usat_x.htm, (consulté le 5 juin 2006).

Wood, David, Eli Konvitz et Kirstie Ball. « 8 : The Constant State of Emergency? : Surveillance after 9/11 ». In Webster, Frank et Kirstie Ball (sous la dir.), *The Intensification of Surveillance : Crime, Terrorism and Warfare in the Information Age*, Pluto Press, 2003.

Woodward, John D. Jr., *Super Bowl Surveillance : Facing Up to Biometrics*, RAND, Arroyo center, [en ligne], http://www.rand.org/pubs/issue_papers/2005/IP209.pdf, (consulté le 10 septembre 2006).

Woodward, John D., Katharine Watkins Webb, Elaine M. Newton, Melissa A. Bradley, David Rubenson, Kristina Larson, Jacob Lilly, Katie Smythe, Brian Houghton, Harold Alan Pincus, Jonathan Schachter et Paul Steinberg, *Rand Army Biometric Applications: Identifying and Addressing Sociocultural Concerns,* Rand Corporation, 2001, 225 pages.

Wright, Benjamin, *Signing tax returns with a digital pen*, Electronic Frontiers Georgie, [en ligne], http://www.efga.org/digsig/penop02.txt, (consulté le 17 septembre 2006).

Wrolstad, Mark, « Hair-matching flawed as a forensic science: DNA testing reveals dozens of wrongful verdicts nationwide », In *The Dallas Morning News*, [en ligne], http://www.law-forensic.com/cfr_hair_3.htm, (consulté le 3 janvier 2007).

Yang Catherine, Kerry Capell et Otis Port, « The State Of Surveillance », In *BusinessWeek online*, 8 août 2005, [en ligne], http://www.businessweek.com/magazine/content/05_32/b3946001_mz001.htm, (consulté le 2 février 2006).

Zamyatin, Yevgeny, *We*, Eos, réédition de 1999, 256 pages.