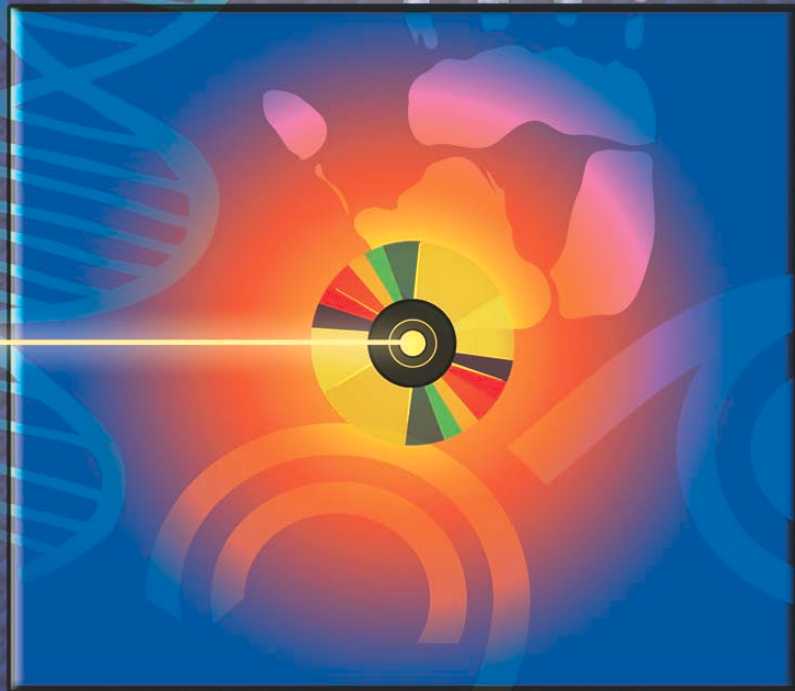


L'utilisation des données
biométriques
à des fins de **sécurité** :
questionnement sur les enjeux éthiques



Document de réflexion

**L'utilisation des données biométriques
à des fins de sécurité :
questionnement sur les enjeux éthiques**

Commission de l'éthique de la science et de la technologie

1200, route de l'Église
3^e étage, bureau 3.45
Sainte-Foy (Québec)
G1V 4Z2

En soutien à la réalisation du Document de réflexion

Recherche et rédaction

Diane Duquet, coordonnatrice de la CEST

Collaborations d'appoint

Bernard Dionne et Èvelyne Racette, Ministère des Relations avec les citoyens et de l'Immigration
Benoît Gagnon, Chaire Raoul-Dandurand et membre de la CEST
André Beauchamp, président de la CEST jusqu'en janvier 2005
M^e Danielle Parent, Commission d'accès à l'information du Québec et membre de la CEST

Soutien technique

Secrétariat et mise en page

Lauraine Bérard

Documentation

Monique Blouin

Conception graphique de la couverture

Créativité Sylvain Vallières Inc.

Document adopté à la 17^e réunion de la Commission de l'éthique de la science et de la technologie le 7 décembre 2004

© Gouvernement du Québec 2005

Dépôt légal : 2^e trimestre 2005
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada

ISBN 2-550-44634-8

Pour faciliter la lecture du texte, le genre masculin est utilisé sans aucune intention discriminatoire.

LES MEMBRES DE LA COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE¹

PRÉSIDENTE

M^e Édith Deleury

Professeure – Faculté de droit
Université Laval

Johane Patenaude

Professeure (éthique) – Faculté de médecine
Université de Sherbrooke

MEMBRES

Patrick Beaudin

Directeur général
Société pour la promotion de
la science et de la technologie

François Pothier

Professeur – Faculté des sciences de
l'agriculture et de l'alimentation
Université Laval

Louise Bernier

Doctorante en droit (bioéthique, génétique et
droit)
Université McGill

Louise Rozon

Directrice
Option Consommateurs

Sabin Boily

Consultant en nanotechnologies

D^r Stanley Vollant

Médecin
Complexe hospitalier de la Sagamie
Saguenay

MEMBRES INVITÉS

D^r Pierre Deshaies

Médecin spécialiste en santé communautaire
Chef du département clinique de santé publique
Hôtel-Dieu de Lévis

Geneviève Bouchard

Sous-ministre adjointe et directrice générale
Direction générale des politiques
Ministère de l'Emploi, de la Solidarité sociale et
de la Famille
Gouvernement du Québec

Benoît Gagnon

Chercheur
Chaire Raoul-Dandurand en études
stratégiques et diplomatiques
Université du Québec à Montréal

Danielle Parent

Secrétaire adjointe à la législation et conseillère
juridique
Commission d'accès à l'information du Québec

Jacques T. Godbout

Sociologue
Institut national de la recherche scientifique –
Urbanisation, Culture et Société

COORDONNATRICE

Michèle S. Jean

Faculté des études supérieures
Université de Montréal
Présidente du Comité international de
bioéthique – UNESCO

Diane Duquet

¹ Au moment de l'adoption du Document de réflexion, André Beauchamp était président de la CEST. M^e Édith Deleury, jusqu'alors membre de la CEST, lui a succédé en janvier 2005.

ACTIVITÉS DE CONSULTATION DE LA COMMISSION ET REMERCIEMENTS

Experts rencontrés par la CEST :

- ***Thème de discussion : Aspects techniques de la biométrie et enjeux éthiques***

M. Bernard Dionne (aspects techniques) et **M^{me} Èvelyne Racette** (enjeux éthiques), professionnels de recherche, ministère des Relations avec les citoyens et de l'Immigration

- ***Thème de discussion : La construction de la peur et le catastrophisme***

M. Jacques de Guise, spécialiste de la communication, professeur retraité de l'Université Laval

M^{me} Hélène Denis, spécialiste de la gestion du risque, professeure retraitée de l'École Polytechnique de Montréal

- ***Thème de discussion : Terrorisme, sécurité, démocratie***

M. Benoît Gagnon, chercheur, Chaire Raoul-Dandurand en études stratégiques et diplomatiques, Université du Québec à Montréal

M. Albert Legault, titulaire de la Chaire de recherche du Canada en relations internationales, Université du Québec à Montréal

M. Kevin McGarr, directeur de la recherche, Administration canadienne de la sécurité du transport aérien (ACSTA), gouvernement du Canada

En avril 2005, les personnes suivantes ont accepté de procéder à une lecture critique d'une première version du document de réflexion de la Commission :

M. Max Chassé, spécialiste de la biométrie, Conseil du trésor (Québec)

M^{me} Jocelyne Couture, directrice des études des cycles supérieurs, département de philosophie, Université du Québec à Montréal

M. Raymond d'Aoust, commissaire adjoint, Commissariat à la protection de la vie privée (Canada)

M. Jérôme Gagnon, conseiller, Direction de la prévention et de la lutte contre la criminalité, ministère de la Sécurité publique (Québec)

M. Albert Legault, titulaire de la Chaire de recherche du Canada en relations internationales, Université du Québec à Montréal

M. Stéphane Leman-Langlois, criminologue, École de criminologie, Université de Montréal

M. Kevin McGarr, directeur de la recherche, Administration canadienne de la sécurité du transport aérien (ACSTA), gouvernement du Canada

M. Pierre Patenaude, professeur titulaire, Faculté de droit, Université de Sherbrooke

La Commission remercie toutes ces personnes. Par leur collaboration, elles ont contribué à l'enrichissement de son document de réflexion.

TABLE DES MATIÈRES

INTRODUCTION.....	1
1. LA NOTION DE « SÉCURITÉ ».....	1
2. LA TECHNOLOGIE BIOMÉTRIQUE.....	4
2.1 Quelques définitions utiles.....	4
2.2 Les secteurs d'utilisation de la biométrie.....	5
2.3 Les différentes technologies actuelles et en développement et leur mode de fonctionnement.....	6
2.4 Les atouts des technologies biométriques.....	7
2.5 Les failles des technologies biométriques.....	8
2.6 Une question d'importance : le stockage de l'information.....	11
2.7 Le marché de la biométrie.....	12
2.8 L'intérêt de la population canadienne.....	12
2.9 Éléments de réflexion.....	13
3. LE CONTEXTE DES APPLICATIONS BIOMÉTRIQUES : LA MISE EN PLACE DE MESURES DE SÉCURITÉ.....	15
3.1 La sécurité internationale : combattre le terrorisme.....	15
3.1.1 Le terrorisme international : une nébuleuse de plus en plus difficile à cerner.....	15
3.1.2 La menace terroriste : comme une épée de Damoclès.....	18
3.1.3 Les incidences des attentats du 11 septembre 2001 sur les démocraties : une tension entre la sécurité et les droits.....	19
3.1.4 La situation canadienne.....	21
3.1.5 La situation québécoise.....	23
3.1.6 Éléments de réflexion.....	24
3.2 La sécurité intérieure : garantir l'identité des personnes.....	24
3.2.1 Un problème majeur : le vol d'identité.....	25
3.2.2 Une nécessité : l'intégrité des documents officiels.....	26
<i>L'intégrité des documents primaires</i>	27
<i>L'intégrité des documents d'admissibilité</i>	27
3.2.3 Éléments de réflexion.....	29
3.3 La sécurité matérielle ou virtuelle : contrôler l'accès aux sites.....	30
3.4 La sécurité : une justification à la surveillance tous azimuts?.....	31
3.4.1 La vidéosurveillance.....	31
3.4.2 La cybersurveillance.....	33
3.5 Éléments de réflexion.....	34

4. L'ENCADREMENT NORMATIF	34
4.1 À l'échelle internationale	35
4.2 À l'échelle canadienne	35
4.3 À l'échelle québécoise	36
4.4 Éléments de réflexion	37
5. LE QUESTIONNEMENT ÉTHIQUE	38
5.1 Quelques considérations pour appuyer la réflexion	38
5.2 Des questions à poser et à débattre	39
5.2.1 ... sur le respect de la démocratie	40
5.2.2 ... sur le renversement du fardeau de la preuve	40
5.2.3 ... sur la validité d'une donnée biométrique	41
5.2.4 ... sur la protection des données personnelles : confidentialité et vie privée	41
5.2.5 ... sur le stockage et la gestion des données : accès, utilisation, divulcation	43
5.2.6 ... sur la discrimination	44
5.2.7 ... sur le manque de transparence : le consentement	44
5.2.8 ... sur le respect des finalités	45
5.2.9 ... sur la proportionnalité des moyens	46
5.2.10 ... sur l'instrumentalisation du corps humain	47
5.2.11 ... sur les effets sur la santé	47
5.2.12 ... sur l'encadrement normatif	48
5.2.13 ... sur les dérives possibles	48
CONCLUSION	49
BIBLIOGRAPHIE	51
ANNEXES :	
Annexe 1 – Profil des principales données biométriques	63
Annexe 2 – Questions d'intérêt public liées à la biométrie pour accroître l'intégrité des documents d'identité et de voyage	67
Annexe 3 – Données fournies sur les passagers aériens	69
Annexe 4 – Articles de lois cités dans le texte (extraits)	71
LISTE DES PUBLICATIONS DE LA CEST	79

Introduction

À n'en pas douter, les événements du 11 septembre 2001 ont changé la donne en matière de sécurité, que ce soit à l'échelle nationale ou internationale. Parce qu'ils estiment essentiel de le faire ou sous la pression des États-Unis – notamment dans le contrôle des voyageurs –, les gouvernements nationaux sont appelés à revoir comment s'exerce la sécurité sur leur territoire et quelles sont les mesures mises en place (ou à mettre en place) pour contrer le terrorisme.

Outre le terrorisme, cependant, les États doivent également contrer la criminalité sur leur territoire, notamment en ce qui a trait au vol d'identité à des fins de consommation et à l'usurpation d'identité dans l'obtention de services gouvernementaux offerts aux citoyens résidents. Comme d'autres gouvernements à travers le monde, le Canada est amené à considérer l'utilisation de données biométriques pour le contrôle de ses frontières. Mais il s'y intéresse aussi dans le cadre de la mise en place d'une politique nationale en matière d'identité souhaitant faire de la biométrie une partie intégrante des pièces d'identité délivrées par le gouvernement canadien.

L'application de technologies nouvelles dans l'implantation de moyens de surveillance des personnes et de contrôle de l'identité constitue donc l'essence des nouvelles approches gouvernementales, mais également organisationnelles en matière de sécurité – certaines entreprises y ayant recours dans le contrôle des accès à des sites matériels ou électroniques. Et ces technologies nouvelles, souvent intrusives – sur le plan du consentement, de la vie privée et de l'intégrité corporelle – reposent majoritairement sur la collecte et le stockage d'informations personnelles et l'utilisation de données biométriques.

C'est ce contexte d'une intensification des mesures de contrôle et de la disponibilité croissante de systèmes biométriques de toutes sortes pour établir ou valider l'identité d'une personne qui amène la Commission de l'éthique de la science et de la technologie à s'interroger sur les enjeux éthiques associés à une telle situation. Et à poser la question suivante, fondamentale sur le plan de l'éthique : y a-t-il corrélation entre les moyens de contrôle et de surveillance mis en place ou envisagés grâce à la technologie biométrique et la finalité recherchée?

Dans le présent *Document de réflexion*, la Commission s'interroge d'abord sur le concept de sécurité et son évolution dans le temps. Elle fait ensuite le point sur les aspects techniques de la biométrie, sur ses champs d'application et sur les encadrements normatifs (lois, règlements ou autres) qui permettent de baliser le domaine, pour ensuite signaler les enjeux éthiques que soulève l'application des technologies biométriques dans une société pluraliste et démocratique. Dans l'immédiat, la Commission n'entend cependant pas apporter de réponses au questionnement éthique qu'elle propose, mais désire soumettre le présent document de réflexion au débat public, par la voie d'une consultation des experts et de la population sur le sujet. Par la suite, un avis sur les enjeux éthiques associés à l'utilisation des données biométriques à des fins de sécurité, accompagné de recommandations à l'intention des divers acteurs concernés, sera remis au gouvernement et rendu public.

1. LA NOTION DE « SÉCURITÉ »²

Assurer la sécurité d'un territoire, d'un pays, d'une ville, d'une habitation est un défi constant car il faut d'une part déterminer correctement les menaces et, d'autre part, mettre en place un système efficace de protection. À l'heure actuelle, surtout depuis l'attentat de 2001, les paramètres du danger et de la sécurité semblent entièrement nouveaux et paraissent exiger l'adoption de mesures également nouvelles tant sur le plan technique que politique. La CEST estime toutefois opportun, dès le départ, de situer dans un contexte plus large la question de la sécurité.

² La Commission remercie Benoît Gagnon pour le texte de la présente section du document, ainsi qu'André Beauchamp pour sa collaboration d'appoint.

Qu'est-ce que la sécurité? Simplement poser la question met déjà en évidence la complexité du concept de sécurité. En effet, non seulement le terme renvoie à différentes notions, notamment sur le plan sociologique, mais son interprétation varie en fonction des langues, des discours et des approches. Quatre questions clefs jalonnent le débat sur la notion de sécurité : « Quelle est la nature de l'insécurité? »; « À quel objet la sécurité fait-elle référence? »; « Qui en assume la responsabilité? »; « Quels sont les moyens d'assurer la sécurité? »³.

Sur le plan individuel, non seulement la sécurité elle-même, mais le sentiment de sécurité semble important et s'inscrit comme un des déterminants de l'humanisation⁴. Dans ce contexte, il est possible d'affirmer que la sécurité fait référence à la survie. De prime abord, c'est pour éviter de subir des préjudices, physiques ou autres, menaçant notre vie que le besoin de sécurité se fait sentir⁵. Mais ce sentiment de sécurité suppose nécessairement la sécurité à l'extérieur; c'est donc fatalement au sein de son groupe que l'être humain trouve l'espace de sécurité qui lui permet de s'épanouir : famille, clan, cité, État. Cette protection du groupe exige en retour diverses formes de contrôles, contrôles contre l'ennemi extérieur mais aussi contrôles contre l'ennemi intérieur, le traître, le délinquant, le marginal. Les deux éléments sont toujours reliés. La surveillance de l'ennemi du dehors est inséparable de celle de l'ennemi du dedans.

Sur le plan sociétal, « la sécurité est conçue ou décidée par un groupe, une ethnie, un État ou une organisation internationale (il est rare qu'un individu puisse agir seul sur la sécurité)⁶. » Selon bon nombre de spécialistes, la définition sociétale de la sécurité ferait référence à trois éléments : la préservation des valeurs fondamentales, l'absence de menace, la formulation de mesures sociopolitiques visant à faire face à des mesures éventuelles⁷. Ainsi, le concept de sécurité est nécessairement lié à celui de danger : c'est parce qu'il y a un sentiment de danger face aux trois fondements de la sécurité que des mesures sécuritaires sont mises en place.

Or, ce qui est considéré comme une menace comporte deux dimensions⁸. Premièrement, une menace peut être réelle. Une attaque terroriste se produisant dans un autobus est une menace réelle. Toutefois, une menace peut aussi être perçue. La simple crainte de voir un attentat terroriste se produire peut être considérée comme une menace. Ce phénomène démontre donc le caractère subjectif de la menace. Deuxièmement, une menace peut avoir des effets directs, par la destruction et les morts par exemple. Ou encore, elle peut avoir des effets indirects, comme modifier la vision du monde d'un acteur tiers⁹.

Traditionnellement, la sécurité sociétale faisait référence au concept de sécurité nationale. La sécurité était définie par la stratégie, qui servait essentiellement à préserver la souveraineté nationale et à préserver ou à augmenter la puissance étatique par les moyens militaires, politiques et économiques. Dans cette vision des choses, « la source de la menace est donc de nature matérielle et s'appréhende objectivement par l'évaluation des capacités d'un État¹⁰. » Depuis la fin de la Guerre froide, on constate toutefois un élargissement du champ sécuritaire. Ainsi, on assiste à la croissance du spectre sécuritaire « [...] pour y inclure des menaces de nature économique,

³ Isabelle MASSON, « Sécurité », in Alex MACLEOD, Evelyne DUFAULT et F. Guillaume DUFOUR (dir.), *Relations internationales : théories et concepts*, Montréal, Athéna éditions, 2004, p.216.

⁴ Jacques RUFFIÉ, *De la biologie à la culture*. Paris, Flammarion, Collection Champs, no 128, 1983.

⁵ En psychologie humaine, la pyramide de Maslow est souvent employée pour classer les besoins humains par ordre d'importance. On y constate que le besoin de sécurité arrive très bas dans l'échelle des besoins, se situant juste au-dessus des besoins physiologiques de base comme manger, boire et dormir. Voir : WIKIPEDIA, *Pyramide des besoins*, [en ligne] http://fr.wikipedia.org/wiki/Pyramide_des_besoins

⁶ Charles-Philippe DAVID, *La guerre et la paix : approches contemporaines de la sécurité et de la stratégie*, Paris, Presses de science po, 2000, p. 31.

⁷ *Idem*.

⁸ *Ibid.*, p. 66.

⁹ Le meilleur exemple de cela est la façon dont le Canada a changé sa politique sécuritaire à la suite des attentats terroristes du 11 septembre 2001. Si ce sont les États-Unis qui ont subi les effets directs des attentats terroristes, les effets indirects du 11 septembre se sont fait sentir au Canada qui, comme d'autres pays ailleurs dans le monde, n'a eu d'autres choix que de se mettre au diapason de nouvelles politiques antiterroristes.

¹⁰ Isabelle MASSON, *op. cit.*, p.217.

environnementale ou « sociétale » ignorées par les études stratégiques¹¹. » Dorénavant, la souveraineté nationale n'est donc plus au centre des prérogatives sécuritaires; la sécurité transcende divers domaines et a des objectifs multiples.

La mise en place de mesures sécuritaires est appelée la sécurisation. De manière générale, il s'agit de l'application de mesures exceptionnelles – sur le plan qualitatif, non pas en termes de durée – dans certains domaines jugés critiques. La sécurisation s'inscrit donc dans un processus décisionnel. Certaines élites politiques identifient des enjeux comme étant des questions sécuritaires et établissent des mesures qui visent à « augmenter »¹² la sécurité.

Le processus de sécurisation se fait en cinq étapes : (1) la désignation d'un objet à sécuriser, (2) l'identification d'une menace – réelle ou perçue – qui est sous-tendue par un discours signifiant sa dangerosité, (3) la mise en place de mesures sécuritaires par des acteurs reconnus comme compétents à le faire, (4) la prise de mesures d'exception¹³ qui serviront à contrer la nouvelle menace, (5) l'acceptation de la nouvelle position sécuritaire par l'ensemble de la société.¹⁴

Conséquemment, ce qu'il est nécessaire de comprendre, c'est que la sécurisation est un élément défendant nécessairement une certaine vision de la société. En effet, puisque (1) ce sont certaines élites politiques – souvent des spécialistes de la sécurité – qui décident des éléments devant être considérés comme des enjeux sécuritaires et que (2) les menaces sont fréquemment perçues, – pas simplement réelles ou objectives – la sécurisation est un processus qui, bien souvent, est très subjectif. La sécurisation, c'est-à-dire la construction sécuritaire, passe donc nécessairement par un biais de valeurs et d'intérêts d'une élite dominante.

Ainsi, la sécurité apparaît à la fois comme un bien à atteindre, un bien indispensable à la vie, mais aussi comme une stratégie mise en œuvre pour que la sûreté soit acquise. Or cette stratégie, soit la sécurisation, suppose toujours des pouvoirs de contrôle, d'inclusion et d'exclusion qui renvoient à un ou à des enjeux politiques qui sont liés à des perceptions de l'environnement sécuritaire. En prétendant protéger, l'État en vient aussi à contrôler même au-delà du nécessaire. Ce contrôle, présenté comme une réponse à une demande d'accroissement sécuritaire, engendre donc un conflit permanent entre la requête de sécurité de l'individu qui demande au groupe d'assurer sa protection par tous les moyens et la requête de liberté suivant laquelle chaque personne peut disposer librement d'elle-même en toute circonstance.

Avec d'autres phénomènes contemporains¹⁵, les événements du 11 septembre 2001 contribuent à relancer la question de la perception des menaces et de l'instrumentalisation de la peur. Déjà en 1986, Beck définissait la société occidentale comme une société du risque : « Dans la société du risque se dessine ainsi par sauts petits ou grands [...] le *potentiel politique des catastrophes*. S'en prémunir et les gérer, voilà qui peut impliquer une *réorganisation du pouvoir et des attributions*. La société du risque est une société *de la catastrophe*. L'état d'exception menace d'y devenir un état normal¹⁶. » Dans ce contexte historique et anthropologique, la question du renouvellement des mesures de sécurité et de contrôle est indissociablement un défi technique et une question à caractère politique et éthique.

¹¹ *Idem*.

¹² Le fait étant que le « degré de sécurité » est difficilement quantifiable. Il est quasi impossible de savoir jusqu'à quel point l'être humain a « assez » de sécurité. À la limite, la sécurisation est absurde, car elle peut impliquer une recherche infinie de la sécurité.

¹³ Ces mesures d'exception passent souvent par des mesures de contrôle; des contrôles contre l'ennemi extérieur mais aussi des contrôles contre l'ennemi intérieur, la traître, le délinquant, le marginal. Les deux éléments sont toujours reliés. La surveillance de l'ennemi du dehors est inséparable de celle de l'ennemi du dedans. Ainsi, bien souvent, ces mesures d'exceptions constituent des entorses aux libertés fondamentales. Elles limitent les actions pouvant être effectuées par les individus étant subordonnés aux décideurs.

¹⁴ Barry BUZAN, Ole WEAVER et Jaap de WILDE, *Security: A New Framework For Analysis*, Londres, Lynne Rienner Publishers, 1998, p. 23-26.

¹⁵ Notamment les préoccupations liées à l'environnement (changements climatiques, pollution, etc.).

¹⁶ Ulrich BECK, *La société du risque : sur la voie d'une autre modernité*, Paris, Flammarion, Collection Champs, no 546, 2001 (1986), p. 43.

2. LA TECHNOLOGIE BIOMÉTRIQUE¹⁷

Mises à part l'utilisation des empreintes digitales dans le système judiciaire et, plus récemment, celle de lecteurs de la main comme moyens de contrôle de l'accès à ou dans certains édifices, les technologies biométriques sont généralement peu connues de la population. Qu'elles soient cependant mal connues ou peu connues, ces technologies n'en suscitent pas moins « fascination et inquiétude¹⁸ », pour reprendre les mots de Jennifer Stoddart, présidente de la Commission d'accès à l'information (CAI) jusqu'en 2004. La CEST s'efforce de démystifier quelque peu le sujet dans les paragraphes qui suivent.

2.1 Quelques définitions utiles

La biométrie. En français, il existe différentes acceptions du terme « biométrie »¹⁹. Sous l'influence de l'anglais, et dans le domaine de la sécurité, le terme en est venu à désigner les « techniques permettant d'identifier une personne à partir de l'un ou plusieurs de ses caractères biologiques ou comportementaux²⁰ ».

Un « **système biométrique** » devient donc une application technologique « permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main...), de traces (ADN, sang, odeurs) ou d'éléments comportementaux (signature, démarche)²¹ ».

Les « **données biométriques** » constituent, pour leur part, les informations à caractère morphologique, biologique ou comportemental propres à une personne. Il y a quelques années à peine, la technologie permettant de mesurer une diversité de caractéristiques biométriques et de les utiliser à des fins d'identification était relativement peu développée – hormis la technologie relative aux empreintes digitales, la plus courante et la plus ancienne. Aujourd'hui, aucun caractère biométrique ne semble exclu *a priori* et n'importe quelle caractéristique personnelle semble pouvoir se prêter à une mesure (à un niveau de fiabilité variable, cependant) par la technologie biométrique : différentes parties du corps, la voix, le geste, l'odeur, la chaleur corporelle, etc.

Les technologies de l'information. Le rôle des technologies de l'information est fondamental dans le traitement (notamment la numérisation de l'information « physique » qui est recueillie) et l'analyse des données, ainsi que dans l'interface qu'elles permettent d'établir avec les bases de données de toutes sortes sur les personnes (données d'identification personnelle, financières, médicales, etc.). Ces technologies permettent aux systèmes biométriques d'effectuer des traitements de masse quasi instantanément et avec un taux de fiabilité qui ne peut qu'augmenter dans les années à venir – tout comme leur « invisibilité », d'ailleurs, en s'intégrant de plus en plus dans notre environnement (les caméras de surveillance en sont un exemple pour le moment, ainsi que tous les moyens de contrôle qui peuvent être intégrés à un logiciel).

Identification/authentification. Dans le domaine de la sécurité, il convient de mentionner que la biométrie est utilisée à deux fins principales : l'**identification** d'une personne, et l'**authentification**

¹⁷ À l'amorce de ses travaux sur le sujet, la Commission a bénéficié de la collaboration du ministère des Relations avec les citoyens et de l'Immigration, grâce à un document d'information sur la biométrie et ses aspects éthiques préparé par Bernard DIONNE et Évelyne RACETTE : « La biométrie : présentation à la Commission de l'éthique de la science et de la technologie », mars 2004. Ce document a servi de point de départ au contenu de la présente section.

¹⁸ Jennifer STODDART, « Des technologies de surveillance sous surveillance », discours, [en ligne] septembre 2001 [http://www.cai.gouv.qc.ca/05_communique_et_discours/discours_24_09_01.html]

¹⁹ Dont, notamment, « science des variations biologiques, des phénomènes qui s'y rattachent et des problèmes qui en découlent », Eugène SCHREIDER, article sur la biométrie dans l'*Encyclopaedia Universalis*.

²⁰ *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en oeuvre*, OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, Christian CABAL, député, Sénat, Assemblée nationale (France), juin 2003, p. 7.

²¹ Définition de la Commission nationale de l'informatique et des libertés (CNIL – France), rapportée dans OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, note 6, p. 8.

d'une personne (ou la vérification de son identité). Avec le développement d'applications de masse, cependant – qui rendront possible la constitution de bases de données biométriques concernant des millions de personnes – une troisième utilisation, le « dépistage » (ou « screening »), pourrait prendre de l'ampleur.

Dans le contexte de l'**identification**, la question suivante est posée : **Qui est cette personne?** et donne lieu à une recherche de type « un à plusieurs » dans une base de données, centralisée ou intégrée au système, souvent dans un contexte judiciaire – par exemple, à partir d'empreintes digitales, avec pour objectif de découvrir l'identité d'une personne (victime d'un crime ou ayant laissé des traces sur le lieu d'un crime).

Dans le contexte de l'**authentification ou de la validation** d'identité, il s'agit de demander : **Cette personne est-elle bien celle qu'elle prétend être?** et donne lieu à une recherche de type « un à un » – il doit y avoir concordance de l'information fournie avec une information déjà colligée sur un support quelconque (informatisé ou non)²², comme dans le cas de droits d'accès à des installations matérielles à partir de la lecture de la main, de l'iris ou d'empreintes digitales. Ce type de recherche « un à un » ne permet pas la traçabilité et le profilage des personnes, c'est-à-dire de cibler des personnes ou des groupes à partir de certaines caractéristiques biométriques. L'identité d'une personne est validée ou confirmée au moment où cette personne requiert un service ou un accès préalablement autorisé.

La distinction entre ces deux finalités est importante car, selon la caractéristique biométrique retenue et son mode de stockage (information centralisée dans une base de données ou inscrite sur un support informatique ou non), mais aussi selon les objectifs poursuivis, le risque pour la protection de la vie privée et des renseignements personnels pourra différer.

En ce qui a trait au dépistage, la question posée pourrait être : **Où est cette personne?** Le procédé permet notamment de confronter les données contenues dans une liste de personnes sous surveillance (criminels, terroristes, activistes, etc.) avec le contenu de bases de données biométriques d'une vaste population (les photos numérisées des passeports, par exemple, ou à partir de caméras de surveillance)²³ afin d'en tirer toute information pouvant contribuer à appréhender un criminel ou un suspect²³.

2.2 Les secteurs d'utilisation de la biométrie

Trois secteurs sont particulièrement concernés par l'utilisation de la biométrie²⁴ :

- ***l'identification judiciaire***
répression du crime : identification de criminels, de terroristes, etc.
- ***la gestion des titres délivrés (ex. passeport, permis de conduire, etc.)***
la biométrie peut éviter un usage frauduleux de documents, mais aussi renforcer la fiabilité du titre délivré.
- ***la gestion des accès physiques et virtuels***²⁵
contrôle de l'accès à des locaux, des sites physiques ;
contrôle de l'accès à des équipements informatiques (matériels et logiciels) ;
contrôle de l'accès à des applications de chiffrement (données encryptées).

²² Information tirée, entre autres, de «Biométrie : incidences et applications pour la citoyenneté et l'immigration», document d'information, Forum tenu par CITOYENNETÉ ET IMMIGRATION CANADA, 7 et 8 octobre 2003, Ottawa, Canada, p.2.

²³ *Biometrics at the Frontiers : Assessing the Impact on Society*, For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS), Technical Report Series, 2005, p.39,40.

²⁴ Bernard DIONNE et Évelyne RACETTE, *op. cit.*

²⁵ À noter que ce type de contrôle peut être utilisé dans la gestion de la paye en permettant de vérifier l'assiduité du personnel et l'utilisation qui est faite de l'équipement informatique.

À ces catégories peut s'en ajouter une quatrième :

- **le contrôle des responsables de la sécurité**

opérations nécessaires à l'attribution d'une responsabilité relative au maintien de la sécurité de sites physiques ou virtuels.

2.3 Les différentes technologies actuelles et en développement et leur mode de fonctionnement

Les systèmes biométriques peuvent être classés en fonction de trois catégories de données particulières à une personne²⁶:

- **les données morphologiques ou physiologiques :**

Cette catégorie s'appuie sur l'identification de traits physiques qui sont uniques et permanents chez une même personne. Les éléments retenus pour fins d'identification biométrique sont généralement reconnus pour leur stabilité et ne subissent pas autant les effets du stress ou du vieillissement, par exemple, que les traits comportementaux²⁷. La biométrie morphologique ou physiologique regroupe notamment la reconnaissance des empreintes digitales, de la forme de la main, de la forme du visage, de la voix, de la rétine (dessin du réseau veineux du fond de l'œil), de l'iris de l'œil et la thermographie.

- **les données comportementales :**

Cette catégorie est fondée sur l'analyse d'actions répétitives et usuelles du comportement humain. La prémisse à ce type d'analyse est que le comportement de chacun constitue une signature personnelle. Certains mouvements chez une personne lui sont propres et peuvent confirmer son identité. La biométrie comportementale comprend la dynamique de la signature, de la frappe au clavier d'ordinateur, la façon de marcher, etc.

- **les données biologiques :**

Cette catégorie recourt à l'analyse de traces biologiques, comme l'empreinte génétique (ADN), l'odeur, la salive, l'urine, etc.

La Commission présente à l'annexe 1 une compilation des avantages, inconvénients et applications des données biométriques suivantes : l'empreinte digitale, la reconnaissance faciale, la géométrie de la main, la reconnaissance de l'iris, la reconnaissance de la rétine, la reconnaissance de la voix, la vérification de signature, la dynamique de la frappe au clavier, le profil génétique (ADN) et la thermographie.

En matière de fonctionnement, tous les systèmes biométriques fonctionnent en deux temps et comportent deux processus :

- **l'enregistrement d'un utilisateur;**
- **le contrôle d'un utilisateur.**

²⁶ Bernard DIONNE et Èvelyne RACETTE, *op. cit.* Il convient toutefois de souligner qu'il peut exister des systèmes de surveillance qui ne comportent pas de phases d'enregistrement tout en permettant une analyse de comportements à risques (surveillance vidéo d'un stationnement, par exemple, et repérage d'un voleur potentiel à partir de ses agissements).

²⁷ Dans un récent rapport de la London School of Economics & Political Science, cette assertion est cependant nuancée pour souligner les effets du vieillissement, non seulement sur la transformation des données biométriques mais aussi dans l'utilisation des moyens techniques mis en place pour la lecture de ces données (tremblements, arthrite, cataractes, paupières tombantes, etc.). Le rapport souligne aussi qu'aucune étude scientifique n'a été réalisée sur la stabilité des caractéristiques biométriques dans le temps. Voir LONDON SCHOOL OF ECONOMICS & POLITICAL SCIENCE, *The Identity Project. An assessment of the UK Identity Cards Bill & its implications*, Interim Report, Project Management by enterprise privacy group, Department of Information Systems, March 2005, p. 49.

Ces deux processus comprennent cinq étapes essentielles au bon déroulement de l'opération²⁸ :

1. **la saisie de l'information à analyser** – lecture de certaines caractéristiques physiologiques, comportementales ou biologiques d'une personne, au moyen d'un terminal de capture biométrique (ou capteur biométrique);
2. **le traitement de l'information** – la transformation de l'information en données numériques;
3. **la création d'un fichier « signature » et son enregistrement** – l'utilisation des données numériques pour créer un modèle ou gabarit qui représente la donnée biométrique captée, c'est-à-dire la signature qui sera conservée sur un support portable (puce ou autre) ou dans une base de données et utilisée pour fins de comparaison;
4. **la comparaison** – les caractéristiques biométriques d'une personne soumise à contrôle (volontairement ou à son insu) sont comparées à la « signature » mémorisée; l'identité de l'utilisateur correspond à l'identité proclamée ou recherchée ; ou elle ne correspond pas;
5. **la décision** – l'opérateur du système ou le système informatisé détermine si l'identité de l'utilisateur correspond ou non à l'identité proclamée (authentification) ou recherchée (identification).

Les techniques biométriques s'appuient sur le principe qu'il est possible de relier une donnée à une personne. Ce principe couvre l'unicité du caractère biométrique choisi et l'unicité de la mesure ou de la représentation graphique de ce caractère, l'un comme l'autre étant propres à une seule et même personne. Parce que l'unicité d'une donnée biométrique n'a jamais été scientifiquement démontrée, la biométrie repose sur des méthodes statistiques destinées à déterminer la probabilité que deux personnes présentent la même donnée (généralement très faible pour la plupart des données biométriques actuelles sauf pour les jumeaux identiques, nulle pour l'iris – les deux iris d'une même personne sont d'ailleurs différents).

Toutes les études insistent sur le caractère crucial de la phase d'enregistrement. Plus les personnes collaborent au processus, plus les systèmes biométriques sont efficaces.

2.4 Les atouts des technologies biométriques

Comme le souligne la Commission d'accès à l'information, « la biométrie est présentée au grand public comme un remède universel propre à terrasser plusieurs maux : terrorisme, fraude, vol d'identité et atteinte à la vie privée, pour n'en citer que quelques-uns. Aux employeurs elle est présentée comme une solution au vol de temps par les travailleurs, comme un moyen facile de produire les données de base servant au calcul de la paye. Aux utilisateurs elle est présentée comme un moyen confortable de s'identifier; plus de cartes qu'on égare et de mots de passe qu'on oublie²⁹. »

Dans son rapport présenté au Sénat français, le député Cabal note que les systèmes biométriques constituent un instrument efficace de lutte contre la fraude – fraude électronique et usage frauduleux de documents (à l'échelle mondiale, des milliards de dollars pour les cartes de crédit), pour assurer la sécurité des échanges financiers et commerciaux, l'accès légitime aux services gouvernementaux, et contrer le vol d'identité sous toutes ses formes³⁰.

Dans l'ensemble, les technologies biométriques sont présentées par leurs promoteurs comme des mécanismes de protection pouvant garantir qu'en aucun cas les caractéristiques personnelles qui

²⁸ Bernard DIONNE et Èvelyne RACETTE, *op. cit.*, et « La biométrie au Québec : Les enjeux », préparé par Max Chassé, document d'analyse, COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, juillet 2002, p. 8 et 9.

²⁹ COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Les enjeux...*, *op. cit.*, p. 23.

³⁰ OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES (France), *op. cit.*, p. 46-51.

sont analysées ne peuvent être utilisées à d'autres fins que celles recherchées par le système d'information, pour les raisons suivantes ³¹ :

- unicité de la donnée biométrique;
- mécanisme de chiffrement fort, pour assurer la confidentialité;
- fonctions de traitement à sens unique, pour assurer l'anonymat. Cette fonction est un processus d'enregistrement qui ne permet pas la régénération de l'image du doigt, du visage, de la main, du code génétique, de la couleur, etc. Ainsi, l'analyse du fichier signature seul ne permet pas d'identifier la personne concernée (ou de découvrir une pathologie quelconque);
- mécanisme de signature des fichiers références, pour garantir leur authenticité et leur intégrité;
- mécanismes pour contrer la falsification.

Pour les tenants des technologies biométriques, leur utilisation présente les possibilités suivantes ³² :

- améliorer la sécurité des personnes (ou réduire la détresse des victimes) ;
- protéger efficacement les données personnelles;
- lutter efficacement contre la fraude, parce que chaque personne possède ses propres caractéristiques physiques, comportementales ou biologiques qui ne peuvent être ni perdues, ni volées;
- contrer la prolifération des mots de passe et la nécessité de les mémoriser – d'autant plus que les gens ont souvent tendance à les inscrire quelque part ou à utiliser des mots de passe ou des NIP facilement devinables (date de naissance, nom d'un enfant, etc.);
- contrer le « social engineering » – une pratique par laquelle les pirates informatiques se font passer pour un spécialiste, un technicien ou une personne en autorité pour subtiliser l'identifiant personnel ou le mot de passe d'une personne.

2.5 Les failles des technologies biométriques

En ce qui a trait aux failles (ou aux inconvénients) des technologies biométriques, les arguments soulevés par les opposants concernent davantage les systèmes d'information et sont liés ³³ :

- aux menaces de la collecte non nécessaire;
- au traitement (risque de restreindre les libertés individuelles);
- à la communication (non autorisée) des informations;
- à l'interconnexion des bases de données facilitée par le recours à un identifiant unique (finalité); et
- au coût.

Par rapport aux caractéristiques de la biométrie, les principaux arguments des opposants sont les suivants ³⁴ :

- information intrinsèquement liée à la personne (possibilité de découvrir des maladies);
- nécessité de se soumettre physiquement au processus de vérification (méthode considérée intrusive);
- difficulté de se défaire de ses caractéristiques biométriques (unicité de la donnée) et difficulté d'apporter la preuve que la personne n'a pas commis les actes qui lui sont imputés en cas de falsification (faux élément biométrique) ou d'usurpation (vol du fichier de signature) d'identité;

³¹ Bernard DIONNE et Èvelyne RACETTE, *op. cit.*

³² *Ibid.*

³³ *Ibid.*

³⁴ *Ibid.*

- comparaison biométrique qui apporte un taux d'incertitude sur la validité du client accepté (fausse acceptation) ou refusé (faux rejet), au contraire de l'utilisation des systèmes traditionnels d'authentification, tels le mot de passe ou le jeton, qui produisent une réponse sûre à 100 % (vrai ou faux). La difficulté est de trouver un compromis acceptable entre l'exigence de sécurité (haut taux de faux rejets) et la nécessité d'un système plus «convivial» (haut taux de fausses acceptations).

L'avantage de l'unicité de la donnée biométrique peut cependant devenir une vulnérabilité. Contrairement à un mot de passe, un certificat électronique ou une clé de chiffrement, il est difficile de modifier une donnée biométrique recueillie pour identifier une personne – une fois cette donnée volée ou usurpée, son véritable propriétaire peut difficilement faire la preuve qu'il en est bien le propriétaire légitime. En outre, les techniques biométriques peuvent elles aussi être trompées par des artifices, même lorsqu'il y a présence de mécanismes pour contrer la falsification (par exemple, un moulage de doigt ou un doigt amputé à son propriétaire dans le cas des empreintes digitales, une photo de l'iris pour la reconnaissance de l'iris). Et plus les mécanismes de contre-mesure se développeront, plus les techniques de falsification gagneront en sophistication.

Pour résumer quelque peu l'information apportée sur les données biométriques dans la présente section, le tableau qui suit fournit une synthèse des principaux critères relatifs aux différentes technologies mises au point ou à venir, tels que rapportés par l'Office d'évaluation des choix scientifiques et technologiques (France) et par l'OCDE. Il est important de noter qu'il s'agit d'un domaine en évolution très rapide; c'est donc dire que les «performances» mentionnées dans le tableau ont pu s'améliorer depuis le moment de l'évaluation d'une technique particulière. En outre, de nombreuses nuances pourraient sans doute être apportées aux évaluations qui sont rapportées dans ce tableau, notamment au regard de la fiabilité.

Enfin, une société américaine – l'*International Biometric Group* – propose le classement suivant de huit techniques biométriques³⁵ :

- « des techniques les moins "intrusives" aux plus "intrusives"³⁶: la voix, la frappe sur le clavier, la signature, la main, la face, l'empreinte digitale, l'iris et enfin la rétine.
- des techniques les plus fiables aux moins fiables: l'iris, la rétine, l'empreinte digitale, la face, la main, la voix, et enfin à un niveau équivalent, la frappe sur le clavier et la signature.
- des techniques les moins chères aux plus chères: la frappe sur le clavier, la voix, la signature, l'empreinte digitale, la face, la main, la rétine et enfin l'iris.
- des techniques les plus faciles d'utilisation aux plus difficiles: la face, la signature, l'iris, la frappe sur le clavier, la voix, l'empreinte digitale, la main et enfin la rétine. »

³⁵ Voir OFFICE PARLEMENTAIRE D'ÉVALUATION ..., *op. cit.*, p. 40.

³⁶ Précisons qu'il s'agit ici de l'intrusion sur le plan physiologique et non en matière de collecte de renseignements personnels.

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 OCDE⁴⁴

³⁷ Parce qu'elle ne peut être réalisée sur le champ, l'analyse de l'ADN ne fait pas partie des données biométriques de ce tableau. Toutefois, l'évolution de la technologie devrait pallier cette contrainte à plus ou moins court terme. La reconnaissance de la démarche est également absente du tableau, les sources utilisées n'en ayant pas fait l'évaluation.

³⁸ La robustesse indique le degré de stabilité de l'élément biométrique pendant une période donnée; cf. OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, p. 37.

³⁹ L'unicité indique la capacité de discrimination d'un individu par rapport à un autre; cf. *Ibid.*

⁴⁰ La fiabilité considère les taux d'erreur : fausses acceptations et faux rejets.

⁴¹ Sur la base de la robustesse, de l'unicité et de la fiabilité, le potentiel biométrique permet d'apprécier la sécurité qu'apporte l'élément biométrique utilisé; cf. OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, p.37.

⁴² Les données concernant l'acceptabilité des personnes relativement à la technique mentionnée, le coût et les applications sont tirées de l'OEDC (OCDE), *Biometric-Based Technologies*, Working Party on Information Security and Privacy, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, Paris, 28 avril 2004.

2.6 Une question d'importance : le stockage de l'information

Il existe différentes façons de conserver l'information contenue dans une donnée biométrique (la « signature ») pour ensuite la récupérer dans un contexte d'authentification ou d'identification de son propriétaire :

- dans une puce intégrée à un document : des renseignements de base peuvent être inscrits sur la carte, des données biométriques et autres informations confidentielles sont intégrées dans une micro-puce; il y a cependant possibilité de double inscription de l'utilisateur pour recevoir des services en double, par exemple, ou d'acquisition frauduleuse de documents au moyen du signalement de perte ou de vol de document; ce type de support «portable» ne permet pas l'identification d'une personne (1 sur n) mais uniquement l'authentification (1 sur 1) car l'information est détenue exclusivement par la personne concernée et n'est présente dans aucune base de données externes. Support utilisé pour les guichets automatiques et l'accès à des locaux, par exemple.
- dans le lecteur du système de captation : étant donné la capacité de stockage limitée de ce type d'équipement, cette façon de faire est rarement utilisée; la plupart des capteurs sont conçus pour la lecture des puces et la comparaison de la «signature» (fichiers numérisés de l'empreinte digitale, de la photo ou de l'iris numérisés) avec l'original capté en temps réel. Support utilisé dans les aéroports, les ports et aux postes-frontières, par exemple⁴⁵.
- disque dur d'un système de captation portable : permet la vérification de ses données personnelles par un client et la possibilité pour le propriétaire du système de détecter les inscriptions multiples et les tentatives de fraude; les défis sont moins complexes que dans le cas d'une base de données en ligne. Support utilisé dans des firmes privées, par exemple, ou de grandes infrastructures comme les aéroports, les gares, les centrales nucléaires, etc.
- dans un fichier central qui ne contient aucune autre donnée d'identification que la « signature » captée : support équivalent à une puce, mais logé dans un système informatisé, qui ne peut donc permettre que l'authentification d'une personne; dans une telle architecture, le propriétaire du système pourrait cependant réaliser des comparaisons avec d'autres bases de données contenant le même type de mesures ou caractéristiques biométriques, afin d'y chercher l'identité des personnes dont il détient la «signature»; il pourrait aussi céder ou communiquer la base à un tiers qui aurait des intentions malveillantes⁴⁶.
- une base (ou dépôt) de données en ligne : reposant sur les services d'un serveur, ce support présente les plus grands défis pour la sécurité et la gestion des données biométriques, la disponibilité et la fiabilité de la base de données, le besoin en ressources et infrastructures supplémentaires; il permet cependant l'identification et l'authentification d'un client dans tous les points de service prévus et l'échange de renseignements avec les partenaires disposant d'une technologie compatible. Support utilisé pour les passeports et les visas, par exemple.

Comme le souligne un groupe de travail de la Commission européenne, « en principe, l'enregistrement des données de référence dans une base de données n'est pas nécessaire aux fins de l'authentification/vérification; un stockage décentralisé des données à caractère personnel est suffisant. En revanche, l'identification n'est réalisable qu'avec un stockage centralisé des données de référence, parce que, pour vérifier l'identité de la personne concernée, le système doit comparer le modèle [la « signature »] ou les données brutes (image) de cette personne avec ceux de toutes les personnes dont les données sont déjà enregistrées dans une mémoire centrale⁴⁷. »

⁴³ *Op. cit.*, p. 38 et 39.

⁴⁴ *Op. cit.*, p. 36.

⁴⁵ « Biométrie dernier cri », Jean-Marc PAPINEAU, Dossier informatique, *Plan*, la revue de l'Ordre des Ingénieurs du Québec, octobre 2004, p.17.

⁴⁶ COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *op. cit.*, p. 33.

⁴⁷ « Document de travail sur la biométrie », Groupe de travail 'article 29' sur la protection des données, COMMISSION EUROPÉENNE, 12168/02/fr, GT 80, [en ligne] 1^{er} août 2003, p. 5. [\[http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_fr.pdf\]](http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_fr.pdf)

2.7 Le marché de la biométrie

Selon Citoyenneté et Immigration Canada, les recettes de l'industrie biométrique totalisaient 601 millions \$US en 2002, pour une estimation de 4 milliards \$US d'ici 2007, en raison de l'intérêt croissant des gouvernements et des firmes pour cette technologie⁴⁸. En août 2004, Industrie Canada estimait qu'environ 200 entreprises se partagent les trois grands créneaux des technologies de la sécurité au Canada : authentification, biométrie et cyber-protection, dont le tiers dans la grande région montréalaise⁴⁹. Ce marché est en pleine expansion et peut exercer une pression sur la prise de décision relative à l'utilisation des données biométriques à des fins de sécurité. La Commission n'a pas exploré cet aspect de la question de façon exhaustive, mais souhaite néanmoins aborder le sujet pour en saisir les incidences éventuelles sur le plan du questionnement éthique.

Le marché est reconnu pour être difficile à appréhender dans sa globalité⁵⁰ car il est fragmenté en fonction des données biométriques privilégiées et du type de système développé (grands systèmes d'identification portant sur les empreintes digitales, par exemple, qui représentent environ 50 % du marché, et petits terminaux ou capteurs biométriques destinés à différentes données biométriques). Sur le plan international, le secteur est largement dominé par les sociétés américaines et la technologie relative aux empreintes digitales.

Compte tenu des objectifs de modernisation et d'harmonisation des instruments d'identification judiciaire afin d'assurer une meilleure coopération entre les États, mais aussi dans la perspective où plusieurs gouvernements envisagent de doter leurs citoyens et résidents de titres biométriques, l'industrie de la biométrie a le vent dans les voiles. Certains estiment, cependant, que le besoin de normalisation du secteur pourra jouer un rôle dans la compétition⁵¹. La normalisation (ou standardisation), dont les objectifs répondent aux préoccupations du gouvernement américain, a pour but de faciliter les échanges et l'interopérabilité (accès à de l'information ou à des bases de données par différents systèmes) des systèmes biométriques – et donc la comparaison de données, d'éviter que les utilisateurs soient dépendants de systèmes propriétaires, d'harmoniser les méthodes et les principes d'évaluation des performances et de déterminer les outils nécessaires pour assurer la sécurité des frontières⁵². Les enjeux de la normalisation sont à la fois politiques et économiques; il est d'ailleurs permis de croire que les pays disposant des meilleures technologies seront sans doute à même d'imposer leurs propres exigences en matière de protection des renseignements personnels et de respect de la vie privée.

2.8 L'intérêt de la population canadienne⁵³

Un sondage téléphonique a été réalisé auprès de la population canadienne en novembre 2002 sur la possibilité d'instaurer une carte d'identité nationale avec des données biométriques. En février 2003, ce sont 16 groupes de consultation composés de citoyens et de résidents permanents qui ont eu à se prononcer sur le sujet. En octobre 2003, Citoyenneté et Immigration Canada tenait un forum public sur les incidences et les applications de la biométrie pour la citoyenneté et l'immigration, et en publiait les actes par la suite.

Il ressort du sondage que les Canadiens sont majoritairement favorables à la mise au point d'une carte d'identité munie d'un identificateur biométrique comme les empreintes digitales ou la numérisation oculaire afin de réduire l'utilisation frauduleuse des documents d'identité (73 %) et

⁴⁸ CITOYENNETÉ ET IMMIGRATION CANADA, Document d'information, *op. cit.*, p. 6 – il a été impossible de trouver l'information qui aurait permis une mise à jour de ces données.

⁴⁹ Voir Industrie Canada, « L'industrie canadienne de la sécurité : centres d'activité » [en ligne] http://strategis.ic.gc.ca/epic/internet/inict_c-g_tic.nsf/fr/tk00526f.html

⁵⁰ Voir particulièrement OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, 2^e partie, p. 49.

⁵¹ *Ibid.*, p. 48.

⁵² *Ibid.*, p. 52.

⁵³ L'information est tirée de CITOYENNETÉ ET IMMIGRATION CANADA, Document d'information, *op. cit.*, p. 10.

pour les passeports ou autres documents d'accessibilité aux programmes gouvernementaux (80 %). Malgré tout, certains croient que l'utilisation de cette technologie irait à l'encontre des valeurs de liberté et d'équité (36 %) et nuirait à la protection des renseignements personnels (53 %).

Dans le cas des groupes de consultation, les participants en faveur de l'instauration d'une carte avec données biométriques y voyaient les avantages suivants : augmentation de la sécurité, amélioration du contrôle de l'immigration et des frontières, réduction de l'utilisation frauduleuse des programmes gouvernementaux, leadership pour le Canada en matière de technologie d'identification. Les opposants soulevaient les points suivants : des préoccupations à l'égard des coûts, l'atteinte à la vie privée et à la liberté, la gestion du système, des résistances à l'égard d'un programme de sécurité dirigé par les États-Unis.

Des mémoires sur le sujet ont également été présentés au Comité permanent de Citoyenneté et Immigration Canada et attestent clairement que les Canadiens veulent être assurés que la biométrie serait « utilisée conformément aux principes de protection de la vie privée généralement reconnus et conformément aux valeurs canadiennes⁵⁴ ». Certains craignent le caractère intrinsèquement intrusif de la biométrie, qui peut toucher des aspects intimes de la personne, comme son état de santé – lecture de l'iris et diabète ou hypertension, empreintes digitales et syndromes de Down ou de Turner –, ainsi que ses répercussions possibles sur les libertés fondamentales. La création d'une « infrastructure de surveillance » fait également partie des préoccupations mentionnées, et toute intrusion de l'État est perçue « comme une action répréhensible, une invasion de l'espace privé, et l'antithèse des principes d'une société libre et ouverte où les valeurs sont tout aussi importantes que l'avancement des technologies⁵⁵. »

La tenue du forum visait les objectifs suivants :

- « explorer la biométrie comme une technologie puissante susceptible de faciliter l'atteinte de futurs objectifs stratégiques importants;
- améliorer et élargir le débat actuel sur les aspects techniques et sociaux reliés à l'utilisation de la biométrie à l'appui de l'intégrité des documents et de la vérification de l'identité;
- comparer les avantages et les inconvénients d'une approche globale de la « carte d'identité nationale » par rapport à une stratégie plus progressive qui consisterait à améliorer les nombreux documents d'identité existants;
- engager un dialogue sur les questions importantes avant la mise en œuvre de toute politique⁵⁶. »

Choisis pour apporter le plus grand nombre de points de vue, de positions et d'opinions sur l'identité, le respect de la vie privée et d'autres questions connexes, les participants ont conclu les débats en reconnaissant qu'il fallait une solution « typiquement canadienne » au problème des documents d'identité et une collaboration avec les provinces et les territoires pour élaborer une approche nationale en la matière. À l'annexe 2, la Commission présente un résumé du questionnaire proposé dans le cadre du forum et un extrait des principales conclusions qui en ont découlé.

2.9 Éléments de réflexion

Le présent tour d'horizon sur les technologies biométriques amène la Commission à considérer l'importance de divers facteurs au regard de l'utilisation des données biométriques :

- le niveau de fiabilité des différentes techniques utilisées – les fausses acceptations et les faux rejets : une fiabilité à près de 100 % avec l'ADN⁵⁷, possibilités de falsification avec les

⁵⁴ *Ibid.*, p. 16

⁵⁵ *Ibid.*

⁵⁶ CITOYENNETÉ ET IMMIGRATION CANADA, *Biométrie : incidences et applications pour la citoyenneté et l'immigration*, Actes du forum tenu à Ottawa les 7 et 8 octobre 2003, p. 2.

empreintes digitales, une fiabilité très faible pour la dynamique de frappe au clavier, la signature, la reconnaissance vocale;

- le perfectionnement des techniques utilisées qui a pour résultat de modifier à la fois les méthodes d'observation des personnes (sur une grande échelle) et de traitement de l'information colligée – avec accès à un nombre infini de bases de données locales, nationales ou internationales;
- la grande diversité des méthodes d'identification/authentification utilisées;
- la possibilité d'effectuer des traitements de masse rapidement, voire quasi instantanément (prévue également pour l'analyse d'ADN), parfois à l'insu des personnes concernées;
- l'élargissement des domaines d'application – de militaires et judiciaires qu'ils étaient, ces domaines couvrent de plus en plus la citoyenneté, le tourisme, le milieu de travail, les transactions commerciales et financières, la santé, l'éducation⁵⁸, etc.;
- la diversité du cadre spatial dans lequel ces technologies s'inscrivent : du local à l'international, à l'intérieur d'un bâtiment ou pour la circulation transfrontalière.

Considérant l'impact de ces divers facteurs, le questionnement actuel sur l'implantation de systèmes de sécurité nationale fondés sur l'utilisation des données biométriques est donc à la fois

- **de nature technique** : un questionnement sur la fiabilité, la performance comparée des systèmes avec les mécanismes qui existent actuellement, les rapports coûts/bénéfices, les finalités recherchées;
- **de nature politique** : à quel besoin national répond le recours à des systèmes biométriques? s'agit-il d'une décision à caractère national ou international? souhaite-t-on la mise en place d'une société « sous surveillance » (ou peut-être « sous influence »...)
- **de nature juridique** : à quel point la société dispose-t-elle d'un encadrement législatif qui protège la population d'une utilisation abusive de ses renseignements personnels et d'une ingérence dans sa vie privée? la mise en place d'instruments internationaux en la matière représente-t-elle un atout ou le risque de voir s'atténuer les droits acquis?

Mais il est en grande partie **de nature éthique** : Est-il acceptable qu'au nom de la sécurité des biens et des personnes les gouvernements puissent accéder aux données biométriques à caractère personnel des citoyens et qu'ils puissent le faire à d'autres fins que celles pour lesquelles elles ont été initialement fournies? Est-il acceptable de passer d'un mode sécuritaire « réactif » (fondé sur le consentement) à un mode « proactif » qui favorise l'utilisation de systèmes d'information en facilitant la collecte de renseignements personnels? De telles mesures de contrôle sont-elles proportionnelles aux finalités recherchées : contrer le terrorisme international, la criminalité et l'usurpation d'identité à l'intérieur du pays?

C'est ce questionnement qui a amené la Commission de l'éthique de la science et de la technologie à produire le présent document de réflexion dans le but de bien saisir les tenants et aboutissants de l'utilisation des données biométriques à des fins de sécurité et, ultérieurement, à produire un avis qui lui permettra d'exprimer son point de vue sur le plan éthique et de formuler des recommandations à l'intention des acteurs concernés.

⁵⁷ Sur le plan scientifique et indépendamment des erreurs humaines lors de la collecte ou de l'analyse des échantillons.
⁵⁸ Certaines cantines scolaires, en Europe, ont implanté un système de lecture du contour de la main afin de contrôler l'accès des élèves à la cantine. Voir Thierry DUPONT, « À Angers, c'est biométrie tous les jours à la cantine des écoles cathos » [en ligne] 9 septembre 2003 <http://www.transfert.net/a9255>

3. Le contexte des applications biométriques : la mise en place de mesures de sécurité

La revue de littérature qu'a réalisée la Commission démontre que le sujet de l'utilisation des données biométriques à des fins de sécurité nationale et internationale est d'actualité et que plusieurs gouvernements dans le monde se penchent sur la question. De l'avis général, les consensus en la matière sont difficiles à réaliser et les décisions auront, dans certains cas, une portée internationale (c'est déjà le cas avec les exigences américaines en matière de passeport).

Mais la recherche de sécurité consiste aussi à vouloir protéger la population contre la criminalité quelle qu'elle soit. Le vol et l'usurpation d'identité font de plus en plus de ravages et représentent des pertes de milliards de dollars chaque année à l'échelle mondiale. Le recours à la technologie biométrique pour vérifier et confirmer l'identité des personnes représente-t-il une solution valable pour aider à contrer ce fléau?

En outre, il y a aussi des espaces physiques et virtuels dont les accès doivent être protégés et contrôlés. Plutôt que les cartes d'accès et les mots de passe – souvent perdus et oubliés, si ce n'est volés – la lecture d'un doigt, de la main, de l'iris ne constitue-t-elle pas le « sésame, ouvre-toi » par excellence, toujours disponible? Et pourquoi ne pas aussi surveiller en permanence ce qui se passe sur les voies publiques pour rendre les lieux plus sûrs? et surveiller les travailleurs, pour s'assurer que leur temps de travail est utilisé à bon escient?

Bref, la mise en place de mesures de sécurité peut s'avérer nécessaire et inévitable dans certains cas; mais jusqu'où aller? Et à quel point ces mesures, quand elles reposent sur l'utilisation des données biométriques et la collecte de renseignements personnels, peuvent-elles être considérées intrusives et sont-elles acceptables dans une société démocratique et pluraliste?

3.1 La sécurité internationale : combattre le terrorisme

Depuis le 11 septembre, un grand nombre de pays se posent la même question : comment échapper aux attentats terroristes et contrer le terrorisme international? Le terrorisme et ses menaces obligent les gouvernements à recourir à des mesures qui englobent la masse des citoyens honnêtes et respectueux de l'État de droit, sans pour autant offrir de garanties de succès et avec des conséquences sociales et éthiques lourdes pour le pluralisme des sociétés modernes et le respect de la démocratie. Une préoccupation ressort de la documentation consultée et c'est celle de la crainte que l'équilibre soit rompu «entre la liberté individuelle, qui se manifeste au travers de la protection de la vie privée, et la nécessité pour l'État de légiférer et de maintenir l'ordre grâce à des politiques appropriées en matière de sécurité reposant pour la plupart sur la technologie⁵⁹. » Et des questions doivent être posées : « que sommes-nous, en tant que société, prêts à sacrifier au nom de la lutte antiterroriste et dans quelle mesure ces sacrifices permettent-ils effectivement de combattre le fléau du terrorisme? C'est-à-dire, de tels sacrifices sont-ils vraiment nécessaires?⁶⁰ »

3.1.1 Le terrorisme international : une nébuleuse de plus en plus difficile à cerner⁶¹

Dans son ouvrage, *A History of Terrorism*, Walter Laqueur énonce une série de six idées préconçues, par rapport au terrorisme :

⁵⁹ INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPT), « Sécurité et respect de la vie privée du citoyen à l'ère du numérique après le 11 septembre : Vision prospective », juillet 2003, p. 2.

⁶⁰ ALBERT LEGAULT, *La lutte antiterroriste ou la tentation démocratique autoritaire*, Québec, Les Presses de l'Université Laval, 2002, p. 82.

⁶¹ La Commission remercie Benoît Gagnon pour le texte qui constitue cette section du document.

1. Le terrorisme est un phénomène nouveau. Pour cette raison, son histoire comporte peu d'intérêt;
2. Le terrorisme est un des plus dangereux et importants problèmes auxquels l'humanité doit aujourd'hui faire face;
3. Le terrorisme est une réponse à l'injustice; s'il n'y avait pas d'injustice, il n'y aurait pas de terrorisme;
4. La seule façon connue de réduire la probabilité de voir naître le terrorisme est la diminution du ressentiment, du stress et de la frustration qu'il sous-tend ;
5. Les terroristes sont des fanatiques religieux désespérés et vivant dans des conditions intolérables. Ils sont pauvres et leur source d'inspiration est profondément idéologique;
6. Le terrorisme peut se produire n'importe où⁶². [traduction libre]

Sans complètement rejeter du revers de la main les fondements de ces préjugés, Laqueur souligne le fait qu'ils reflètent une incompréhension du phénomène terroriste. Il invite ainsi à avancer vers une analyse plus nuancée du phénomène.

Notons, entre autres, le fait que le terrorisme est un phénomène très ancien. Les premières traces écrites d'actes terroristes se trouvent au Moyen-Orient au premier siècle de notre ère⁶³. C'est la secte des Zélotes, une organisation juive ayant pour objectif de rejeter l'autorité impériale romaine, qui « [...] constitue l'un des premiers groupes ayant pratiqué la technique de la terreur de manière systématique et dont on possède aujourd'hui une trace écrite⁶⁴. » Depuis, la technique du terrorisme, qui vise essentiellement à inspirer la crainte, s'est répandue. Le phénomène s'est profondément transformé et complexifié, rendant ainsi son analyse très difficile.

Il ne s'agit pas ici de faire une étude sur ce qu'est exactement le terrorisme, le contexte du présent document ne s'y prêtant pas. Il importe cependant de noter que les travaux sur le sujet tendent à démontrer qu'il n'y a pas de définition consensuelle sur ce que représente le phénomène terroriste dans son ensemble⁶⁵. En fait, pour aborder ce sujet, il serait plus juste de parler des terrorismes. D'ailleurs, dans son livre *Terrorisme : peurs et réalités*, François Légaré⁶⁶ présente une typologie très symptomatique du caractère indéfinissable du terrorisme.

À travers un exercice de recension des définitions les plus utilisées pour décrire le terrorisme, Légaré démontre que le terrorisme incorpore une série de termes, concepts et expressions qui complexifient grandement le processus même de définition. Ainsi, tantôt le terrorisme est défini comme étant une action violente. À d'autres moments, c'est son caractère spectaculaire qui le décrit. Bref, le terrorisme est un terme fourre-tout employé pour décrire plusieurs réalités fort complexes telles la criminalité, la guerre clandestine ou encore la guerre psychologique⁶⁷.

Une définition du terrorisme – souvent employée dans la littérature consacrée au sujet – est celle d'Alex P. Schmid et d'Albert J. Jongman :

Le terrorisme est une méthode épétée d'action violente inspirant l'anxiété, la peur et qui est employée par des individus, des groupes (semi-)clandestins ou des acteurs étatiques pour des raisons particulières, criminelles ou politique où – au contraire de l'assassinat – la cible initiale de l'acte de violence ne représente que la cible secondaire et non la cible principale. La cible initiale de l'acte de violence est généralement choisie au hasard (opportunité) ou de manière sélective (symbolisme) parmi une population donnée et sert à propager un message. Le processus de menace et de violence entre les terroristes, les victimes (cible initiale) et la cible principale (audience) est utilisé dans le but de manipuler la cible principale, ce qui transforme

⁶² Walter LAQUEUR, *A History of Terrorism*, Transaction Publisher, New Jersey, 2002, p. 5.

⁶³ Gérard CHALIAND et Arnaud BLIN, *Histoire du terrorisme : de l'Antiquité à Al Qaida*, Paris, Bayard, 2004, p. 59.

⁶⁴ *Idem*.

⁶⁵ Il existe toutefois des définitions du terrorisme touchant à des domaines bien précis, notamment dans diverses conventions internationales. Si ces définitions réussissent à circonscrire certaines facettes du phénomène, le caractère spécialisé de ces définitions met de côté d'autres aspects qui s'inscrivent dans le terrorisme.

⁶⁶ Voir François LÉGARÉ, *Terrorisme: peurs et réalités*, Outremont (Québec), Athéna, , 2002.

⁶⁷ *Ibid.*, p. 25.

celle-ci en une cible de terreur, une cible de demandes ou une cible d'attention, selon que l'intimidation, le chantage ou la propagande représente l'objectif visé⁶⁸. [Traduction libre]

Malgré l'intérêt manifeste de cette définition, elle pose d'importants problèmes. Par exemple, la définition de Schmid et Jongman ne réussit pas à montrer la différence entre une attaque terroriste ciblant des infrastructures et un attentat visant des humains. Cet exemple rapide montre ainsi toute la difficulté résidant dans la définition du terrorisme.

En fait, seulement deux éléments font quasi-consensus chez les spécialistes du terrorisme. Le premier est que le terme comporte une connotation péjorative et subjective. L'utilisation du terme implique nécessairement un jugement moral; si un acteur peut réussir à attacher l'étiquette de « terroriste » à son opposant, il a alors indirectement persuadé les autres d'adopter son point de vue moral. Conséquemment, identifier un individu ou une organisation comme étant terroriste devient un geste presque obligatoirement subjectif⁶⁹. Avec ce genre de vision, il apparaît clair que tout est une question de perception : les terroristes des uns sont, en fait, les soldats libérateurs des autres. L'identification d'un individu, d'un groupe d'individus ou même d'un État comme terroriste amène forcément une interprétation des actions de violences posées.

Le second élément faisant consensus : le terrorisme exploite une violence qui tend à être communicative. L'objectif terroriste est de faire passer un message et la violence devient alors une méthode lui permettant de pénétrer les canaux de communication, notamment les mass médias. Cet état de fait a, dans une certaine mesure, pour conséquence de limiter les outils des terroristes. En effet, ces derniers doivent employer des moyens qui sont spectaculaires pour pouvoir espérer obtenir un effet psychologique et communicationnel important. C'est d'ailleurs pour cette raison que la bombe est un instrument privilégié par les terroristes⁷⁰.

Un examen des travaux consacrés au terrorisme révèle qu'en ce moment il existe un affrontement entre deux écoles de pensée. La première affirme que le phénomène terroriste ne s'est que très peu transformé depuis les dernières années⁷¹. Le terrorisme actuel serait donc à peu près le même que le terrorisme « classique » qui avait cours durant les années 1960-70. La seconde soutient plutôt que le terrorisme s'est radicalement transformé depuis la fin de la Guerre froide⁷². Dans cette vision des choses, les mouvements terroristes auraient saisi les occasions apportées par la mondialisation, la montée des technologies de l'information et l'affaiblissement de certains États, notamment ceux de la région de l'ancienne Union soviétique. Ce « nouveau » terrorisme aurait pour principales caractéristiques d'être plus violent, radical et intransigeant que le terrorisme classique ayant des objectifs sociopolitiques plus conciliants.

Certes, il faut l'avouer, les attentats terroristes du 11 septembre 2001 sur New York et Washington ont donné une nouvelle dimension aux menaces terroristes. Ces dernières semblent non seulement mal définies, mais également très complexes, diffuses et intangibles. Le professeur Thomas Homer Dixon aborde d'ailleurs la question dans ce sens en parlant de la montée d'un terrorisme complexe; un terrorisme dont les actions sont dirigées contre les centres névralgiques des sociétés⁷³. En frappant ces centres névralgiques, les terroristes viseraient des effets déstabilisateurs, nuisant aux activités normales des citoyens et créant des effets néfastes dans leur psyché collective. En somme, les terroristes contemporains seraient des adeptes de l'utilisation d'armes de perturbations massives, soit des armes capables à la fois de porter atteinte aux structures sociales actuelles et d'attirer l'attention des médias.

⁶⁸ Alex P. SCHMID, Albert J. JONGMAN ET AL., *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, New Brunswick, Transaction Books, 1988, p. 28.

⁶⁹ Bruce HOFFMAN, *Inside Terrorism*, Columbia University Press, New York, 1998, p. 31.

⁷⁰ À ce sujet, voir : Pippa NORRIS, Montague KERN et Marion JUST (ed.), *Framing Terrorism: The News Media, the Government, and the Public*, New York, Routledge, 2003.

⁷¹ C'est, entre autres, la pensée de Pierre Manonni. Voir : Pierre MANONNI, *Les logiques du terrorisme*, Paris, In Press, 2004.

⁷² Un excellent exemple de la pensée reliée à cette école se trouve chez Walter Laqueur. Voir : Walter LAQUEUR, *The New Terrorism: Fanaticism and the Arms of Mass Destruction*, Oxford, Oxford University Press, 1999.

⁷³ Thomas Homer DIXON, « The Rise of Complex Terrorism », *Foreign Policy*, janvier-février 2002, p. 52-62.

Autre caractéristique importante du terrorisme complexe : les réseaux terroristes sont de plus en plus difficiles à saisir. Les structures hiérarchiques pyramidales, rigides et statiques, font désormais partie du passé. Aujourd'hui, les hiérarchies terroristes sont structurées selon les théories réseautiques⁷⁴, ce qui a pour résultat de créer des hiérarchies décentralisées, voire sans chef (*leaderless structure*)⁷⁵.

L'exemple d'Al-Qaïda est souvent cité comme étant un archétype de structure terroriste en réseau. Diverses cellules fonctionnent de manière indépendante les unes des autres. Elles coordonnent leurs activités en exploitant le potentiel offert par les technologies de l'information – comme Internet ou les téléphones cellulaires – ce qui leur permet de communiquer dans un anonymat relatif. Le principe de la structure « sans chef » est qu'elle décentralise l'autorité décisionnelle à travers toutes les cellules du groupe terroriste. D'un côté, cela met en place un recrutement plus efficace et plus diffus⁷⁶. De l'autre côté, le groupe terroriste est moins sensible à des opérations sécuritaires : advenant l'arrestation d'une cellule de l'organisation, les autres membres du groupe peuvent continuer à fonctionner car ils ne sont pas dépendants des activités des autres cellules. Cette décentralisation à outrance est la raison pour laquelle il est désormais commun de parler de la « nébuleuse » d'Al-Qaïda.

Finalement, notons que le terrorisme contemporain sous-tend de plus en plus des objectifs « radicaux » et « punitifs ». Ces terroristes cherchent à détruire le système sociopolitique, plutôt qu'à le transformer. La montée des terroristes aux vues nihilistes ou religieuses entre d'ailleurs dans cette veine. Les terroristes séculiers voient la violence comme étant un moyen permettant de corriger des failles du système. De leur côté, les terroristes religieux ne se perçoivent pas comme étant partie prenante d'un système valant la peine d'être préservé, mais plutôt comme un acteur externe cherchant à perpétrer des changements fondamentaux dans l'ordre actuel. Cette distanciation amène les terroristes religieux à considérer la mise en place d'opérations plus violentes et meurtrières que les terroristes séculiers⁷⁷. Le terrorisme contemporain apparaît donc comme étant un terrorisme plus dangereux, le faisant passer du statut de menace dérangeante (*annoying threat*) à celui de menace importante à la sécurité, voire de menace globale pour le système international.

3.1.2 La menace terroriste : comme une épée de Damoclès...

L'attentat terroriste a ses particularités : outre le fait qu'il soit imprévisible, il tend à être spectaculaire, catastrophique et terrifiant⁷⁸. Personne ne se sent à l'abri et le risque est constant, jour après jour, dans un quotidien des plus banals – utiliser les transports en commun, s'amuser dans une discothèque, fréquenter des édifices multi-étagés ou de grands stades, etc. À quand notre tour? se demandent les citoyens de la communauté internationale, inquiets de la vulnérabilité des sociétés démocratiques.

Comme le souligne le Comité sénatorial permanent de la Sécurité nationale et de la défense, « les terroristes n'ont pas besoin de bombes pour paralyser les réseaux informatiques, lesquels transportent maintenant le flot nourricier de notre vie économique. [...] pas besoin de bombes non plus pour commettre des attentats bactériologiques⁷⁹. » D'ailleurs, s'agissant de la menace

⁷⁴ À ce sujet, voir entre autres : David S. ALBERTS et Richard E. HAYES, *Power to the Edge: Command and Control in the Information Age*, Command and Control Research Program, Washington D.C., 2003.

⁷⁵ John ARQUILLA et David RONDFELT, *Networks and Networks: The Future of Terror, Crime and Militancy*, Editions RAND National Defense Research Institute, Washington, 2001, p. 8.

⁷⁶ À ce titre, une récente étude faite par le INTERNATIONAL INSTITUTE FOR STRATEGIC STUDIES démontre qu'Al-Qaïda a des cellules actives dans environ 60 pays. Voir : Richard NORTON-TAYLOR, « Thinktank: invasion aided Al-Qaïda », *The Guardian* [en ligne] 20 octobre 2004 [<http://www.guardian.co.uk/Iraq/Story/0,2763,1331362,00.html>]

⁷⁷ Bruce HOFFMAN, *Inside Terrorism*, New York, Columbia University Press, 1998, p. 95.

⁷⁸ Communication de Hélène Denis, spécialiste du risque, devant la Commission de l'éthique de la science et de la technologie, le 8 avril 2004.

⁷⁹ « Les urgences nationales : Le Canada, fragile en première ligne. Stratégie de renforcement », COMITÉ SÉNATORIAL PERMANENT DE LA SÉCURITÉ NATIONALE ET DE LA DÉFENSE, Volume 1, [en ligne] mars 2004, p.10. [<http://www.parl.gc.ca/37/3/parlbus/commbus/senate/com-f/defe-f/rep-f/rep03vol1-f.htm>]

informatique, rappelons l'acte de piraterie de « Mafia Boy », cet adolescent montréalais de 15 ans, qui a fait subir des pertes estimées à 1,2 milliard de dollars à diverses entreprises. Certes, il ne s'agissait pas d'un acte terroriste, mais les conséquences d'un acte d'amateur permettent de saisir l'ampleur que pourrait prendre une véritable attaque cyberterroriste.

Une question semble s'imposer pour déterminer quelles seraient les mesures de protection à mettre en place pour prévenir les attentats terroristes : quelles formes peut prendre l'attentat terroriste? Toutes les réponses sont bonnes dans la mesure où les dégâts seront importants. Et c'est ce qui rend la prévention si difficile compte tenu de la vulnérabilité⁸⁰ des sociétés contemporaines à des attaques de toute nature (bactériologiques, chimiques, informatiques, physiques) sur les réseaux de transport et les réseaux énergétiques, sur les méga-complexes commerciaux, stades et autres, etc., y compris la prise d'otages. Comment se prémunir efficacement contre de telles attaques? Comment évaluer l'impact d'un recours à la biométrie dans un contexte où la menace est diffuse et la vulnérabilité omniprésente? Comment ne pas tenir compte des incidences d'une vigilance et d'un contrôle constants dans une société libre, pluraliste et démocratique?

3.1.3 Les incidences des attentats du 11 septembre 2001 sur les démocraties : une tension entre la sécurité et les droits

Est-il besoin de le rappeler, les événements du 11 septembre 2001 aux États-Unis ont bouleversé les sociétés démocratiques : un tel attentat en temps de paix et sans déclaration de « guerre » préalable semblait impossible. Et pourtant. Les vieux spectres de menaces à la sécurité mondiale, atténués si ce n'est disparus avec la chute du Mur de Berlin et la fin du communisme en Union soviétique, refaisaient surface. La crainte d'une attaque nucléaire cédait la place à celle omniprésente d'une attaque sournoise et imprévisible pouvant surgir de nulle part et foudroyer n'importe qui dans un conflit qualifié d'asymétrique et d'hors normes. D'autres attentats moins spectaculaires ont eu lieu depuis, mais celui du 11 mars 2004 à Madrid a clairement rappelé à tous que nul n'est à l'abri.

Premier à réagir pour mieux assurer la sécurité sur son territoire et tenter d'empêcher d'autres attaques terroristes, le gouvernement américain adoptait – 43 jours après l'événement – le Patriot Act qui amplifiait considérablement les pouvoirs de la police et de la justice, limitant d'autant le respect de la vie privée et la protection des renseignements personnels. Quelques mois plus tard, le 21 mars 2002, était adoptée la National Homeland Security Agency Act ayant pour but de créer une agence nationale pour assurer la sécurité du territoire américain. Le 30 juillet suivant, cette Agence était transformée en ministère, le Department of Homeland Security, avec tous les pouvoirs afférents. Relevant de ce ministère, la Transportation Security Administration (TSA), chargée de la sécurité des moyens de transport, a défini trois applications spécifiques des technologies biométriques : le contrôle d'accès aux aéroports et aux gares, la surveillance/détection des voyageurs susceptibles de menacer la sécurité, et le contrôle des passagers⁸¹. En juin de la même année, était également implanté le National Security Entry-Exit Registration System (NSEERS), qui a pour but de mieux contrôler l'entrée aux États-Unis de ressortissants de l'Iran, de l'Iraq, de la Libye, du Soudan et de la Syrie ou d'autres pays qui présentent un risque élevé sur le plan de la sécurité⁸². Le contenu d'une base de données gérée par le service d'immigration, comprenant neuf millions d'empreintes digitales dont celles des criminels et terroristes étrangers, gérée par le service d'immigration, a été intégré au système⁸³. Depuis le 31 décembre 2003, un programme de contrôle des frontières pour les détenteurs de visas, le

⁸⁰ À cet égard, voir notamment le scénario présenté par le Comité sénatorial permanent de la Sécurité nationale et de la défense dans son rapport *Les côtes du Canada : Les plus longues frontières mal défendues au monde*, 28 octobre 2003, « Cauchemars pour le nouveau millénaire » [en ligne] [\[http://www.parl.gc.ca/37/2/parlbus/commbus/senate/com-f/defe-f/rep-f/rep17oct03-f.htm\]](http://www.parl.gc.ca/37/2/parlbus/commbus/senate/com-f/defe-f/rep-f/rep17oct03-f.htm)

⁸¹ Voir particulièrement OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, 2^e partie, p. 35.

⁸² Voir http://usinfo.state.gov/is/Archive_Index/EntryExit_Registration_System.html.

⁸³ OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, 2^e partie, p. 35.

US_Visit Program, a également été mis en place – la plupart des Canadiens n'y sont pas assujettis. La vérification des entrées et sorties des visiteurs avec visa s'appuiera sur un contrôle d'identité à partir des documents de voyage et la prise d'empreintes digitales⁸⁴.

Dans l'Union européenne, les mesures adoptées ont d'abord été de moindre ampleur qu'aux États-Unis. La plupart des pays ont cherché à accroître la sécurité de leur territoire en adoptant diverses mesures, particulièrement en ce qui a trait aux contrôles frontaliers. En mai 2004 cependant, après bien des tergiversations – notamment en raison des lois européennes sur la confidentialité des renseignements personnels –, la Commission européenne acceptait de se conformer aux exigences américaines et de fournir au Department of Homeland Security 34 des 39 éléments d'information demandés⁸⁵ (voir l'annexe 3) sur les voyageurs empruntant les lignes aériennes européennes à destination des États-Unis. Les autorités américaines ont également assuré la Commission européenne que toute information pouvant révéler l'origine ethnique ou l'état de santé d'un passager serait supprimée⁸⁶. Par ailleurs, dans la foulée de l'attaque de Madrid, d'autres mesures avaient été rapidement adoptées le 25 mars 2004 à l'échelle européenne, dont la nomination d'un coordonnateur de la lutte contre le terrorisme⁸⁷ qui a pour responsabilité principale la coordination de l'action antiterroriste dans la communauté européenne⁸⁸. Il faut aussi souligner que le Conseil de l'Union européenne a adopté, à sa réunion des 13 et 14 décembre 2004⁸⁹, un règlement établissant des normes pour les éléments de sécurité et les éléments biométriques (photo faciale numérisée et empreintes digitales inscrits sur une puce électronique⁹⁰) à intégrer au passeport européen. Toutefois, l'échéance de juin 2005 imposée par les États-Unis ne pourra pas être respectée puisqu'il faut compter un délai d'au moins 18 mois pour la mise en application d'un règlement après son adoption définitive par le Conseil et qu'un délai de 36 mois est prévu pour l'intégration des empreintes digitales dans le passeport⁹¹.

Depuis le 11 septembre 2001, plusieurs gouvernements ont saisi l'occasion qui se présentait pour introduire ce que certains⁹² appellent un « nouveau paradigme sécuritaire » et agir à l'égard de la sécurité de leur territoire en adoptant des politiques ou des mesures qui ont pour effet global de modifier l'équilibre sécurité/vie privée en faveur des intérêts sécuritaires du pays⁹³. L'utilisation de systèmes informatiques qui facilitent la saisie de données et leur partage entre de multiples sources afin de faciliter la collecte d'informations s'inscrivent dans les mesures adoptées. De façon générale, selon une étude réalisée pour la Commission européenne, « les initiatives ainsi prises en matière de sécurité ont également renforcé les pouvoirs des gouvernements et des organismes d'application des lois qui peuvent désormais accéder aux données à caractère personnel à d'autres fins que celles pour lesquelles elles ont été initialement fournies. En effet, pour que le citoyen puisse accéder normalement à de nombreux services commerciaux et publics, il doit aujourd'hui fournir des données à caractère personnel beaucoup plus détaillées qu'auparavant⁹⁴. »

⁸⁴ Voir <http://www.amcits.com/us-visit.asp>.

⁸⁵ Les documents relatifs aux passagers aériens en contiennent généralement de 10 à 15 et il ne sera pas nécessaire de fournir les informations manquantes; voir http://europa.eu.int/comm/external_relations/us/intro/apis_en.pdf.

⁸⁶ *Ibid.*

⁸⁷ *LE NOUVEL OBSERVATEUR*, « Consensus à Bruxelles sur un 'Monsieur Terrorisme' », [en ligne] 19 mars 2004. [http://permanent.nouvelobs.com/cgi/edition/gobs_imprime?cle=20040319.OBS6161] [page consultée le]

⁸⁸ « Déclaration sur la lutte contre le terrorisme », Bruxelles, [en ligne] 25 mars 2004 [http://ue.eu.int/ueDocs/cms_Data/docs/pressdata/fr/ec/79639.pdf]

⁸⁹ Voir le document officiel du Conseil de l'Union européenne : <http://register.consilium.eu.int/pdf/fr/04/st15/st15918.fr04.pdf>

⁹⁰ Voir le contenu du règlement à l'adresse suivante : <http://register.consilium.eu.int/pdf/fr/04/st15/st15152.fr04.pdf>

⁹¹ Estelle DUMOUT, « Passeports : visage et empreintes numériques imposés par le Conseil de l'UE », *ZDNet France*, [en ligne] 27 octobre 2004 [<http://www.zdnet.fr/actualites/informatique/0,39040745,39179891,00.htm>]

⁹² IPTS – INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES, *op. cit.*, p.4.

⁹³ *Ibid.*

⁹⁴ *Ibid.*

3.1.4 La situation canadienne⁹⁵

Au Canada, la défense du territoire est sous la responsabilité du gouvernement fédéral, en collaboration avec les provinces et les territoires.

Dès le 12 décembre 2001, dans la foulée du 11 septembre, était signée la Déclaration canado-américaine sur la frontière intelligente, dans le but de renforcer la sécurité à la frontière et d'améliorer l'infrastructure frontalière. Il s'agit d'un plan d'action en 30 points, dont le premier fait spécifiquement référence à l'utilisation des données biométriques en exigeant la création d'identificateurs biométriques communs dans les documents de voyage (passeport ou carte de résident permanent); y figure aussi une mesure visant l'élaboration d'une entente entre les deux pays afin d'adopter une technologie «interopérable» et compatible, c'est-à-dire capable de lire ces identificateurs⁹⁶. En sont parties intégrantes le programme EXPRES⁹⁷ (programme d'expéditions rapides et sécuritaires) qui vise à accélérer le mouvement des marchandises à faible risque – actuellement en vigueur à 12 grands postes frontaliers –, et le programme NEXUS⁹⁸ qui doit faciliter le passage accéléré des voyageurs aux postes frontières; ces postes passeront bientôt de 11 à 13 sur le territoire canadien (deux sont situés au Québec : Lacolle et St-Armand Philipsburg). S'y ajoute également le programme CANPASS⁹⁹ qui vise à faciliter l'entrée au Canada de voyageurs aériens préautorisés et considérés à faible risque. La technologie de reconnaissance de l'iris est utilisée dans le cadre de ce programme; en outre, les membres doivent se soumettre à une vérification de sécurité au moment de l'inscription et du renouvellement annuel de leur laisser-passer.

Par ailleurs, le 18 décembre 2001, était sanctionné le projet de loi C-36 – la Loi antiterroriste – qui « modifie le *Code criminel*, la *Loi sur les secrets officiels*, la *Loi sur la preuve au Canada*, la *Loi sur le recyclage des produits de la criminalité* et plusieurs autres lois, et qui édicte la *Loi sur l'enregistrement des organismes de bienfaisance (renseignements de sécurité)*, en vue de combattre le terrorisme¹⁰⁰. » Le gouvernement du Canada considère que cette loi « représente un aspect important de l'engagement du Canada d'unir ses efforts à ceux de ses partenaires internationaux en vue d'affronter et d'éradiquer le terrorisme dans le monde entier¹⁰¹. » Préalablement à l'adoption de la loi G36, une conférence de deux jours a été tenue sur son contenu les 9 et 10 novembre 2001 à la Faculté de droit de l'Université de Toronto; la conférence, intitulée « The Security of Freedom », a permis à 24 conférenciers de donner leur opinion et, dans la plupart des cas, de faire une critique importante du projet¹⁰². La conférence a attiré plus de 350 personnes de tous horizons, préoccupées par l'ampleur des changements proposés dans la loi et inquiètes de ses conséquences sur la démocratie et les libertés civiles.

À la Déclaration canado-américaine sur la frontière intelligente, s'ajoutent les mesures suivantes qui reposent elles aussi sur le recours aux données biométriques :

- la mise en place d'une Initiative de la sécurité publique et de l'antiterrorisme en vue d'améliorer la sécurité des Canadiens, qui voit à l'amélioration de la prise d'empreintes digitales à l'aide d'appareils électroniques « Live Scan » à imagerie numérisée;

⁹⁵ Ces informations sont majoritairement tirées des documents suivants : *Rapport de la vérificatrice générale du Canada à la Chambre des communes*, Chapitre 3 – La sécurité nationale au Canada – L'initiative de 2001 en matière d'antiterrorisme, BUREAU DU VÉRIFICATEUR GÉNÉRAL DU CANADA, mars 2004; *Budget 2004*, Chapitre 4 – Concrétiser les priorités des Canadiens. L'importance des relations du Canada avec le reste du monde, GOUVERNEMENT DU CANADA, mars 2004.

⁹⁶ Voir <http://www.dfait-maeci.gc.ca/can-am/menu-fr.asp?act=v&mid=1&cat=1&did=2465>

⁹⁷ Voir <http://www.cbsa-asfc.gc.ca/import/fast/menu-f.html>

⁹⁸ Voir http://www.cbp.gov/xp/cgov/travel/frequent_traveler/nexus.xml.

⁹⁹ AGENCE DES SERVICES FRONTALIERS DU CANADA, « CANPASS AIR », Document d'information, [en ligne] octobre 2004 <http://www.asfc.gc.ca/travel/canpass/canpassair-f.html>

¹⁰⁰ Lois du Canada (2001), *Loi C-36, chapitre 41*, Sommaire.

¹⁰¹ « Les amendements au projet de loi C-36 », Bureau du Conseil privé, GOUVERNEMENT DU CANADA [en ligne] 20 novembre 2001 [http://canada.justice.gc.ca/fr/news/nr/2001/doc_27902.html]

¹⁰² Voir la recension des présentations dans l'ouvrage *The Security of Freedom : Essays on Canada's Anti-Terrorism Bill*, Edited by Ronald J. DANIELS, Patrick MARCLEM, and Kent ROACH, University of Toronto Press, 2001, 500p.

- la mise sur pied de l'Administration canadienne de la sûreté du transport aérien (ACSTA), qui fait rapport au Parlement par l'entremise du ministre des Transports, et assume les responsabilités suivantes;
 - contrôle des passagers et de leurs effets personnels avant l'embarquement;
 - acquisition, déploiement et fonctionnement de systèmes de détection des explosifs;
 - mise en œuvre du Programme canadien de protection des transporteurs aériens;
 - mise en œuvre d'une carte d'identité dans les zones réglementées des aéroports;
 - contrôle des personnes qui entrent dans les zones réglementées des aéroports mais ne sont pas des passagers;
 - contribution aux services supplémentaires de police dans les aéroports.

Les besoins de protection du territoire canadien, ainsi que les exigences américaines relatives à la protection des frontières, ont amené le gouvernement du Canada à adopter un certain nombre d'autres mesures et à mettre en place de nouvelles infrastructures ou de nouveaux programmes de sécurité publique depuis 2001, dont :

- la création du nouveau ministère de la Sécurité publique et de la Protection civile (qui englobe les services frontaliers et la protection civile);
- la création d'un comité ministériel spécial sur la sécurité publique et l'antiterrorisme;
- la création d'un poste de Conseiller à la sécurité nationale auprès du premier ministre pour assurer la collaboration entre les organismes ainsi que l'élaboration et la mise en œuvre d'une politique efficace en matière de sécurité nationale;
- la création d'une nouvelle Agence des services frontaliers du Canada (ASFC) qui relève du ministère de la Sécurité publique et de la Protection civile et qui a pour mandat d'assurer l'adoption d'une approche cohérente pour atteindre les objectifs sur le plan du commerce et de la sécurité frontalière;
- pour la première fois, l'adoption d'une politique canadienne en matière de sécurité nationale.

En matière de sécurité, le gouvernement canadien s'est donné les priorités suivantes : les activités de renseignement, la protection des frontières et la sécurité maritime et informatique, le renforcement de la coordination des systèmes, de l'information, de l'évaluation des menaces et des interventions en cas d'urgence.

Toutefois, de l'avis de la Vérificatrice générale dans son rapport de 2004, il subsiste des lacunes dans la gestion du renseignement, et le gouvernement n'a pas réussi à rendre les systèmes d'information sur la sécurité plus aptes à échanger les uns avec les autres. Elle note également « des lacunes et des incohérences dans les listes de surveillance [voir encadré] qui servent à filtrer les demandeurs de visa ou de statut de réfugié et les voyageurs qui veulent entrer en territoire canadien. » Elle note qu'il n'y aurait aucune vérification de renseignements criminels pour filtrer les demandeurs de cotes de sécurité pour l'accès aux zones réglementées des aéroports et qu'en l'occurrence, des cotes de sécurité seraient accordées à de nombreuses personnes dont la fiabilité est douteuse¹⁰³.

Dans son rapport de février 2005, la Vérificatrice générale touche un point important en matière de sécurité des technologies de l'information et des renseignements personnels que contiennent les systèmes informatiques du gouvernement. Elle note que « les systèmes du gouvernement et les données de nature délicate qu'ils contiennent sont vulnérables en cas d'atteinte à la sécurité informatique¹⁰⁴ »; et elle ajoute que « bien qu'un certain nombre de points de vulnérabilité viennent de l'extérieur de l'organisation, la plupart des incidents de sécurité (intentionnels ou accidentels)

¹⁰³ BUREAU DU VÉRIFICATEUR GÉNÉRAL DU CANADA, *op. cit.*, p. 2.

¹⁰⁴ BUREAU DU VÉRIFICATEUR GÉNÉRAL DU CANADA, Communiqué, Chapitre 1 – La sécurité des technologies de l'information, Ottawa, 15 février 2005.

proviennent de l'intérieur, là où les personnes ont facilement accès à l'information et aux systèmes¹⁰⁵. »

Les listes de surveillance

Les listes de surveillance jouent un rôle essentiel en matière de sécurité nationale. Elles constituent un outil crucial de lutte contre le terrorisme car elles permettent d'intercepter les terroristes avant qu'ils ne gagnent le territoire canadien ou lorsqu'ils se présentent aux points d'entrée du Canada; elles sont un moyen essentiel de vérification pour la délivrance de visas (900 000 en 2003). Sont inscrites dans ces listes les personnes jugées non admissibles en territoire canadien, y compris celles qui représentent vraisemblablement une menace pour le pays (terroristes connus ou personnes soupçonnées de terrorisme, personnes à surveiller de près). La plupart des ajouts aux listes de surveillance proviennent du programme TIPOFF du gouvernement américain, un carrefour où convergent les renseignements de nature délicate qui émanent d'organismes tant canadiens qu'étrangers. Étrangement, n'y figurent pas une liste des passeports canadiens perdus ou volés (65 000 dans la base de données du Bureau des passeports) et tous les mandats d'arrestation non exécutés à l'échelle du Canada pour de graves infractions criminelles (sans compter les mandats de l'Immigration) (162 000 en 2003).

Information tirée du « Rapport de la vérificatrice générale »¹⁰⁶

3.1.5 La situation québécoise¹⁰⁷

Il convient d'abord de rappeler que la sécurité nationale et le contrôle des frontières sont des domaines de compétence fédérale. Dans ce contexte, le Québec s'est engagé à collaborer pleinement aux efforts des autorités gouvernementales canadiennes et américaines pour combattre le terrorisme en intervenant directement dans les domaines relevant de sa propre compétence.

Au nombre des actions entreprises, signalons les suivantes :

- le Québec se dotera prochainement d'un *Plan québécois de gestion contre le terrorisme* devant définir le cadre d'intervention à l'intérieur duquel s'articule la réponse policière et gouvernementale à un incident terroriste survenant au Québec;
- le Service de la lutte contre le terrorisme de la Sûreté du Québec intervient dans les sphères d'activité suivantes : usurpation identitaire, crimes haineux et extrémistes, suivi de seconde ligne en matière d'immigration, suivi de la criminalité parallèle sur le territoire québécois et observation des phénomènes ayant un impact à haut risque pour la sécurité du Québec; le Service coordonne la prévention des accidents terroristes, assure la préparation des intervenants et définit la réponse opérationnelle face aux incidents terroristes pouvant survenir sur le territoire québécois;
- participation de la Sûreté du Québec et du Service de police de la Ville de Montréal à l'Équipe intégrée de sécurité nationale (EISN) de Montréal, avec la Gendarmerie Royale du Canada qui coordonne les travaux de cette unité d'enquête, du Service canadien du renseignement de sécurité ainsi que de l'Agence des services frontaliers du Canada;
- mise sur pied par le ministère de la Sécurité publique (MSP) d'une table de concertation sur les risques de nature chimique, bactériologique, radiologique et nucléaire (CBRN), afin d'améliorer l'état de préparation et la coordination des intervenants en cas de catastrophe majeure de type CBRN nécessitant une gestion des conséquences;
- adoption de protocoles d'échange de renseignements destinés à l'exécution de la loi avec le Vermont, le Maine et le New Hampshire et de collaboration en matière de lutte contre le

¹⁰⁵ BUREAU DU VÉRIFICATEUR GÉNÉRAL DU CANADA, *Le Point*, Chapitre 1 – La sécurité des technologies de l'information, Ottawa, février 2005, p. 15.

¹⁰⁶ *Ibid.*, pages 32 et 36.

¹⁰⁷ La Commission remercie monsieur Louis Morneau, directeur de la coordination au ministère de la Sécurité publique du Québec, pour l'information fournie en la matière dans sa lettre du 1^{er} décembre 2004.

terrorisme avec l'État de New York; ces protocoles se situent dans la foulée des engagements pris – dans le cadre des accords de coopération entre le gouvernement du Québec et les gouvernements de ces États – pour conjuguer leurs efforts afin de mieux protéger leur frontière commune et d'assurer la sécurité de la population, notamment par l'échange de renseignements;

- le MSP participe au projet Canada–United States Cargo Security Project (CUSCSP) qui consiste à développer et à mettre à l'essai des équipements technologiques pour détecter des radiations de matières dangereuses pouvant être introduites dans des conteneurs intermodaux et, en cas d'anomalies, à prévenir en temps réel les autorités gouvernementales et policières concernées.

3.1.6 Éléments de réflexion

Comme le remarquait l'écrivain israélien David Grossman peu de temps après les événements du 11 septembre, «Parce qu'il pourrait insidieusement la vie, le terrorisme est d'une certaine façon toujours gagnant. [...] la terreur rend la vie amère. Elle oblige chacun de nous à des comportements " militaires ", nous impose un état de tension militaire sans fin qui s'insinue peu à peu dans notre existence et la gâche. Les terroristes n'ont pas à s'en faire : dès l'instant où ils ont persuadé la population qu'ils n'avaient pas de limites, ils peuvent se contenter d'attaques occasionnelles, ici et là. La peur va se propager partout, telle une bactérie carnivore¹⁰⁸. »

Au nombre des éléments qui ressortent de ce bref tour d'horizon sur le terrorisme international et sur les mesures mises en place pour tenter de le contrer, la Commission retient les points suivants :

- le caractère insaisissable de l'attaquant;
- la diversité, la perversité et l'ampleur des attentats qui peuvent être perpétrés;
- l'existence d'une cause, d'une idéologie qui sous-tend les attaques;
- l'incapacité à prévoir où, quand, comment se fera le prochain attentat;
- les gains réalisés au détriment de la démocratie;
- le nombre et la diversité des mesures mises en place pour combattre le terrorisme;
- la discrimination latente ou affichée à l'égard de certains groupes qui en résulte.

Ce sont des éléments qu'il importe de garder à l'esprit au regard de la technologie biométrique et de son utilisation pour contrer le terrorisme international et pour répondre à la question fondamentale : y a-t-il corrélation entre les moyens utilisés ou envisagés et la finalité recherchée – en d'autres mots, la biométrie représente-t-elle un instrument adéquat pour contrer le terrorisme à l'échelle internationale ou nationale? S'y ajoutent aussi d'autres questions, par exemple : les mesures mises en place qui n'ont pas recours à cette technologie pourraient-elles être suffisantes? faut-il que l'ensemble de la population soit touchée par des mesures destinées à contrer le terrorisme?

3.2 La sécurité intérieure : garantir l'identité des personnes

Outre le souci de se conformer aux exigences internationales pour combattre le terrorisme, le gouvernement canadien, comme tout autre gouvernement dans le monde, doit aussi faire face à des problèmes internes de criminalité comme l'usurpation ou le vol d'identité. Ce type de criminalité peut constituer un problème individuel (un citoyen victime d'une usurpation d'identité) mais aussi, à plus large échelle, un problème qui touche la collectivité lorsqu'il y a usage abusif

¹⁰⁸ « Cette terreur qui corrompt tout », David GROSSMAN, *Le Temps*, Genève, repris dans *Le Courrier international*, no 570, [en ligne] 4 octobre 2001. [http://www.courrierinternational.com/article.asp?obj_id=12618&provenance=zop.archives] [page consultée le 17 mars 2004]

des services gouvernementaux offerts à la population à partir des contributions de l'ensemble des citoyens. Dans ce dernier cas, il apparaît tout à fait légitime de se demander quelles mesures un gouvernement peut utiliser pour s'assurer de réserver l'admissibilité à ses services aux ayants droit.

3.2.1 Un problème majeur : le vol d'identité

Comme l'observe un expert français de la fraude documentaire, « la lutte contre le terrorisme est la partie émergée de l'iceberg. Notre combat quotidien, c'est plutôt l'usurpation d'identité. [...] La fausse identité est la base du crime organisé, de l'immigration et du travail illégal, mais aussi de l'utilisation frauduleuse de la carte Vitale [en France] ou des prestations sociales¹⁰⁹. » Pour Roger Clarke, un expert mondial dans le domaine de la biométrie, cette technologie ajoute une nouvelle dimension effarante (*frightening*) au vol d'identité, notamment parce que l'aura de précision et de fiabilité qui l'entoure fera en sorte qu'il sera extrêmement difficile à une victime de prouver son innocence¹¹⁰.

Le Commissariat à la protection de la vie privée du Canada définit ainsi le vol d'identité : « Le vol d'identité est la collecte et l'utilisation non autorisées de vos renseignements personnels, habituellement à des fins criminelles¹¹¹. » Au nombre des renseignements qui peuvent être ainsi utilisés, le Commissariat mentionne le nom d'une personne, sa date de naissance, son adresse, son numéro de carte de crédit, son numéro d'assurance sociale (NAS) et tout autre numéro d'identification personnel comme le NIP d'une carte bancaire. Selon l'organisme, la possession de telles données permet, entre autres, d'ouvrir un compte bancaire, d'obtenir une carte de crédit, un passeport ou tout autre document donnant accès à des services, de faire suivre du courrier, de s'abonner à un service de téléphone cellulaire, de louer un véhicule, de l'équipement ou un local, et même d'obtenir un emploi. Tout devient possible, sans les responsabilités inhérentes à l'utilisation de sa propre identité, puisque ces responsabilités sont ainsi déléguées à une autre personne à son insu¹¹².

Selon le Solliciteur général du Canada, « le vol d'identité est devenu l'une des formes de crime qui connaît la croissance la plus rapide au Canada et aux États-Unis¹¹³. » En 2002, à l'échelle canadienne, ce sont plus de 8 000 plaintes qui ont été déposées auprès de la Gendarmerie royale du Canada, par l'intermédiaire du centre d'appel antifraude du Canada – PhoneBusters – et plus de 13 000 l'année suivante, pour des pertes totalisant 11,7 millions de dollars en 2002 et 21,5 millions de dollars en 2003¹¹⁴. Si l'augmentation de la fraude avoisine les 170 % à l'échelle canadienne, elle se situe à plus de 220 % pour le Québec (voir le tableau ci-dessous). Pour sa part, le Conseil canadien des bureaux d'éthique commerciale estime que « l'usurpation d'identité et la fraude identitaire coûteraient 2,5 milliards de dollars aux gouvernements, aux consommateurs, aux banques, aux entreprises émettrices de cartes de crédit, aux magasins de détails et autres entreprises¹¹⁵. »

¹⁰⁹ « Biométrie. Des données physiques stockées sur une puce. Le corps pour tout passeport », Eléna SENDER, *Sciences et avenir*, septembre 2004, p. 67.

¹¹⁰ Roger CLARKE, « Biometrics and Privacy », [en ligne] 15 avril 2001 <http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html>

¹¹¹ COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Le vol d'identité : qu'est-ce que c'est, et quoi faire », Fiches d'information [en ligne] http://www.privcom.gc.ca/fs-fi/02_05_d_10_f.asp.

¹¹² Voir, entre autres, Christophe NAUDIN, *ALIAS. Le nouvel empire des crimes d'identité*, Paris, La Table Ronde, 2005.

¹¹³ SOLLICITEUR GÉNÉRAL DU CANADA, *Avis public aux consommateurs : Rapport spécial sur le VOL D'IDENTITÉ* (non daté)

¹¹⁴ PhoneBusters, Gendarmerie royale du Canada [en ligne]. <http://www.phonebusters.com/francais/statistics.html>

¹¹⁵ CITOYENNETÉ ET IMMIGRATION CANADA, « Biométrie : incidences... », Document d'information, *op. cit.*, p. 24, note 4.

PLAINTES POUR VOL D'IDENTITÉ – CANADA 2002 ET 2003

Province	2002		2003	
	Victimes (n)	Pertes (\$)	Victimes (n)	Pertes (\$)
Colombie Britannique	1 046	1 221 733	1 829	1 808 318
Alberta	635	767 110	1 079	1 282 717
Saskatchewan	106	84 937	202	687 993
Manitoba	196	187 844	195	194 719
Ontario	4 031	7 188 126	5 772	12 682 219
Québec	1 646	1 916 012	3 711	4 246 802
Nouveau-Brunswick	131	150 017	200	261 206
Nouvelle-Écosse	185	222 516	223	273 347
Île du Prince Edouard	16	7 083	14	2 150
Terre-Neuve	46	27 480	94	115 993
Autres ou inconnus	147	13 985	38	8 640
TOTAL	8 187	11 786 843	13 359	21 564 104

Source : PhoneBusters [en ligne] [<http://www.phonebusters.com/francais/statistics.html>]

De quelle façon s'y prennent les fraudeurs? Les moyens sont nombreux : vol de cartes et de documents de paiement, vol du NIP dans les guichets automatiques, «écrémage» au moment d'un paiement par carte de crédit – un lecteur caché enregistre les données de la carte de crédit au moment d'un paiement –, mystification au moyen de courriers électroniques, de sites Internet ou d'appels téléphoniques incitant les personnes à fournir des renseignements personnels contre la possibilité d'un gain, piratage de bases de données ou corruption du personnel ayant accès à de telles bases¹¹⁶. Certains de ces vols pourraient sans doute être évités si les consommateurs adoptaient une attitude plus prudente et devenaient plus méfiants. Dans d'autres cas, cependant, le recours à la technologie pour contrer le phénomène apparaît inévitable – mais cette technologie doit-elle nécessairement être de nature biométrique et appliquée à tous les citoyens?

Il existe aussi un autre type de vol ou d'usurpation d'identité qui vise l'accès à des services offerts par le gouvernement (fédéral ou provincial) à ses citoyens éligibles et qui n'a pas pour conséquences d'entraîner des pertes financières pour celui ou celle qui est dépossédé de son identité (souvent une personne décédée). C'est alors l'ensemble de la société qui est dépossédée d'une partie de ses ressources au profit de personnes qui, selon les règles en vigueur, n'y ont pas droit et qui ont agi de façon frauduleuse pour s'en prévaloir. Comment s'assurer que seuls les ayants droit auront accès aux services gouvernementaux? Comment le faire sans marginaliser systématiquement certains groupes, dont les immigrants? Le recours aux données biométriques constitue-t-il la solution par excellence ou existe-t-il d'autres façons de faire tout aussi valables ou efficaces?

3.2.2 Une nécessité : l'intégrité des documents officiels

Il existe deux grandes catégories de documents utilisés pour confirmer l'identité ou le statut d'une personne au Canada : les documents primaires et les documents d'admissibilité, qui donnent lieu à un partage des responsabilités entre le gouvernement fédéral et les gouvernements provinciaux.

¹¹⁶ SOLICITEUR GÉNÉRAL DU CANADA, *op. cit.*

Le gouvernement canadien reconnaît que l'intégrité des documents officiels qu'il émet ou qui sont émis par les provinces est essentielle, notamment pour «garantir l'accès aux programmes et services gouvernementaux à ceux qui y ont droit et [...] préserver la sécurité nationale, protéger les programmes gouvernementaux, réduire les crimes commerciaux, protéger les renseignements personnels et permettre les voyages internationaux¹¹⁷. » Dans son document d'information préparé pour les fins du forum d'octobre 2003, Citoyenneté et Immigration Canada mentionnait que le recours à la biométrie était considéré pour rehausser l'intégrité des pièces d'identité délivrées sous sa responsabilité¹¹⁸.

L'intégrité des documents primaires

Les documents primaires comprennent les certificats de naissance¹¹⁹ et de décès qui sont délivrés par les gouvernements provinciaux, et les documents d'immigration et de citoyenneté sous responsabilité fédérale. Ces derniers documents sont la « carte de citoyenneté » et la « carte de résident permanent »¹²⁰ :

- la *carte de citoyenneté* – délivrée par Citoyenneté et Immigration Canada, il s'agit d'un document juridique, de format portefeuille, qui atteste que le titulaire est citoyen canadien. Cette carte n'est pas obligatoire, mais elle permet de prouver la citoyenneté canadienne d'une personne qui demande une carte d'assurance sociale, vote, demande un passeport, veut entrer de nouveau au Canada, postule certains emplois.
- la *carte de résident permanent* – également délivrée par Citoyenneté et Immigration Canada, la carte RP a été lancée en juin 2002, conformément à la *Loi sur l'immigration et la protection des réfugiés* (2002). Depuis le 31 décembre 2003, les résidents permanents qui souhaitent rentrer au Canada à bord d'un transporteur commercial (avion, bateau, train ou autocar) doivent présenter cette carte pour prouver leur statut. Des renseignements personnels sur le détenteur sont encodés dans une bande optique dont la lecture est accessible uniquement aux fonctionnaires autorisés. Un projet de doter cette carte de données biométriques n'a pas abouti pour le moment.

L'intégrité des documents d'admissibilité

Les documents primaires sont généralement requis pour obtenir les documents dits d'admissibilité. Ces documents comprennent les passeports et les cartes d'assurance sociale (responsabilité fédérale), les cartes d'assurance-maladie et les permis de conduire (responsabilité provinciale). À noter que la carte d'assurance sociale est obligatoire pour travailler au Canada ou pour recevoir des prestations du gouvernement fédéral.

Un dernier document délivré par le gouvernement fédéral constitue à la fois un document primaire et un document d'admissibilité : le certificat du statut d'Indien. Ce certificat indique que son titulaire est inscrit comme Indien conformément à la *Loi sur les Indiens* et qu'il est de ce fait éligible aux services fédéraux et aux exemptions fiscales que son statut lui octroie¹²¹.

En ce qui a trait aux passeports, il convient de signaler que le passeport biométrique devrait être obligatoire pour entrer aux États-Unis à partir du 30 novembre 2006 (l'échéance du 24 octobre 2004 ayant été reportée)¹²² – ce que certains experts estiment prématuré sur le plan technologique¹²³. En mai 2003, les États membres de l'Organisation de l'aviation civile internationale (OACI) se sont mis d'accord sur la présence d'une photo numérisée du titulaire sur

¹¹⁷ CITOYENNETÉ ET IMMIGRATION CANADA, document d'information, *op. cit.*, p. 3.

¹¹⁸ *Ibid.*

¹¹⁹ Au Québec, jusqu'en novembre 2001, le baptistaire – ou extrait de baptême – tenait lieu de certificat de naissance.

¹²⁰ L'information au sujet de ces cartes est tirée du site Internet de Citoyenneté et Immigration Canada, [en ligne] [\[http://canada.gc.ca/cdns/wallet/wallet_f.html\]](http://canada.gc.ca/cdns/wallet/wallet_f.html) et du document d'information « Biométrie : incidences et applications pour la citoyenneté et l'immigration », *op. cit.*, p. 2.

¹²¹ *Ibid.*, document d'information, p. 2.

¹²² Eléna SENDER, *op. cit.*, p. 64.

¹²³ *Ibid.*, p. 67.

une puce intégrée au passeport¹²⁴. Lors du contrôle d'identité aux passages frontaliers, la photo contenue dans la puce et celle apposée dans le passeport seront lues et comparées électroniquement. Cette opération permet de vérifier si le passeport a été falsifié avec la photo d'une autre personne. La fiabilité de la comparaison n'étant pas de 100 %, les autorités européennes ont convenu d'y ajouter la lecture des empreintes digitales.

Sur la scène canadienne, le Bureau des passeports du Canada a entrepris une étude sur le sujet¹²⁵. Réalisée sur une période de 18 mois¹²⁶, l'étude (voir l'encadré) a donné des résultats suffisamment satisfaisants pour que le Bureau des passeports recommande l'adoption de la technologie et son utilisation dans les passeports. Un rapport sur cette étude a été remis pour examen au Commissariat à la protection de la vie privée qui doit y réagir. Selon l'ombudsman du Bureau des passeports, le modèle biométrique qui serait utilisé dans les passeports est « tout à fait anonyme¹²⁷ » et ne contient pas de renseignements personnels : « il y a davantage de renseignements personnels sur votre permis de conduire que dans un modèle biométrique¹²⁸ », ajoutant « nous sommes convaincus que la technologie de la reconnaissance faciale répondra à nos besoins et nous aidera à contrer les menaces réelles qui pèsent sur la sécurité canadienne¹²⁹ ». Pour certains, cependant, « l'inscription de données personnelles sur des puces électroniques ouvre la voie à une circulation beaucoup plus large de ces données¹³⁰ » et « la création, par les gouvernements, de toute une infrastructure de surveillance technologique a de réelles conséquences pour notre mode de vie démocratique¹³¹ ».

¹²⁴ Ce qui en étonne certains, comme l'IPTS qui estime que c'est la technologie qui affiche l'une des pires performances parmi les technologies les plus courantes (empreintes, iris, ADN) pour la plupart des facteurs considérés; par ailleurs, c'est cependant la technologie la plus facilement acceptée par les utilisateurs. Voir *Biometrics at the Frontiers: Assessing the Impact on Society*, Technical Report Series, For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), EUR21585EN, 2005, p. 72.

¹²⁵ « Mise à l'essai – La biométrie faciale est-elle à la hauteur? » *IJJ@L'ŒUVRE*, Numéro spécial sur la biométrie, été 2004, p. 20, 21 et 44.

¹²⁶ Communication personnelle avec M. Jocelyn Francoeur, arbitre et ombudsman au Bureau des passeports du Canada, le 21 septembre 2004.

¹²⁷ *IJJ@L'ŒUVRE*, op. cit., p. 21

¹²⁸ *Ibid.*

¹²⁹ *Ibid.*, p. 44.

¹³⁰ Une opinion de Andrew Clement, professeur à l'université de Toronto, rapportée par Jim BRONSKILL, dans « De nouveaux passeports avec des données biométriques », *Le Devoir*, 19 juillet 2004.

¹³¹ Une opinion de Valerie Steeves, professeure de droit à l'université Carleton, rapportée par Jim BRONSKILL, dans « De nouveaux passeports... », op. cit.

**Le Bureau des passeports du Canada
- Étude sur la reconnaissance faciale -**

« [...] le Bureau des passeports a entrepris d'élaborer une méthodologie susceptible de donner des résultats pratiques et pertinents. Cette méthodologie (inspirée des modèles existants) consistait à comparer des paires d'images : à prendre deux photos différentes de la même personne et à déterminer si les technologies disponibles actuellement permettaient d'établir une concordance entre les deux avec un degré élevé de certitude. »

Dans la base de données de l'essai, le Bureau a utilisé plus de 6 000 paires d'images auxquelles ont été ajoutées 143 000 autres images individuelles, le plus grand nombre d'images jamais employé pour ce genre d'essai. « Dans un environnement de reconnaissance faciale, chacune des photos mises en correspondance doit être comparée à des photos de personnes dont les noms figurent sur les listes de surveillance des services de sécurité. »

« Le Bureau des passeports a fait examiner et valider sa méthodologie par le Département de mathématiques et de statistiques de l'Université d'Ottawa. La taille de l'échantillon d'images utilisé a permis d'obtenir des résultats dont le coefficient de confiance s'élevait à 99,7 %. Les résultats de l'essai eux-mêmes étaient assez positifs, s'échelonnant de 75 % à plus de 90 % selon la qualité des images et la taille des archives auxquelles elles étaient comparées [...] »

« [...] aucun système de reconnaissance faciale ne pourrait prendre de décisions strictement automatisées. Lorsqu'une photo semble concorder avec celle d'une personne dont le nom figure sur une liste de surveillance dans une banque de données, un agent de sûreté est averti et invité à pousser l'examen un peu plus loin. [...] cela constitue un avantage par rapport à la dactyloscopie [...] il est beaucoup plus facile de former les gens à comparer et évaluer des photos. »

IIJ@L'ŒUVRE ¹³²

3.2.3 Éléments de réflexion

Il est bien connu que les terroristes peuvent utiliser des documents frauduleux tels que passeports, permis de conduire et certificats de naissance pour voyager clandestinement et à l'insu des autorités. À quel point le recours aux données biométriques permettra-t-il de contrer le problème et d'arrêter aux frontières un éventuel terroriste? Citoyenneté et Immigration Canada reconnaît d'ailleurs que « les 19 individus soupçonnés d'avoir commis les attentats du 11 septembre étaient tous entrés " légalement " aux États-Unis, en déjouant les contrôles américains par de fausses déclarations et des moyens frauduleux¹³³. » Et de plus en plus¹³⁴, le recrutement d'éventuels terroristes se ferait auprès des citoyens de pays visés par une attaque possible, nouvellement convertis à des mouvements extrémistes de type religieux ou partageant l'idéologie terroriste. Qu'y changera la biométrie? Le rapport au Sénat français, cité précédemment, souligne « que la mise en circulation des cartes d'identité infalsifiables s'était accompagnée en France d'un développement de la fraude "en amont", non seulement pour la carte d'identité mais aussi pour les passeports. De vrais titres sont ainsi délivrés sur la base de faux éléments d'identité (fausses pièces d'état civil ou pièces d'une autre personne)¹³⁵. »

D'ici 2015, plus d'un milliard de personnes pourraient faire partie d'une immense base de données mise en place à la demande de l'OACI à des fins de reconnaissance faciale des voyageurs¹³⁶. Il s'agit d'une situation qui préoccupe grandement des organismes comme Privacy International et

¹³² IIJ@L'ŒUVRE, *op. cit.*, p. 21.

¹³³ « Sécurité publique et antiterrorisme », Rapport final, CITOYENNETÉ ET IMMIGRATION CANADA, septembre 2003, p. 8.

¹³⁴ SMOLAR, Piotr, « Les convertis à l'islam radical, une minorité croissante d'activistes », *Le Monde.fr*. [en ligne] 3 juin 2004 [<http://www.lemonde.fr/web/article/0,1-0@2-3226,36-367343,0.html>] ; PERKEL COLIN, « La guerre contre le terrorisme a rendu Al-Qaïda plus dangereux, dit un agent du SCRS », *Le Devoir*, 15 mars 2005 ; « Al-Qaïda, une menace directe pour le pays, selon le SCRS », *Le Soleil*, 15 mai 2005.

¹³⁵ OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, p. 48.

¹³⁶ « Concern over biometric passports », *BBC News*, [en ligne] 30 March 2004., [<http://news.bbc.co.uk/2/hi/technology/3582461.stm>]

The American Civil Liberties Union qui y voient, entre autres, un risque de développement beaucoup plus vaste encore d'une infrastructure de surveillance des déplacements des personnes et de compilation de données accessibles par les gouvernements – y compris ceux qui sont reconnus pour bafouer les libertés civiles et les droits de la personne¹³⁷. La base de données servira-t-elle aussi à des fins d'identification de personnes ou seulement d'authentification des passagers? En France, la Commission nationale informatique et libertés (CNIL) s'interroge¹³⁸, notamment sur la nature des documents qui devraient comporter une information biométrique et sur le type de bases de données qui réduiraient les risques d'attaque ou de piratage d'information : un seul fichier complet et centralisé plus efficace ou plusieurs bases indépendantes moins vulnérables? Au Canada, la Commissaire à la protection de la vie privée constate que « la fréquence croissante avec laquelle les renseignements personnels circulent par-delà les frontières, dans des économies interdépendantes de plus en plus mondialisées, a d'importantes répercussions sur la protection de la vie privée des Canadiens et des Canadiennes. Nous avons le devoir de protéger les renseignements personnels des Canadiens et des Canadiennes. Il nous faut une stratégie équilibrée et sensée de protection des renseignements personnels¹³⁹. » D'autant plus dans un contexte où les systèmes informatisés, du moins au Canada, sont reconnus pour être vulnérables¹⁴⁰.

Enfin, bien que Citoyenneté et Immigration Canada ait tenu un forum de consultation sur l'utilisation des données biométriques dans les documents de citoyenneté et d'immigration, la population n'a pas été consultée spécifiquement sur l'intégration de la technologie dans les passeports et ses retombées possibles en matière de protection de la vie privée, des renseignements personnels et du respect des libertés civiles et de la démocratie.

3.3 La sécurité matérielle ou virtuelle : contrôler l'accès aux sites

L'accès à des sites comporte deux segments d'intérêt : l'accès physique et l'accès informatique. L'accès physique concerne le contrôle de l'accès à une entité matérielle (grandes infrastructures, immeubles, bureaux, gymnases, bibliothèques ou tout autre lieu). L'accès informatique concerne le contrôle de l'accès à un ordinateur, à un serveur, à un logiciel ou à un service informatique.

Le contrôle de l'accès à des sites vise généralement le personnel d'une entreprise, d'une organisation, des abonnés, etc. Tous ces sites n'ont cependant pas la même importance et les répercussions d'une intrusion malfaisante ne seront pas les mêmes selon qu'il s'agit d'un gymnase ou d'une centrale nucléaire ou hydroélectrique, de l'ordinateur d'une PME ou du serveur informatique d'une grande banque, d'un gouvernement, ou utilisé dans la distribution de l'eau potable.

Dans le cas des contrôles d'accès à des sites (matériels ou virtuels), l'utilisation des données biométriques se fait uniquement à des fins d'authentification de l'identité des personnes disposant d'un droit d'accès. L'utilisation des empreintes digitales est très répandue (généralement l'index), mais la lecture de l'iris est de plus en plus utilisée. Quand un seul critère d'identification est utilisé, le profil biométrique peut être conservé dans la mémoire de l'appareil d'authentification. Avec plus d'un critère (par exemple, l'utilisation d'une carte et d'un mot de passe), le profil est conservé sur une carte à puce ou stocké dans une base de données centrale. Par ailleurs, selon de nouvelles exigences de sécurité, une carte d'identité devrait aussi inclure la photo numérisée de l'utilisateur¹⁴¹.

L'utilisation de plus en plus répandue de données biométriques pour contrôler l'accès à des sites physiques ou informatiques est-elle toujours justifiée, ne risque-t-elle pas de mener à une banalisation des caractéristiques biométriques de chaque citoyen? À cet égard, Jennifer Stoddart, alors qu'elle était présidente de la Commission d'accès à l'information, manifestait son inquiétude

¹³⁷ *Ibid.*

¹³⁸ Eléna SENDER, *op. cit.*, p. 67.

¹³⁹ Jennifer STODDART, Commissariat à la protection de la vie privée, Communiqué, [en ligne] 18 août 2004, Ottawa. [\[http://www.privcom.gc.ca/media/nr-c/2004/nr-c_040818_f.asp\]](http://www.privcom.gc.ca/media/nr-c/2004/nr-c_040818_f.asp)

¹⁴⁰ Voir section 3.1.4 et la référence au rapport de février 2005 de la Vérificatrice générale.

¹⁴¹ Jean-Marc PAPINEAU, *op. cit.*, p. 16.

dans le cadre d'une émission *Découverte* consacrée à la biométrie : « Je pense que la biométrie et toutes les techniques de surveillance réduisent notre marge d'autonomie comme citoyen. Et ce sont des libertés très précieuses. Je pense qu'il ne faut pas renoncer à ces libertés sans se poser des questions¹⁴². »

3.4 La sécurité : une justification à la surveillance tous azimuts?

Les mesures de sécurité qui précèdent s'appuient sur une utilisation de la technologie biométrique à des fins de contrôle et de surveillance et c'est l'objet principal du présent document de réflexion de la CEST. La Commission estime cependant qu'elle ne peut passer sous silence d'autres moyens de contrôle et de surveillance qui, strictement parlant, ne reposent pas sur une utilisation de données biométriques, mais soulèvent néanmoins la question d'une intrusion possible de l'État et des organisations dans la vie privée des citoyens et des travailleurs¹⁴³, notamment la vidéosurveillance et la cybersurveillance.

À titre indicatif seulement, et sur un tout autre plan, il convient aussi de signaler que d'autres dispositifs de surveillance virtuelle (bracelets¹⁴⁴ ou puces électroniques¹⁴⁵ permettant de suivre ou d'enregistrer les déplacements d'une personne) sont déjà utilisés ou pourraient se répandre bientôt, par exemple pour les détenus en libération conditionnelle, voire certains ex-détenus – notamment en matière de criminalité sexuelle – qui ont purgé leur peine mais dont la probabilité de récidive est estimée importante, ou encore pour la surveillance des enfants par leurs parents. Enfin, à l'échelle domestique, l'utilisation des « web cams » pour surveiller le comportement des gardiennes à la maison ou s'assurer de la sécurité de parents âgés¹⁴⁶ fait également partie de mécanismes de surveillance qui peuvent être mis en place dans la sphère privée. Au même titre que le recours aux données biométriques, la mise au point de ces divers dispositifs soulève aussi des questions sur la proportionnalité des moyens par rapport à la finalité et sur le respect de la vie privée de chacun.

3.4.1 La vidéosurveillance

Au Québec, la Commission d'accès à l'information s'est penchée sur le phénomène de la vidéosurveillance (voir l'encadré). Considérant la prolifération de ce type de surveillance dans des lieux publics ou lors d'événements publics – dont le Sommet des Amériques constitue un exemple – la CAI pose deux questions fondamentales : « les caméras de surveillance sont-elles

¹⁴² « Biométrie : sécurité ou menace », journaliste et réalisateur Normand GRONDIN, *Découverte*, RADIO-CANADA [en ligne], 14 septembre 2003. [<http://www.radio-Canada.ca/actualite/decouverte/reportages/2003/09-2003/14/biometrie.html>]

¹⁴³ Un constat que documente notamment la Commission d'accès à l'information (CAI) dans son dossier sur l'utilisation de caméras de surveillance par des organismes publics dans les lieux publics [en ligne] – [http://www.cai.gouv.gc.ca/home_00_portail/thema_camera.html]

¹⁴⁴ À noter que de tels dispositifs sont actuellement utilisés au Canada, notamment en Ontario (depuis 2003) [<http://ogov.newswire.ca/ontario/GPOE/2002/10/18/c2533.html?match=&lang=e.html>] et sont envisagés ou mis en place, en France et en Grande-Bretagne par exemple : « Récidive : la gauche s'oppose au bracelet électronique », Patrick ROGER, *Le Monde*, [en ligne] 15 décembre 2004 [http://www.lemonde.fr/web/imprimer_article/0,1-0@2-3224,36-390997,0.html] [page consultée le 15 décembre 2004]; « Récidive : le Sénat rejette le bracelet », [en ligne] 10 février 2005 [<http://archivo.nouvelobs.com/cgi/articles?ad=politique/20050210.OBS8446.html&datebase=20050210>]; « La prison GPS testée en Grande-Bretagne », Armelle THORAVALL, *Libération.fr*, [en ligne] 17 décembre 2004 [<http://www.tu5ex.org/index.php?op=articles;id=65>]

¹⁴⁵ Voir « Human chips more than skin-deep », Michael KANELLOS, *Cnet New.com* [en ligne] 23 août 2004 [http://news.com.com/Human+chips+more+than+skin-deep/2009-7337_3-5318076.html]; « Élève ou bétail? », *Canoe* [en ligne] 11 février 2005 [<http://www2.canoe.com/techno/nouvelles/archives/2005/02/20050211-105834.html>] [page consultée le 14 février 2005].

¹⁴⁶ Notons que la chose est également envisagée par certains États – voir « States consider allowing cameras in nursing homes », Charnicia E HUGGINS, *Elder Law Journal*, 23 août 2004, reproduit dans *MedicineNet.com* [en ligne] [<http://www.medicinenet.com/script/main/art.asp?articlekey=38589&pf=3&track=gpa385>]

nécessaires? Si oui, dans quelles situations et selon quelles modalités?¹⁴⁷ » afin d'établir où se situe le juste équilibre entre la vie privée et la sécurité.

Les vidéocaméras : le difficile équilibre entre sécurité et vie privée

« Pour les uns, les caméras de surveillance sont un segment de marché de consommation qui ne demande qu'à se développer. Pour d'autres, il s'agit d'un outil de travail indispensable pour prévenir les crimes et les infractions aux lois. Pour certains, la surveillance de lieux par caméras entraîne chez la population un sentiment de sécurité. Pour plusieurs, ce nouveau gadget technique provoque une rupture de confiance chez les individus par une intrusion injustifiée dans leur vie privée. »

Commission d'accès à l'information¹⁴⁸

La CAI a donc entamé une réflexion sur le sujet qui l'a menée à la préparation d'un état de situation pour les fins d'une consultation de la population en septembre 2003, suivi d'un bilan de la consultation et de l'élaboration de règles d'utilisation destinées aux organismes publics. Préalablement à la consultation, un sondage¹⁴⁹ réalisé auprès d'un échantillon d'une centaine d'organismes publics (ministères ou organismes gouvernementaux, municipalités, sociétés de transport, écoles, cégeps, commissions scolaires, centres hospitaliers) a permis à la CAI de dénombrer l'utilisation de près de 5 000 caméras par les répondants au sondage¹⁵⁰. Selon les représentants de l'industrie de la sécurité, le marché de la vidéosurveillance au Québec afficherait une croissance d'environ 10 % par année¹⁵¹. Pour information, signalons que la Grande-Bretagne, avec plus de quatre millions de caméras de surveillance installées à travers le pays est en voie de devenir « une société sous surveillance », de l'avis de la Commission informatique et libertés britannique¹⁵².

Le document de présentation de la problématique préparé par la CAI fait le point sur le sujet de la vidéosurveillance, notamment au regard du cadre législatif en vigueur, mais aussi sur les notions de vie privée, de droit à l'image et à l'anonymat et soulève des interrogations sur le recours à la vidéosurveillance. L'ensemble du processus (état de situation et consultation) a donné lieu à la publication de *Règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*¹⁵³. Au total, la CAI propose un total de 20 règles à respecter concernant 1) les éléments à considérer avant d'opter pour la vidéosurveillance, 2) la collecte des renseignements, 3) la gestion des renseignements et 4) la nécessité d'une révision périodique de la décision de recourir à la vidéosurveillance. La CAI a aussi demandé que les organismes publics se dotent d'une politique d'utilisation de la vidéosurveillance à la lumière des règles proposées.

Dans un récent rapport sur l'installation de caméras de surveillance par le Service de police de la Ville de Montréal, la CAI a pu démontrer, en fonction des règles applicables signalées ci-dessus, que l'utilisation des caméras de surveillance dans le Quartier latin de la ville n'était pas justifiée et

¹⁴⁷ COMMISSION D'ACCÈS À L'INFORMATION, « Consultation publique. L'utilisation de caméras de surveillance par des organismes publics dans les lieux publics », Document de présentation, [en ligne] mai 2003, p. 9 [http://www.cai.gouv.qc.ca/05_communique_et_discours/01_pdf/cons_cam.pdf]

¹⁴⁸ *Ibid.*, p. 22.

¹⁴⁹ *Ibid.*, Annexe 1.

¹⁵⁰ COMMISSION D'ACCÈS À L'INFORMATION, « Consultation publique. L'utilisation de caméras de surveillance par des organismes publics dans les lieux publics », Sommaire du bilan de la consultation publique, [en ligne] juin 2004, p. 3 [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/sommaire_bilan.pdf]

¹⁵¹ *Ibid.*

¹⁵² « Big Brother : ' le danger existe ' de voir la Grande-Bretagne devenir ' une société sous surveillance ' », avec l'Agence France Presse [en ligne] 16 août 2004 [http://www.bethel-fr.com/afficher_info.php?id=11026.9]

¹⁵³ COMMISSION D'ACCÈS À L'INFORMATION, *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, [en ligne] juin 2004, p. 3 [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/nouvelles_regles_2004.pdf]

rappeler que le Service de police de la Ville de Montréal est tenu de respecter les règles en vigueur¹⁵⁴.

Mais qu'en est-il pour le secteur privé et les droits des travailleurs, des usagers ou des visiteurs de certaines installations sous surveillance? Dans son Livre blanc consacré à la sécurité privée, le ministère de la Sécurité publique observe à cet égard que «à travers les diverses législations [canadiennes], la sécurité interne aux entreprises ne fait pas partie du champ d'application de la loi, mais demeure un sujet de préoccupation [...]»¹⁵⁵.

3.4.2 La cybersurveillance

Dans son rapport quinquennal de 2003, la CAI s'interroge sur les développements de la cybersurveillance des travailleurs et note que «la capacité de surveillance risque de remettre en question l'équilibre actuel des rapports entre employeur et employé, au détriment de ce dernier. Elle risque aussi de réduire de façon significative l'espace de la vie privée des travailleurs, car la nouvelle technologie digitale ne distingue pas entre les activités de la vie privée et celles du monde du travail¹⁵⁶. » L'organisme n'en reconnaît pas moins les droits traditionnels d'un patron dans la bonne gestion de son entreprise et la supervision du travail de son personnel en ce sens et propose donc cinq principes à respecter en milieu de travail :

- le droit à la vie privée ;
- la surveillance la moins intrusive possible ;
- les moyens proportionnels à l'objet ;
- l'avis aux employés ;
- la sécurité et la confidentialité.

En outre, il est important de noter que le droit canadien, comme l'observe Michael Geist¹⁵⁷, a graduellement reconnu au fil des ans, des normes adoptées et de leur application dans diverses situations, que la surveillance sur les lieux de travail ne peut être justifiée par un simple avis au personnel. Les activités de surveillance doivent avoir un caractère raisonnable qui témoigne de la recherche d'un équilibre entre les préoccupations des employeurs et la vie privée de leurs employés.

En France, la Commission nationale de l'informatique et des libertés (CNIL) note, dans un rapport publié en 2004 : «[...] avec l'émergence des nouvelles technologies de communication et tout particulièrement l'introduction d'internet dans l'entreprise, c'est une véritable migration des technologies de contrôle qui s'opère de la périphérie jusqu'au cœur du processus de travail proprement dit.¹⁵⁸ »

¹⁵⁴ COMMISSION D'ACCÈS À L'INFORMATION, communiqué de presse, [en ligne] 7 avril 2005 www.cai.gouv.qc.ca/05_communiques_et_discours/commun_07_04_05.html] et *Rapport final d'enquête concernant l'installation de caméras de surveillance par le Service de police de la Ville de Montréal*, [en ligne] février 2005 [\[http://www.cai.gouv.qc.ca/06_documentation/01_pdf/Robot_Cam_rapportfinal.pdf\]](http://www.cai.gouv.qc.ca/06_documentation/01_pdf/Robot_Cam_rapportfinal.pdf)

¹⁵⁵ MINISTÈRE DE LA SÉCURITÉ PUBLIQUE, *La sécurité privée partenaire de la sécurité intérieure*, Livre blanc, décembre 2003, p. 21.

¹⁵⁶ COMMISSION D'ACCÈS À L'INFORMATION, *Une réforme de l'accès à l'information : le choix de la transparence*, Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dans le secteur privé, [en ligne] novembre 2002, p.135 [\[http://www.cai.gouv.qc.ca/06_documentation/01_pdf/quin.pdf\]](http://www.cai.gouv.qc.ca/06_documentation/01_pdf/quin.pdf)

¹⁵⁷ Michael A. GEIST, "Computer and e-mail workplace surveillance in Canada: the shift from reasonable expectation of privacy to reasonable surveillance", *The Canadian Bar Review/La Revue du Barreau canadien*, vol. 82, no 2, août 2003, p. 178.

¹⁵⁸ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS – CNIL (France), « La cybersurveillance sur les lieux de travail », [en ligne] 2004, p. 9 [\[http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf\]](http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf)

La cybersurveillance : entre la sécurité de l'employeur et la vie privée de son personnel

« Jusqu'à présent, qu'il s'agisse d'autocommutateur téléphonique, de badges et de contrôle d'accès ou de vidéosurveillance, la surveillance concernait principalement la présence ou la localisation physique de l'individu. [...] Progressivement, l'information dont disposent les entreprises est numérisée, quelle que soit la nature de cette information. Dès lors qu'elle est informatisée et susceptible d'accès par internet ou intranet, des risques d'accès indus à cette information sont réels. Pour l'entreprise, les nouvelles technologies de l'information et de la communication vont naturellement poser des problèmes nouveaux en matière de sécurité dès lors que se trouvent externalisées des informations sur toute la vie de l'entreprise, ses fichiers de personnels, la gestion des commandes, ses secrets de fabrique, etc. Pour les salariés, la différence de nature entre les TIC et tout ce qui précède réside en la capacité nouvelle de la technologie de conserver toutes les traces laissées par la personne connectée. [...] Un message électronique que le salarié a cru supprimer peut avoir été sauvegardé sur un serveur de messagerie ou sur un support magnétique de sauvegarde. »

Commission nationale de l'informatique
et des libertés (France)¹⁵⁹

À l'instar de la CAI au Québec, la CNIL s'interroge aussi sur l'équilibre à préserver entre les droits légitimes de l'entreprise en matière de sécurité et le droit à la vie privée des travailleurs, dans un contexte où existe un lien de subordination entre le travailleur et son employeur mais où existe aussi « la part irréductible de liberté des hommes et des femmes dans une société démocratique.¹⁶⁰ » Parce que l'employeur veut protéger l'information inhérente à son entreprise et s'assurer d'une utilisation judicieuse du temps de travail de chacun, est-il par le fait même autorisé à exercer un contrôle sur les courriels personnels de ses employés et sur les sites internet auxquels ils accèdent pendant leurs heures de travail?

S'appuyant sur les principes de proportionnalité (moyens utilisés par rapport aux finalités recherchées) et de protection de l'intimité de la vie privée du salarié sur son lieu de travail et sur l'obligation de transparence imposée par les lois en vigueur, la CNIL souligne que « les impératifs de l'entreprise et le nécessaire respect de la vie privée des salariés doivent [...] être conciliés, grâce à la discussion collective et à la formation des utilisateurs à la sécurité informatique.¹⁶¹ » Bref, selon la CNIL, s'il est normal et légitime qu'un employeur utilise les moyens technologiques à sa disposition pour assurer la sécurité de son système informatique et de ses différentes applications (comme la messagerie et l'accès à internet), il serait inacceptable qu'il se livre à un contrôle constant des faits et gestes de son personnel¹⁶².

3.5 Éléments de réflexion

Plusieurs craignent aujourd'hui l'avènement d'une société sous surveillance et l'omniprésence de « Big Brother ». Les mesures mises en place ou envisagées pour assurer la sécurité du territoire, celle des citoyens et celle des entreprises portent à croire que le scénario n'est pas surréaliste. Au nom de la sécurité, il apparaît aujourd'hui possible d'avoir des exigences moindres à l'égard de la protection des renseignements personnels et de leur confidentialité, du droit à la vie privée et des libertés civiles. Faut-il que ce soit le cas? Peut-il exister un équilibre entre la sécurité et les libertés individuelles et civiles?

4. L'ENCADREMENT NORMATIF

Depuis de nombreuses années déjà, des lois ont été édictées pour protéger les renseignements personnels et le droit à la vie privée des citoyens. Toutefois, le développement fulgurant de

¹⁵⁹ *Ibid.*

¹⁶⁰ *Ibid.*, p. 7.

¹⁶¹ *Ibid.*, p. 22.

¹⁶² *Ibid.*

l'information et de la communication électroniques a fait en sorte que cette législation n'est pas toujours adaptée aux réalités nouvelles et qu'il est possible d'aller à l'encontre de l'esprit de la loi en cette matière. Des aménagements importants ont été faits aux lois existantes afin d'y inclure de nouvelles règles ou d'adapter les règles existantes. Le besoin se répète aujourd'hui avec l'émergence des technologies biométriques qui imposent de nouvelles législations ou l'adaptation de celles qui existent pour assurer la protection de la vie privée et des droits fondamentaux des citoyens.

4.1 À l'échelle internationale

En juin 2002, une sous-commission « biométrie » (SC 37) a été instituée au sein de la commission ISO/IEC (JTC1) sur les technologies de l'information et la présidence en a été confiée en décembre 2002 au National Institute of Standards and Technology (NIST – États-Unis) pour les trois prochaines années. Cet organisme est ainsi appelé à coordonner les travaux de normalisation conduits au niveau national au sein de l'InterNational Committee for Information Technology Standards (INCITS) et au niveau international, avec l'objectif d'accélérer les procédures nécessaires pour aboutir à la définition de normes de compatibilité et d'évaluation des performances des technologies biométriques.

Pour sa part, le General Accounting Office (GAO – États-Unis) a émis des réserves sur les technologies biométriques en mars 2003. Il a mis en évidence les bouleversements introduits dans les procédures de contrôle, proposant que, pendant dix années, les visas actuels coexistent avec des « visas biométriques ». Il a aussi souligné les failles d'un système insuffisamment préparé, tant en ce qui concerne les règles de gestion d'une liste de contrôle que la sécurité du document lui-même, s'est interrogé sur la portée juridique du dispositif envisagé au regard du Privacy Act de 1974 et a enfin rappelé le principe de réciprocité applicable en matière de visas et de passeports – les exigences des États-Unis à l'égard des ressortissants étrangers donneront lieu à des exigences semblables de la part d'autres pays à l'égard des ressortissants américains – et la nécessité d'unifier les données biométriques susceptibles d'être retenues par d'autres pays pour leurs passeports¹⁶³.

4.2 À l'échelle canadienne

En 2003, Citoyenneté et Immigration Canada reconnaissait qu'il n'existe pas encore de loi fédérale qui considère l'utilisation des technologies biométriques comme outils de collecte d'information et établisse les balises nécessaires en la matière, notamment en ce qui a trait à la protection de la vie privée et des renseignements personnels¹⁶⁴. Pour le moment, et de façon indirecte, ce sont la *Charte canadienne des droits et libertés*, le *Code criminel*, la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques*, cette dernière en vigueur depuis janvier 2001, qui servent de garde-fou aux abus et aux dérives qui pourraient se produire (voir l'encadré). Deux provinces, l'Ontario et le Québec, se démarquent cependant par le cadre juridique qu'elles ont mis en place pour protéger les citoyens : la *Loi de 1997 sur le programme Ontario au travail* (Ontario) et la *Loi concernant le cadre juridique des technologies de l'information* (Québec)¹⁶⁵.

¹⁶³ OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, 2^e partie, p. 37 et 38.

¹⁶⁴ CITOYENNETÉ ET IMMIGRATION CANADA, « Biométrie : incidences ... », Document d'information, *op. cit.*, p. 20.

¹⁶⁵ *Ibid.*, p. 21.

Faut-il revoir les lois en fonction de la biométrie?

« Au niveau fédéral, la *Loi sur la protection des renseignements personnels*, entrée en vigueur en 1983, régit la manière dont quelque 150 institutions fédérales recueillent, utilisent et communiquent les renseignements personnels au sein du secteur public. Chaque province et territoire a adopté un texte semblable applicable au secteur public.

Le gouvernement du Canada a fait un pas de plus en établissant des normes de protection des renseignements personnels applicables au traitement des renseignements dans le secteur privé commercial. Progressivement depuis 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques [LPRPDÉ]* régit le traitement des renseignements personnels dans le secteur privé pour l'ensemble du pays. Plusieurs provinces ont adopté des normes semblables de confidentialité. La *LPRPDÉ* harmonise le droit canadien avec les normes élaborées par l'Union européenne en matière de renseignements personnels, et elle signifie que nos normes concernant la protection des renseignements personnels, lorsqu'elles sont appliquées par une organisation commerciale, comptent parmi les plus rigoureuses au monde. La *LPRPDÉ* établit un cadre progressiste, fondé sur les normes internationales les plus élevées, par rapport auxquelles seront évaluées les pratiques de gestion des renseignements personnels observées par les secteurs public et privé au Canada. Elle constitue un cadre de référence en matière de pratiques exemplaires, et elle encourage les organisations qui recueillent et traitent les renseignements personnels à observer ces pratiques de saine gestion. »

Commissariat à la protection
de la vie privée au Canada¹⁶⁶

Pour sa part, le Commissariat à la protection de la vie privée du Canada a émis quatre critères ayant pour but de déterminer les répercussions des technologies biométriques et d'autres mesures de sécurité sur la vie privée¹⁶⁷ :

1. la mesure est manifestement nécessaire pour répondre à certains besoins;
2. tout indique que la mesure sera probablement efficace pour satisfaire les besoins à l'origine du déploiement proposé;
3. l'ingérence dans la vie privée est proportionnelle à l'avantage en matière de sécurité;
4. il peut être montré qu'aucune autre mesure comportant une ingérence moindre dans la vie privée ne permettrait pas d'atteindre les mêmes résultats.

En ce qui a trait à la loi ontarienne, elle spécifie que tous les renseignements biométriques doivent être recueillis directement et au su de l'intéressé et qu'ils doivent être encodés; ils ne peuvent servir d'identificateur de dossier unique, ni être emmagasinés dans une base de données centrale¹⁶⁸.

4.3 À l'échelle québécoise¹⁶⁹

Au Québec, la *Charte des droits et libertés de la personne* (L.R.Q., c. G12) garantit à toute personne le droit au respect de sa vie privée. La technologie biométrique ne peut être déployée sans que soit pris en compte ce droit fondamental reconnu aux citoyens québécois.

Depuis 2001, la *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q., c. C-1.1) répond en partie aux inquiétudes que soulève le recours à la biométrie. Ainsi, conformément à

¹⁶⁶ « Communication transfrontalière de renseignements sur les Canadiens et les Canadiennes – Répercussions de la *USA Patriot Act* », Mémoire du COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA présenté au Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, Jennifer Stoddart, Commissaire à la protection de la vie privée du Canada, [en ligne] 18 août 2004. [http://www.privcom.gc.ca/media/nr-c/2004/sub_usapa_040818_f.pdf]

¹⁶⁷ « La biométrie faciale est-elle à la hauteur? », Le Bureau des passeports du Canada répond à la question, *IJJ@L'ŒUVRE*, Numéro spécial sur la biométrie, été 2004, p. 21.

¹⁶⁸ *Ibid.*

¹⁶⁹ La Commission remercie M^e Danielle Parent pour sa collaboration au contenu de cette section du texte.

l'article 44 de cette loi¹⁷⁰, un organisme public ou privé ne peut obliger une personne à établir son identité au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. Pour avoir recours à un tel procédé, un consentement exprès de la personne doit être obtenu. De plus, la saisie de données biométriques doit se limiter à ce qui est strictement nécessaire et ne doit pas être faite à l'insu de la personne. L'article 45 de cette loi ajoute aux obligations des organismes celle de divulguer à la Commission d'accès à l'information la création de toute banque de caractéristiques ou de mesures biométriques. Toujours en vertu de cette disposition, la CAI possède divers pouvoirs qui lui permettent, par exemple, de suspendre ou interdire la mise en service d'une base de données biométriques ou même d'en ordonner la destruction.

Mais quelle est la portée réelle de ces articles 44 et 45 ? Ces deux dispositions sont inscrites au chapitre de la loi qui détermine les règles pour établir un lien entre une personne et un document technologique. Les règles pour la collecte des données biométriques peuvent-elles s'appliquer pour d'autres fins, par exemple pour assurer le contrôle des accès à des locaux ou autres sites physiques ou virtuels ?

Outre la *Loi concernant le cadre juridique des technologies de l'information*, la législation québécoise précise d'autres obligations qui doivent s'appliquer à la collecte, l'utilisation, la conservation ou la communication de renseignements personnels, qu'ils s'agisse de renseignements biométriques ou non. Ces obligations sont précisés dans les lois suivantes : pour les organismes publics, il s'agit de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) et, pour les entreprises du secteur privé, de la *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1).

Dans la foulée de son document d'analyse¹⁷¹, la Commission d'accès à l'information a défini neuf principes d'application de la biométrie qui découlent des effets combinés de ces trois lois québécoises. Ces principes, accompagnés d'une série de questions pour guider toute personne souhaitant utiliser la biométrie au sein de son organisation, sont¹⁷² :

1. les solutions de rechange à la biométrie;
2. le caractère indispensable des renseignements recueillis;
3. la collecte auprès de la personne concernée;
4. le consentement à l'utilisation de la biométrie;
5. la conservation et la sécurité des données biométriques;
6. l'utilisation des données biométriques;
7. la communication de données biométriques;
8. la destruction de données biométriques;
9. les droits d'accès et de rectification.

4.4 Éléments de réflexion

Il est important de reconnaître que des efforts sont réalisés sur le plan juridique pour accompagner l'évolution des technologies de l'information et de la communication, y compris leur ouverture récente sur les technologies biométriques. Toutefois, compte tenu des utilisations actuelles et potentielles de ces dernières, tout autant par l'État que par l'entreprise privée et même les

¹⁷⁰ Voir l'annexe 4 pour les articles de loi signalés dans le texte.

¹⁷¹ COMMISSION D'ACCÈS À L'INFORMATION, « La biométrie au Québec : Les enjeux... », *op. cit.*

¹⁷² COMMISSION D'ACCÈS À L'INFORMATION, « La biométrie au Québec : Les principes d'application pour un choix éclairé », juillet 2002.

particuliers, il importe de s'interroger sur la capacité des lois actuelles à contrer les dérives éventuelles et à assurer la population que ses droits fondamentaux seront protégés.

5. LE QUESTIONNEMENT ÉTHIQUE

Le tour d'horizon qui précède et le questionnement soulevé au fil du texte illustrent que l'utilisation de la biométrie à des fins de sécurité doit être l'objet de préoccupations de la part des citoyens et d'une réflexion éclairée de la part des gouvernements, entre autres en ce qui a trait à la protection des renseignements personnels et au respect de la vie privée. Mais d'autres questions se posent aussi, dans une société démocratique, sur le glissement éventuel vers un renversement du fardeau de la preuve – prouver son innocence plutôt que sa culpabilité – et vers la marginalisation de certains groupes en raison de leur origine ethnique et de leurs croyances. Une double interrogation apparaît fondamentale : le recours aux données biométriques constitue-t-il le moyen le plus adéquat pour contrer les problèmes de sécurité associés au terrorisme, au vol d'identité et à l'intrusion malfaisante dans des sites physiques ou informatiques? ses retombées possibles sur la démocratie, sur les libertés civiles, sur la protection des renseignements personnels, sur le respect de la vie privée, sur certains segments de la population sont-elles suffisamment prises en considération?

Dans la présente section consacrée à l'éthique, la Commission entend soulever des questions et les soumettre au débat public, sans prendre position de façon systématique. Tel que mentionné en introduction, elle le fera lors d'une étape ultérieure, dans le cadre d'un avis et de recommandations aux décideurs politiques et institutionnels, et à la suite d'une consultation qu'elle mènera sur le sujet auprès d'experts et de la population dans le cadre d'un forum.

Voici donc, dans les paragraphes qui suivent, quelques considérations qui ressortent d'un premier contact de la Commission avec la problématique de l'utilisation des données biométriques à des fins de sécurité et les principaux axes dans lesquels elle estime approprié d'orienter la réflexion sur le plan de l'éthique.

5.1 Quelques considérations pour appuyer la réflexion

Les considérations suivantes découlent de l'état de situation présenté tout au long du texte et en rappellent brièvement certains éléments jugés importants pour une réflexion d'ordre éthique, notamment en ce qui concerne les technologies biométriques, la lutte au terrorisme et au vol d'identité, les contrôles d'accès à des sites matériels ou virtuels, les encadrements normatifs.

Les technologies biométriques : il importe de considérer la diversité et le niveau de fiabilité des différentes techniques utilisées, la nature des méthodes d'observation des personnes et de traitement de l'information, le traitement de masse qui peut en résulter, l'élargissement des domaines d'application sur tous les plans et de s'interroger sur les retombées possibles en matière de démocratie et de respect de la vie privée. Pour certains, cependant, ces techniques constituent « de réelles garanties au regard du respect de la vie privée car elles assur[ent] l'intégrité de l'information, évit[ent] l'usurpation d'identité et permett[ent] de limiter l'accès aux données sensibles. À ce titre, elles font partie des techniques protectrices de la vie privée (*PET – Privacy enhancing technology*)¹⁷³. »

La sécurité internationale et le combat antiterrorisme : il faut sans doute se demander si la peur est bonne conseillère... et si une recherche inconditionnelle de sécurité est garante de l'adoption de politiques ou de mesures à la fois valables, efficaces et équitables. Des décisions politiques et gouvernementales ont été prises rapidement dans la foulée du 11 septembre; peut-

¹⁷³ John D. WOODWARD, « Biometrics: Privacy's Foe or Privacy's Friend », *Proceedings of the IEEE*, vol. 85, n° 9, septembre 1997, p. 1487 – traduction tirée de OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, 1^{ère} partie, p. 59.

être le fallait-il, car l'État a une obligation de protection à l'égard de ses citoyens et ceux-ci exigent d'être adéquatement protégés. Mais toutes les facettes et les implications des mesures mises en place ont-elles été correctement évaluées et pesées en ce qui a trait aux exigences de la démocratie et au respect des citoyens?

La sécurité intérieure et la lutte contre le vol d'identité : le problème n'est certes pas nouveau mais l'augmentation de la pauvreté, de l'immigration, des transactions électroniques et d'autres facteurs comme l'importance accordée à la consommation et la facilité à obtenir du crédit ont fait en sorte qu'il s'est considérablement amplifié. Les pièces d'identité sont devenues des documents précieux; il importe qu'elles demeurent des documents uniques qui répondent aux exigences de sécurité et qui puissent garantir la libre circulation des citoyens ainsi que leur accès aux services qui leur sont destinés. De plus en plus, les sociétés occidentales envisagent l'adoption d'une carte d'identité nationale avec données biométriques, mais très souvent aussi la population manifeste des réserves à cet égard et se demande quelles pourraient être les solutions de rechange.

La sécurité matérielle ou virtuelle et les contrôles d'accès aux sites : la Commission d'accès à l'information note que « ce qui saute d'abord aux yeux c'est qu'un remède pour l'un n'est pas toujours bon pour l'autre. Par exemple, l'employeur qui installe un système biométrique pour enregistrer les entrées et sorties de son personnel peut y voir une solution au vol de temps dont il croit être victime. Pour les employés le recours à la biométrie par leur employeur peut constituer un système de surveillance des plus invasifs pour la vie privée. En fait, bien que la plupart des techniques biométriques soient des outils de sécurité fort efficaces, ils ne brillent pas par leur innocuité en ce qui concerne la protection de la vie privée des personnes qui les utilisent¹⁷⁴. » Bien des organisations disposent de contrôles d'accès qui ne reposent pas sur l'utilisation de données biométriques; l'existence même de ces technologies suffit-elle pour en banaliser à la fois l'usage et la collecte de renseignements censés être « personnels »?

Les encadrements normatifs : la Commission européenne estime que « les outils de protection des données et de la vie privée préservent les personnes des mesures d'ingérence excessives de la part des autorités gouvernementales ou des acteurs privés. Ils protègent les individus d'un déséquilibre dans les pouvoirs qui porterait atteinte à leur liberté individuelle, mais aussi de pratiques comme le profilage, l'exploration et le suivi des données qui permettent d'exercer sur eux un contrôle presque total¹⁷⁵. » Il apparaît légitime de se demander si c'est bien le cas et si la législation actuelle permet non seulement d'assurer aux citoyens le niveau de protection auquel ils s'attendent mais aussi d'intervenir rapidement et efficacement auprès des contrevenants.

Quel que soit l'angle sous lequel sont abordées les technologies biométriques, les enjeux politiques, sociaux, éthiques et économiques de cette évolution de la science et de la technologie sont importants. La Commission estime qu'une réflexion globale s'impose pour garantir la pertinence des moyens mis en œuvre et leur innocuité sur la société et sur l'ensemble de ses citoyens.

5.2 Des questions à poser et à débattre

Les technologies biométriques peuvent être considérées comme des techniques répressives et intrusives, par exemple¹⁷⁶ :

- le fait de pouvoir être constamment filmé ou photographié de près ou de loin, à notre insu ou non;
- le fait de pouvoir être suivi à la trace dans nos déplacements dans nos lieux de travail ou ailleurs ou par notre clavier d'ordinateur;

¹⁷⁴ COMMISSION D'ACCÈS À L'INFORMATION, « La biométrie au Québec : Les enjeux... », *op. cit.*, p. 23.

¹⁷⁵ INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPITS), *op. cit.*, p. 7.

¹⁷⁶ Cf. Bernard DIONNE et Évelyne RACETTE, *op. cit.*, p. 9.

- le fait de pouvoir être pisté par notre odeur corporelle ou la température de notre corps ou par notre manière de marcher;
- le fait de devoir présenter nos mains, notre visage, nos empreintes digitales, nos oreilles, nos yeux, notre ADN pour s'identifier ou être reconnu par un appareil quelconque;
- le fait de pouvoir être présumé coupable d'être un terroriste ou un fraudeur ou d'avoir des intentions malveillantes dans certains de nos agissements;
- le fait de devoir être obligé de se soumettre plusieurs fois par jour à des technologies de reconnaissance pour être reconnu ou identifié.

Mais elles sont aussi perçues comme des techniques pouvant protéger la vie privée. Il y a donc là un paradoxe important. Dans les paragraphes qui suivent, en s'appuyant sur cette prémisse, la Commission tente d'aborder la question en fonction d'un certain nombre d'enjeux que soulève la problématique sur le plan de l'éthique.

5.2.1 ... sur le respect de la démocratie

Le respect de la démocratie est une question relativement peu traitée dans la documentation consacrée aux technologies biométriques. De façon générale, la mise en place de systèmes biométriques soulève des inquiétudes sur la protection des libertés, de la vie privée et des droits fondamentaux des personnes, des valeurs qui sont représentatives des sociétés démocratiques. Et des observateurs notent « une évolution vers une forme de maintien de l'ordre reposant sur la collecte d'information grâce à l'utilisation de technologies de surveillance de masse très performantes¹⁷⁷. »

Citoyenneté et Immigration Canada convient qu'assurer la sécurité collective des citoyens est une responsabilité fondamentale de l'État. Pour ce faire, précise l'organisme, il peut cependant arriver que les mesures mises en place par l'État constituent une atteinte à la vie privée et aux libertés des citoyens. Si certains estiment que de telles façons de faire sont justifiées en raison des bénéfices escomptés, d'autres maintiennent que la protection des libertés individuelles et de celles des minorités est le fondement d'une société saine et démocratique¹⁷⁸.

La biométrie est reconnue comme une technologie qui, par les mécanismes de surveillance qu'elle permet, donne un pouvoir important aux États et aux organisations dans le contrôle des personnes (citoyens ou employés)¹⁷⁹. Comment exprimer sa dissension, manifester son désaccord, exercer un libre choix dans une société sous surveillance où un secret bien gardé sera bientôt un anachronisme? À la suite du 11 septembre, bon nombre des mesures de sécurité qui ont été mises en place ont eu pour effet de renforcer les pouvoirs des gouvernements et des systèmes judiciaire et policier, notamment pour leur permettre d'exiger des citoyens des informations à caractère personnel beaucoup plus détaillées qu'auparavant et d'y accéder à d'autres fins que celles pour lesquelles elles ont été initialement fournies¹⁸⁰.

Question : L'utilisation des technologies biométriques risque-t-elle de porter atteinte à la démocratie et de quelle façon? (enjeu du respect de la démocratie, enjeu de rationalité instrumentale)

5.2.2 ...sur le renversement du fardeau de la preuve

Dans les sociétés de droit, toute personne bénéficie d'une présomption d'innocence face à la loi. Le recours à l'utilisation des technologies biométriques pour confirmer l'identité d'une personne

¹⁷⁷ INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS), *op. cit.*, p.5

¹⁷⁸ CITOYENNETÉ ET IMMIGRATION CANADA, « Biométrie: incidences ... », Document d'information, *op. cit.*, p. 15.

¹⁷⁹ Roger CLARKE, « Biometrics and Privacy », *op. cit.*, p. 7.

¹⁸⁰ INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS), *op. cit.*, p. 4.

risque de renverser ce principe juridique. En effet, advenant le refus d'un système biométrique à authentifier l'identité d'une personne dans le contexte d'une comparaison avec sa signature biométrique (à un poste frontière, par exemple) ou dans le cas d'un vol d'identité, comment prouver qui l'on est – « en théorie, personne d'autre qu'un individu ne peut utiliser son propre corps¹⁸¹ » et si les caractéristiques biométriques de ce corps sont utilisées par deux personnes différentes, comment rétablir la vérité? « Comment un utilisateur de bonne foi peut-il démontrer son innocence en cas de problème? Comment peut-il découvrir et exposer les failles d'un système complexe dont il ignore le fonctionnement?¹⁸² ». Quels sont les droits de la victime?

Question : Dans un contexte où contrôle et surveillance visent à créer un environnement sécuritaire au bénéfice de l'ensemble de la population, comment protéger l'*a priori* d'innocence? comment assurer les droits des victimes? (enjeu de justice)

5.2.3 ...sur la validité d'une donnée biométrique

L'interrogation qui précède sur le renversement du fardeau de la preuve soulève la question de la validité d'une donnée biométrique, de son caractère « authentique », advenant contestation de la part d'une personne qui en aurait été dépossédée. Ainsi, dans le cas¹⁸³ d'une personne qui ne serait pas autorisée à monter à bord d'un avion ou à entrer dans un pays donné à la suite d'une erreur d'identité reposant sur des données biométriques, de quels recours dispose-t-elle si, par exemple, ses propres empreintes digitales, les caractéristiques de son visage ou de son iris ne sont pas reconnues par le système ou sont attribuées à un terroriste potentiel? S'agit-il d'une preuve « incontestable »?

Dans un contexte judiciaire, par exemple, l'information stockée dans un système biométrique pourrait-elle éventuellement tenir lieu de preuve pour incriminer ou innocenter un prévenu, comme c'est déjà le cas pour l'ADN et les empreintes digitales?

Question : Faut-il mettre en place des mécanismes pour protéger les citoyens des erreurs qui pourraient se produire sur la foi de résultats fournis par un système biométrique? (enjeu d'équité et de justice, de respect de la personne)

5.2.4 ... sur la protection des données personnelles : confidentialité et vie privée

La question de la protection des données personnelles est indissociable des systèmes biométriques car les mesures biométriques sont considérées comme des renseignements confidentiels. C'est à ce titre qu'elles sont protégées par des mécanismes propres à assurer leur caractère confidentiel, comme la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1, art. 53), la *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1, art. 10) et la *Loi concernant le cadre juridique des technologies de l'information* (L.Q. 2001, c. 32, art. 44 et 45) mentionnées précédemment.

En principe, seules les personnes autorisées à accéder aux données personnelles y accéderont effectivement. Un problème peut toutefois se poser lorsqu'une personne exerce son droit d'accès à l'information colligée ou de rectification de cette information (articles 83 et 89 de la Loi sur l'accès, articles 27 et 28 de la Loi dans le secteur privé et article 40 du Code civil¹⁸⁴), en raison du processus de numérisation appliqué à l'information brute qui rend celle-ci visuellement indéchif-

¹⁸¹ COMMISSION D'ACCÈS À L'INFORMATION, « La biométrie au Québec : Les enjeux... », *op. cit.*, p.28.

¹⁸² *Ibid.*

¹⁸³ COMMISSION EUROPÉENNE, *op. cit.*, p. 10.

¹⁸⁴ COMMISSION D'ACCÈS À L'INFORMATION, « La biométrie au Québec : Les enjeux... », *op. cit.*, p. 37.

frable¹⁸⁵. Il devient dès lors quasi impossible de vérifier l'authenticité et la qualité de la « signature ». Ce que toute personne peut faire dans le cas de son dossier de crédit, par exemple, quand elle veut s'assurer que son contenu est à jour et conforme à la réalité.

Comme l'observe l'IPTS, « la protection de la vie privée et des données devient plus importante à mesure que nos sociétés évoluent vers ce que nous pourrions appeler des sociétés de "surveillance"¹⁸⁶. » Dans son document d'information, Citoyenneté et Immigration Canada note cependant que « des experts de l'industrie insistent sur le fait que la biométrie n'est pas en soi une technologie intrusive et qu'elle peut être utilisée de façon efficace pour réduire les atteintes à la vie privée. Selon eux, il ne faut pas nécessairement sacrifier la vie privée pour garantir la sécurité et vice versa et, en principe, les deux peuvent bénéficier d'une utilisation transparente et légitime d'un système biométrique bien conçu. Les répercussions sur la vie privée dépendent de la façon dont la biométrie est utilisée, pas de la technologie elle-même¹⁸⁷. » Il peut être utile de rappeler ici à quel point les avis sont partagés sur ce sujet. En outre, dans un système conçu pour l'authentification des personnes (1 sur 1), un stockage décentralisé de l'information est généralement suffisant; mais dans une perspective d'identification (1 sur n), notamment en matière judiciaire, le processus repose sur le balayage de données centralisées dans une ou plusieurs bases de données. Or, certains experts en sécurité admettent que les bases de données centralisées constituent un risque en soi¹⁸⁸; en outre, pour les données biométriques conservées sur un support portable, les possibilités de vol du support lui-même et de la capture d'information à l'insu des utilisateurs doivent être envisagées¹⁸⁹.

Il apparaît important de souligner que les systèmes biométriques sont des systèmes informatiques autonomes ou installés en réseaux. Lorsqu'elles sont stockées dans une mémoire centralisée et non pas sur un disque dur ou sur une micro-puce, les données biométriques « voyagent » et peuvent être couplées avec des données présentes dans d'autres bases de données ayant en mémoire d'autres types d'information sur les mêmes personnes, permettant ainsi de créer un profil de plus en plus complet d'une personne au fur et à mesure que les renseignements la concernant s'apparient. Autre possibilité, plus l'information s'« enrichit » et plus la base de données s'élargit, plus s'excite la convoitise des pirates informatiques qui chercheront à profiter de façon malveillante et mercantile des « nombreuses vulnérabilités de ces réseaux, des logiciels qui les soutiennent et des bases de données¹⁹⁰ » qu'ils contiennent.

Heureusement, comme l'observe la CAI, la loi québécoise ne permet pas aux organismes de partager l'information recueillie sur les personnes, sauf dans certaines circonstances, et encourage un cloisonnement de l'information susceptible de protéger la vie privée¹⁹¹. Toutefois, dans un contexte où la centralisation et l'intégration des systèmes d'information constituent un atout sur le plan économique et en matière d'accès à l'information par un plus grand nombre de personnes, il y a un risque accru que l'État souhaite tirer profit de cette mine d'information¹⁹² à toutes sortes de fins, bénéfiques ou non pour la société dans son ensemble ou certains segments de la population particulièrement vulnérables.

La question des transferts transfrontaliers présenterait les incertitudes les plus inquiétantes. En effet, souligne le rapport français déjà mentionné, « on peut [...] estimer qu'à terme, par l'effet de l'intensification des échanges de données, les États ayant défini des règles strictes quant au traitement des données biométriques seront conduits à s'aligner sur ceux ayant fait preuve d'une plus grande souplesse, d'autant que, à la différence des numéros d'identification nationaux, les

¹⁸⁵ OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, 2^e partie, p. 21 et 22.

¹⁸⁶ INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS), *op. cit.*, p. 7.

¹⁸⁷ CITOYENNETÉ ET IMMIGRATION CANADA, « Biométrie : incidences... », Document d'information, *op. cit.*, p. 19.

¹⁸⁸ COMMISSION D'ACCÈS À L'INFORMATION, « La biométrie au Québec : Les enjeux... », *op. cit.*, p. 30.

¹⁸⁹ *Ibid.*, p. 33.

¹⁹⁰ *Ibid.*, p. 30.

¹⁹¹ *Ibid.*, p. 26.

¹⁹² *Ibid.*

techniques biométriques permettront de fournir des identifiants 'universels'¹⁹³. » À noter que le G8 a adopté, en mai 2003, des principes directeurs afin d'améliorer l'échange d'informations sur les empreintes génétiques¹⁹⁴.

Question : Les mécanismes actuels de protection des renseignements personnels permettent-ils d'en assurer pleinement la confidentialité et le respect de la vie privée? sont-ils adéquatement adaptés à l'émergence des technologies biométriques? d'autres mesures s'imposent-elles à cet égard? (enjeu de confidentialité et de respect de la vie privée, d'équité)

5.2.5 ...sur le stockage et la gestion des données : accès, utilisation, divulgation

Contrairement à bien d'autres sociétés occidentales, le Québec peut s'appuyer sur un cadre législatif en ce qui a trait aux bases de données biométriques. En effet, l'article 45 de la *Loi concernant le cadre juridique des technologies de l'information* donne à la Commission d'accès à l'information un pouvoir d'ordonnance sur les bases de données biométriques en matière de confection, d'utilisation, de consultation, de communication et de conservation des données biométriques, y compris l'archivage ou la destruction des mesures ou des caractéristiques qui auraient été prises pour établir l'identité d'une personne, pouvoir qui l'autorise même à ordonner la destruction d'une base de données si elle le juge nécessaire.

Les principaux points prévus dans la législation actuelle sont les suivants :

- l'accès à l'information colligée : seules les personnes mandatées pour recevoir et utiliser cette information dans l'exercice de leurs fonctions peuvent y accéder (art. 62, *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et art. 20, *Loi sur la protection des renseignements personnels dans le secteur privé*);
- la qualité de l'information : les renseignements doivent être exacts et à jour (art. 72 de la *Loi sur l'accès...* et art. 11 de la *Loi dans le secteur privé*);
- la divulgation de l'information : exige le consentement de la personne concernée ou une disposition législative qui autorise la divulgation (art. 59 de la *Loi sur l'accès...* et art. 13 de la *Loi dans le secteur privé*);
- la destruction de l'information : exige la destruction de l'information quand l'objet qui fondait la vérification est accompli ou que le motif qui la justifie n'existe plus (art. 44 de la *Loi concernant le cadre juridique des technologies de l'information*, 3^e alinéa)

La CAI estime cependant qu'elle n'a pas à intervenir si aucune journalisation (ou conservation en mémoire informatique ou support papier) des accès n'est effectuée; ce serait le cas, par exemple, si l'utilisation des données biométriques sert uniquement à autoriser l'ouverture d'une porte pour donner accès à un local, sans qu'une heure d'entrée, l'identité de la personne ou toute autre donnée personnelle ne soit enregistrée. Il en est ainsi également dans le cas de la conservation des données biométriques sur un support portable ou sur le disque dur d'un ordinateur personnel. Dans ces situations, la collecte de données biométriques n'a pas pour objet d'établir un lien entre une personne et un document et l'article 45 de la *Loi concernant le cadre juridique des technologies de l'information* ne trouverait pas application.

Question : Tous les éléments pertinents au stockage et à la gestion des bases de données biométriques sont-ils pris en compte dans la législation actuelle? et protègent-ils suffisamment l'information colligée contre toute utilisation malveillante? (enjeu de sécurité, d'équité et de confidentialité)

¹⁹³ OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES, *op. cit.*, 2^e partie, p. 23.

¹⁹⁴ *Ibid.*, p. 24.

5.2.6 ...sur la discrimination

Les données biométriques peuvent être qualifiées de « délicates » car certaines d'entre elles, outre l'ADN, peuvent révéler l'origine ethnique d'une personne (la reconnaissance faciale, par exemple) ou son état de santé (la lecture de l'iris, par exemple). Particulièrement sur le plan ethnique, ce sont des données qui peuvent éventuellement se prêter au « ciblage » de certaines catégories de personnes, notamment dans le contexte actuel de lutte au terrorisme.

Sur ce plan, mais aussi sur d'autres aspects de l'information véhiculée par une donnée biométrique, il faut également considérer que des décisions concernant des personnes peuvent être prises de façon automatique par des systèmes informatisés, sur la seule base de l'information disponible. De telles décisions, prises à l'insu de la personne, et fondées sur une information utilisée hors contexte et sur des faits parfois incomplets, imprécis, non pertinents ou utiles, peuvent s'avérer préjudiciables à la personne concernée¹⁹⁵.

Question : Quelle peut-être l'ampleur des risques de discrimination associés à l'utilisation de systèmes biométriques à des fins de sécurité? de quelle façon contrer ces risques? (enjeu d'équité)

5.2.7 ...sur le manque de transparence : le consentement

L'article 44 de la *Loi concernant le cadre juridique des technologies de l'information* stipule que toute vérification ou confirmation de l'identité d'une personne au moyen de mesures biométriques ne peut se faire sans son « consentement exprès ». Il convient cependant de souligner que même le consentement d'une personne à la prise de mesures biométriques ne permet pas de passer outre à l'obligation de nécessité (c'est-à-dire que ce type d'information soit jugé nécessaire) prévue à l'article 64 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et aux articles 4 et 5 de la *Loi sur la protection des renseignements personnels dans le secteur privé*. En d'autres termes, il est interdit à un organisme public de recueillir une donnée biométrique si cette donnée n'est pas nécessaire à l'exercice de ses fonctions ou à la mise en œuvre d'un programme dont il a la gestion. L'obtention d'un consentement ne permet pas de contourner cette interdiction. Il en va de même pour une entreprise du secteur privé qui ne peut recueillir que les seules données qui sont nécessaires à l'objet du dossier constitué sur une personne.

Or, nombre de données biométriques peuvent être recueillies à l'insu de la personne concernée (les empreintes digitales, l'ADN, les traits du visage, la démarche ou la dynamique de frappe sur un clavier, par exemple). Ces technologies ayant un « faible niveau d'intrusion »¹⁹⁶, leur utilisation peut facilement être généralisée et servir à toute sortes de fins, y compris judiciaires. Comme en témoigne la CAI, même des technologies qui normalement nécessitent un consentement des utilisateurs peuvent être modifiées pour identifier une personne sans son consentement. À preuve cet événement récent rapporté par le *National Geographic*¹⁹⁷ : à partir de la comparaison de photos prises d'une jeune inconnue afghane à 17 ans d'intervalle (à 12 ans et à 29 ans), il a été possible de confirmer qu'il s'agissait bien de la même personne sur la base d'une comparaison des traits du visage, mais aussi en procédant à une lecture de l'iris au moyen d'une numérisation des photos et en comparant les données obtenues – à noter que la lecture de l'iris de l'œil se fait habituellement sur l'organe lui-même et à 40cm d'une caméra¹⁹⁸.

¹⁹⁵ COMMISSION D'ACCÈS À L'INFORMATION, « La biométrie au Québec : Les enjeux... », *op. cit.*, p. 31.

¹⁹⁶ COMMISSION EUROPÉENNE, *op. cit.*, p. 5.

¹⁹⁷ « A Life Revealed », Cathy NEWMAN, Special Report, *National Geographic*, avril 2002 (non paginé). Pour réaliser l'authentification de la jeune femme, le magazine a fait appel à un expert du FBI pour la reconnaissance faciale, et à l'inventeur du procédé automatisé de reconnaissance de l'iris, John Daugman à l'université de Cambridge en Angleterre.

¹⁹⁸ COMMISSION D'ACCÈS À L'INFORMATION, « La biométrie au Québec : Les enjeux... », *op. cit.*, p.29.

La Commission de l'éthique s'est déjà penchée sur la notion de consentement dans un avis précédent¹⁹⁹ et a reconnu que, « pour être valide, un consentement doit être libre, éclairé, explicite et donné par une personne apte²⁰⁰ », c'est-à-dire majeure et saine d'esprit. La CAI ajoute qu'il doit également être donné à des fins spécifiques²⁰¹.

Question : Comment s'assurer que l'obligation de consentement est respectée, notamment dans le cas des technologies biométriques qui peuvent être utilisées à l'insu de la personne? comment éviter que le libre choix ainsi autorisé par la loi n'ait pas de conséquences négatives pour la personne qui s'en prévaut? (enjeu de la transparence et du libre choix)

5.2.8 ... sur le respect des finalités

Selon la *Loi concernant le cadre juridique des technologies de l'information*, « la donnée biométrique servira essentiellement à identifier l'individu pour y lier un document. La nécessité d'identifier la personne dans le cadre de la finalité poursuivie devra être intrinsèquement indispensable²⁰². » Ainsi, au moment de la collecte d'une donnée, déclaration doit être faite à la personne sur les finalités poursuivies par la constitution du fichier et l'utilisation qui sera faite des renseignements recueillis (art. 65 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et art. 8 de la *Loi sur la protection des renseignements personnels dans le secteur privé*). Conformément à la loi, c'est donc dire que la finalité doit être explicite, légitime et clairement définie²⁰³ et qu'aucune information révélée par ces données ne peut être utilisée à quelque autre fin que ce soit²⁰⁴.

Toutefois, compte tenu de la somme d'information qui peut être extraite d'une base de données spécifique ou à partir d'un croisement de plusieurs bases de données (biométriques et autres), « le risque d'accroître les possibilités de réutilisation de ces données par des tiers comme éléments de comparaison et de recherche dans le cadre de leurs propres activités, sans que cet objectif ait été envisagé initialement²⁰⁵ » ne peut être occulté – ce que certains appellent le « glissement de fonctions » (fonctions creep) ou le dévoiement des finalités initiales²⁰⁶. Dans le contexte de la lutte au terrorisme et à la criminalité, et à des fins de protection de la population et du territoire, il est permis de croire que les autorités chargées d'appliquer la loi pourraient être du nombre des tiers intéressés²⁰⁷. En fait, il faut noter que les données biométriques, de par leur nature, peuvent contenir davantage d'information que celles nécessaires aux fonctions d'identification ou d'authentification²⁰⁸, sans que ce soit le but recherché. En ce qui a trait aux données biométriques utilisées à des fins de contrôle d'accès, par exemple, « leur utilisation en vue d'évaluer l'état émotionnel de la personne concernée ou de surveiller une personne sur son lieu de travail ne serait pas compatible avec la finalité initiale²⁰⁹. »

Enfin, il faut rappeler que « le stockage centralisé de données biométriques accroît également le risque que ces données soient utilisées comme une clé pour interconnecter différentes bases de données, ce qui pourrait permettre d'obtenir un profil détaillé des habitudes d'un individu, tant dans la sphère publique que dans la sphère privée. La question de la compatibilité des finalités pose également le problème de l'interopérabilité de différents systèmes reposant sur la biométrie. La

¹⁹⁹ *Les enjeux éthiques des banques d'information génétique : pour un encadrement démocratique et responsable*, COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, Gouvernement du Québec, 2003, p. 42 à 49.

²⁰⁰ *Ibid.*, p. 42.

²⁰¹ COMMISSION D'ACCÈS À L'INFORMATION, « La biométrie au Québec : Les enjeux... », *op. cit.*, p. 35.

²⁰² *Ibid.*, p. 36.

²⁰³ COMMISSION EUROPÉENNE, *op. cit.*, p. 6.

²⁰⁴ COMMISSION D'ACCÈS À L'INFORMATION, « La biométrie au Québec : Les enjeux... », *op. cit.*, p. 36.

²⁰⁵ COMMISSION EUROPÉENNE, *op. cit.*, p. 2.

²⁰⁶ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *25^e Rapport d'Activité 2004*, France, p.93.

²⁰⁷ *Ibid.*

²⁰⁸ *Ibid.*, p. 8.

²⁰⁹ *Ibid.*, p. 7.

standardisation qu'exige l'interopérabilité pourrait entraîner une plus forte interconnexion entre les bases de données²¹⁰. »

Question : Comment s'assurer que les finalités énoncées sont respectées et qu'aucun détournement ne puisse se produire au détriment de certaines personnes ou groupes de personnes vulnérables? (enjeu de confiance, de transparence, de respect des personnes, d'équité)

5.2.9 ...sur la proportionnalité des moyens

Les données biométriques et les systèmes biométriques mis en place ont pour but l'identification et l'authentification (la vérification) des personnes pour assurer la sécurité de la population (sur le plan national et international) et des infrastructures matérielles ou informatiques. Les auteurs du document de travail de la Commission européenne notent qu'«une évaluation du respect des principes de proportionnalité et de légitimité doit être effectuée en tenant compte des risques concernant la protection des libertés et des droits fondamentaux de la personne; il s'agit notamment d'établir si la finalité poursuivie ne pourrait pas être atteinte d'une façon moins intrusive²¹¹. »

Dans cet ordre d'idées, il semble opportun de signaler que des techniques de «surveillance de masse», qui misent le plus souvent sur la reconnaissance faciale, sont de plus en plus utilisées par les responsables de l'ordre public qui espèrent ainsi repérer des personnes ou des agissements suspects, et prévenir la criminalité ou les actes terroristes. Toute la population est ainsi susceptible d'être filmée à son insu, pour des motifs qui peuvent sembler louables. De tels procédés sont courants dans les aéroports, ils ont été utilisés à l'étranger lors d'événements sportifs susceptibles de rassembler des milliers de personnes (jeux olympiques, matchs de soccer, etc.), ils sont utilisés dans certaines rues de Montréal propices au trafic de la drogue, etc. À l'heure actuelle, la Grande-Bretagne serait la championne toutes catégories pour l'utilisation de la vidéosurveillance et les particuliers commencent à utiliser cette technique dans leurs foyers (pour se prémunir contre le vol, surveiller des personnes âgées, des enfants ou des gardiennes).

En ce qui a trait aux systèmes biométriques mis en place pour les voyageurs qui utilisent l'avion, et le train dans certains cas, ils ont pour but de contrer l'entrée illicite d'éventuels terroristes. Toutefois, les terroristes peuvent aussi être des citoyens de plein droit du pays qui effectue le contrôle et ceux qui ne le sont pas savent généralement comment contourner les mesures de contrôle qui sont instaurées. Mais tous les citoyens, en majorité des gens qui n'ont rien à se reprocher, seront sous peu soumis au contrôle biométrique de leur identité. Pour le moment, une seule donnée biométrique est retenue pour les passeports : la photo numérisée qui sera authentifiée par un système de reconnaissance faciale. Toutefois, pour augmenter le niveau de sécurité, il est de plus en plus question d'y ajouter aussi les empreintes digitales ou la lecture de l'iris. Jusqu'où ira la collecte d'informations biométriques pour authentifier l'identité des voyageurs?

De la même façon, il convient de s'interroger sur la proportionnalité des mesures de contrôle biométrique utilisées sur les lieux de travail en fonction des objectifs poursuivis et sur les solutions de rechange qui pourraient être envisagées.

Considérant les incidences d'un système qui permet l'identification des personnes et un autre qui se limite à l'authentification ou à la vérification de l'identité d'une personne, il importe de bien saisir quels sont les objectifs poursuivis afin de s'assurer qu'il y a compatibilité entre les finalités et les moyens mis en place. Quel est le problème public à résoudre grâce à l'utilisation de la biométrie et quelle doit être l'ampleur du moyen à mettre en place? S'agit-il de pouvoir identifier des terroristes potentiels ou de certifier l'authenticité des personnes et des documents leur

²¹⁰ *Ibid.*, p. 8.

²¹¹ *Ibid.*, p. 2.

octroyant des droits comme citoyens et résidents d'un pays? La complexité, le coût et le recours aux renseignements personnels sont supérieurs dans un système d'identification qui se prête à des applications plus nombreuses et diversifiées que le système d'authentification/vérification.

Question : Les mesures biométriques constituent-elles une solution souhaitable et appropriée pour répondre aux besoins actuels de contrer le terrorisme, de combattre la criminalité sur le territoire et de protéger les infrastructures matérielles et informatiques contre toute intrusion malveillante? d'autres moyens moins intrusifs pourraient-ils s'avérer tout aussi efficaces? (enjeu de proportionnalité des moyens et d'équité)

5.2.10 ... sur l'instrumentalisation du corps humain

Dans deux de ses avis précédents²¹², la Commission a soulevé un tel risque au regard des problématiques étudiées. Se fondant sur la définition suivante de l'instrumentalisation du corps humain : « toute conception qui réduit la vie à des composantes physico-chimiques et considère que les processus vitaux ne sont pas différents des processus physiques²¹³ », la Commission estime qu'il faut considérer ce risque en ce qui concerne le recours aux technologies biométriques et que cette préoccupation doit faire partie du questionnement éthique. Pour sa part, Roger Clarke parle plutôt de déshumanisation (« *dehumanisation* ») et estime que si les humains méritent encore un respect particulier (par rapport aux biens manufacturés ou aux animaux domestiques), les technologies biométriques sont répugnantes pour les sociétés libres (« *contemporary free societies* »)²¹⁴.

Question : Le recours aux technologies biométriques comporte-t-il un risque d'instrumentalisation du corps humain et de quelle nature serait ce risque? (enjeu du respect de la dignité humaine)

5.2.11 ... sur les effets sur la santé

Le rapport de l'IPTS²¹⁵ publié au printemps de 2005 est l'un des rares documents consultés à s'interroger sur les « aspects médicaux » de la biométrie. Le rapport distingue entre les conséquences médicales directes sur la santé et les conséquences indirectes. Les premières concernent les risques de dommages potentiels qui sont associés à l'utilisation d'appareils de lecture biométrique, les secondes concernent les risques, dits éthiques, que les données biométriques soient utilisées pour révéler des informations confidentielles sur la santé de leur propriétaire.

En ce qui a trait aux effets directs sur la santé, les technologies qui soulèvent des questions à cet égard sont celles qui concernent l'œil (iris et rétine) et celles qui comportent un contact physique direct avec un capteur biométrique (empreintes digitales et paume de la main). Dans le premier cas, les craintes concernent les lésions que les rayons infrarouges pourraient causer à l'œil; dans l'état actuel des choses, la lecture rétinienne n'est pas encore suffisamment développée pour que des problèmes aient été détectés; quant à la reconnaissance de l'iris, aucun problème n'aurait été rapporté jusqu'à présent, malgré le caractère assez répandu de cette technologie. En ce qui concerne les contacts physiques, les craintes sont associées à la contamination possible par le

²¹² Pour une gestion éthique des OGM, COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, Québec, décembre 2003 (p. 78 à 80) et *Le don et la transplantation d'organes : dilemmes éthiques en contexte de pénurie*, COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, Québec, novembre 2004 (p.33).

²¹³ Pour une gestion éthique des OGM, *op. cit.*, p. 78.

²¹⁴ Roger CLARKE, « «Biometrics and Privacy », *op. cit.*, p. 7 – « If we're happy to treat humans in the same manner as manufactured goods, shipping cartons, and pets, then biometrics technologies are unobjectionable. If, on the other hand, humans continue to be accorded special respect, then biometrics technologies are repugnant to contemporary free societies. »

²¹⁵ IPTS, *Biometrics at the Frontier*, *op. cit.*, p.50-54.

biais de la présence de germes ou de bactéries sur le capteur; il est généralement reconnu que ces appareils exigent des mesures spécifiques (nettoyage aux rayons ultraviolets, par exemple) pour contrer le problème.

S'agissant des effets indirects sur la santé, les technologies susceptibles de fournir de l'information sur la santé de la personne concernée sont la lecture rétinienne qui pourrait « peut-être » permettre de détecter un dysfonctionnement vasculaire, la reconnaissance de l'iris (dans la mesure où l'iridologie²¹⁶ obtiendrait une reconnaissance du milieu scientifique) et la reconnaissance faciale qui pourrait révéler l'état émotionnel d'une personne. Pour l'ADN, advenant son utilisation courante en biométrie, le problème des risques de diffusion d'informations personnelles et confidentielles est bien connu. Toutefois, il convient peut-être de souligner ici que l'ADN utilisé à des fins biométriques n'est en fait qu'un fragment non codant qui ne contient aucune information sur le patrimoine génétique de la personne tout en permettant d'obtenir le code qui lui est unique²¹⁷.

Quoi qu'il en soit, la documentation consultée témoigne du peu d'intérêt ou d'attention accordées à la question des effets de la biométrie sur la santé et d'une relative absence d'évaluations scientifiques sur ce sujet.

Question : Peut-il y avoir des effets nocifs pour la santé qui résultent de l'utilisation de certaines applications de la biométrie? de quelle nature pourraient-ils être? des recherches en ce sens sont-elles entreprises? (enjeu de protection de la santé)

5.2.12 ...sur l'encadrement normatif

Le Québec dispose d'une réglementation qui peut tenir compte de la mise en place et de l'utilisation de la biométrie. Le Canada, pour sa part, souhaite une approche législative uniforme qui pourrait utiliser les lois en vigueur au Québec et en Ontario comme point de départ. Par ailleurs, si le Canada dispose d'un régime national de protection de la vie privée qui repose sur le code de l'OCDE, bien d'autres pays n'ont encore aucune loi à cet effet, ce qui soulève la question de la réciprocité dans les échanges d'information.

Question : Y a-t-il un risque de gain ou de perte pour la population québécoise? À quelles fins faut-il également rechercher une harmonisation internationale en la matière? Qu'en sera-t-il de la réciprocité dans les échanges de renseignements personnels, le cas échéant, et dans quelle mesure les règles en vigueur au Canada et au Québec seront-elles respectées à l'étranger? (enjeu de respect de la vie privée et de confidentialité)

5.2.13 ... sur les dérives possibles

Les dérives possibles d'une offre croissante de systèmes biométriques sur le marché ne sont pas négligeables. De tels systèmes sont déjà offerts et utilisés par différents niveaux de gouvernement tout comme par l'entreprise privée. Outre des objectifs de protection contre le terrorisme et contre la criminalité, leur utilisation pourra répondre à toutes sortes de finalités, plus ou moins légitimes, dont la surveillance au travail ou dans les maisons privées, le contrôle des entrées et des sorties du personnel, l'évaluation de l'état émotionnel de certaines personnes (données reposant sur la chaleur dégagée, par exemple), ou de leur état de santé (ADN, réseaux veineux, rétine, etc.) ne constituent que quelques exemples.

²¹⁶ Méthode de diagnostic fondée sur l'examen de l'iris (Le Robert).

²¹⁷ *Ibid.*, p. 95 et *NewScientist*, "Will DNA profiling fuel prejudice?", Anna GOSLINE, 19 April 2005, p. 13.

Question : À quel point les dérives possibles de l'utilisation de systèmes biométriques par les secteurs public et privé sont-elles prises en considération par la législation actuelle? chaque personne est-elle suffisamment protégée contre les abus possibles que peut entraîner le recours aux données biométriques dans sa vie personnelle et professionnelle. (enjeu de responsabilité morale)

CONCLUSION

Au terme de son état de situation sur les technologies biométriques, sur le contexte qui en sous-tend les applications et sur l'encadrement normatif mis en place pour en contrer les dérives possibles, la Commission de l'éthique de la science et de la technologie a proposé un questionnement éthique sur l'ensemble de la problématique. Ce questionnement, elle l'a orienté sur de nombreux axes : le respect de la démocratie, le renversement du fardeau de la preuve, la validité d'une donnée biométrique, la protection des données personnelles (confidentialité et vie privée), le stockage et la gestion des données, la discrimination, le manque de transparence (le consentement), le respect des finalités, la proportionnalité des moyens, l'instrumentalisation du corps humain, les effets sur la santé, l'encadrement normatif, les dérives possibles.

Les questions que la Commission se pose à la suite de la préparation de ce document de réflexion pourraient en fait se résumer de la façon suivante : *Dans le but d'assurer la sécurité internationale et nationale, notamment au moyen de l'utilisation des données biométriques, les fondements de la démocratie et les droits des citoyens sont-ils encore respectés? L'objectif de sécurité représente-t-il une situation où la fin justifie les moyens?*

Avant de proposer aux décideurs publics et institutionnels un avis et des recommandations sur le sujet, la Commission soumet le présent document de réflexion au débat public. Elle souhaite entendre les points de vue d'experts de divers horizons disciplinaires et de spécialistes de l'éthique sur le questionnement qu'elle a soulevé. Mais elle souhaite également entendre ce qu'en pense la population, dans le cadre d'un forum public qui lui permettra de recueillir des réactions à son questionnement afin d'alimenter sa réflexion dans la préparation d'un avis sur les enjeux éthiques de la technologie biométrique qui soit bien ancré dans la réalité sociale et citoyenne.

BIBLIOGRAPHIE²¹⁸

➤ Textes cités en référence :

AGENCE DES SERVICES FRONTALIERS DU CANADA, « CANPASS Air », Document d'information [en ligne] octobre 2004 [<http://www.asfc.gc.ca/travel/canpass/canpassair-f.html>].

ALBERTS, David S. et Richard E. HAYES, *Power to the Edge : Command and Control in the Information Age*, Command and Control Research Program, Washington D.C., 2003.

ARQUILLA, John et David RONDFELT, *Networks and Netwars : The Future of Terror, Crime and Militancy*, Washington, Editions RAND National Defense Research Institute, 2001.

BBC NEWS, "Concern over biometric passports", [en ligne] 30 March 2004 [<http://news.bbc.co.uk/2/hi/technology/3582461.stm>]

BECK, Ulrich, *La société du risque : sur la voie d'une autre modernité*, Paris, Flammarion, Collection Champs, no 546, 2001 (1986).

BRONSKILL, Jim, « De nouveaux passeports avec des données biométriques », *Le Devoir*, 19 juillet 2004.

BUREAU DU VÉRIFICATEUR GÉNÉRAL DU CANADA, Communiqué, Ottawa, 15 février 2005.

BUREAU DU VÉRIFICATEUR GÉNÉRAL DU CANADA, *Le Point*, Ottawa, février 2005.

BUREAU DU VÉRIFICATEUR GÉNÉRAL DU CANADA, *Rapport de la vérificatrice générale du Canada à la Chambre des communes*, Ottawa, mars 2004.

BUZAN, Barry, Ole WEAVER et Jaap de WILDE, *Security: A New Framework For Analysis*, Londres, Lynne Rienner Publishers, 1998.

CANOË, « Élève ou bétail ? » [en ligne] 11 février 2005 [<http://www2.canoe.com/techno/nouvelles/archives/2005/02/20050211-105834.html>] [page consultée le 14 février 2005]

CHALIAND, Gérard et Arnaud BLIN, *Histoire du terrorisme : de l'Antiquité à Al Qaida*, Paris, Bayard, 2004.

CITOYENNETÉ ET IMMIGRATION CANADA, *Biométrie : incidences et applications pour la citoyenneté et l'immigration*, Actes, Forum des politiques publiques, Ottawa, 7 et 8 octobre 2003.

CITOYENNETÉ ET IMMIGRATION CANADA, *Biométrie : incidences et applications pour la citoyenneté et l'immigration*, Document d'information, Forum des politiques publiques, Ottawa, 7 et 8 octobre 2003.

CITOYENNETÉ ET IMMIGRATION CANADA, « Sécurité publique et antiterrorisme », Rapport final, septembre 2003 [en ligne] [<http://www.cic.gc.ca/francais/recherche-stats/evaluation/securite-publique.html>]

CLARKE, Roger, "Biometrics and Privacy", Australian National University, 15 April 2001 [en ligne] [<http://www.anu.edu.au/people/Roger.Clarke/DV/Biometrics.html>]

COLIN, Perkel, « La guerre contre le terrorisme a rendu Al-Qaïda plus dangereux, dit un agent du SCRS », *Le Devoir*, 15 mars 2005.

COMITÉ SÉNATORIAL PERMANENT DE LA SÉCURITÉ NATIONALE ET DE LA DÉFENSE, « Les urgences nationales : Le Canada, fragile en première ligne. Stratégie de renforcement », Volume 1, [en ligne] mars 2004, [<http://www.parl.gc.ca/37/3/parlbus/commbus/senate/com-f/defe-f/rep-f/rep03vol1-f.htm>]

²¹⁸ Sauf quand il est fait mention de la date de consultation, toutes les adresses Internet étaient accessibles le 20 mai 2005, soit directement, soit par le biais des archives de certains sites.

COMITÉ SÉNATORIAL PERMANENT DE LA SÉCURITÉ NATIONALE ET DE LA DÉFENSE, « Les côtes du Canada : Les plus longues frontières mal défendues au monde », 28 octobre 2003, « Cauchemars pour le nouveau millénaire » [en ligne] [<http://www.parl.gc.ca/37/2/parlbus/commbus/senate/com-defe-f/rep-f/rep17oct03-f.htm>]

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Communication transfrontalière de renseignements sur les Canadiens et les Canadiennes – Répercussions de la *USA Patriot ACT* », Mémoire présenté au Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, Jennifer Stoddart, Commissaire à la protection de la vie privée du Canada [en ligne] 18 août 2004 [http://www.privcom.gc.ca/media/nr-c/2004/sub_usapa_040818_f.pdf]

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « Le vol d'identité : qu'est-ce que c'est, et quoi faire », Fiches d'information [en ligne] non daté [http://www.privcom.gc.ca/fs-fi/02_05_d_10_f.asp]

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Rapport final d'enquête concernant l'installation de caméras de SURVEILLANCE par le Service de police de la Ville de Montréal*, [en ligne] février 2005 [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/Robot_Cam_rapportfinal.pdf]

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, [en ligne] juin 2004 [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/nouvelles_regles_2004.pdf]

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Consultation publique. L'utilisation de caméras de surveillance par des organismes publics dans les lieux publics », Sommaire du bilan de la consultation publique [en ligne] juin 2004, [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/sommaire_bilan.pdf]

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Consultation publique. L'utilisation de caméras de surveillance par des organismes publics dans les lieux publics », Document de présentation [en ligne] mai 2003, [http://www.cai.gouv.qc.ca/05_communiques_et_discours/01_pdf/cons_cam.pdf]

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Une réforme de l'accès à l'information : le choix de la transparence*, Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dans le secteur privé, [en ligne] novembre 2002, [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/quin.pdf]

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec : Les enjeux*, Document d'analyse, préparé par Max CHASSÉ, analyste en informatique, Gouvernement du Québec [en ligne] juillet 2002 [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_enj.pdf]

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La biométrie au Québec : Les principes d'application pour un choix éclairé*, Gouvernement du Québec [en ligne] juillet 2002 [http://www.cai.gouv.qc.ca/06_documentation/01_pdf/biom_appl.pdf]

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *Le don et la transplantation d'organes : dilemmes éthiques en contexte de pénurie*, Gouvernement du Québec [en ligne] novembre 2004 [<http://www.ethique.gouv.qc.ca/fr/publications.html>]

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *Pour une gestion éthique des OGM*, Gouvernement du Québec [en ligne] décembre 2003 [<http://www.ethique.gouv.qc.ca/fr/publications.html>]

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *Les enjeux éthiques des banques d'information génétique : pour un encadrement démocratique et responsable*, Gouvernement du Québec [en ligne] février 2003 [<http://www.ethique.gouv.qc.ca/fr/publications.html>]

COMMISSION EUROPÉENNE, « Document de travail sur la biométrie », Groupe de travail 'article 29' sur la protection des données, 12168/02/fr, GT 80, [en ligne] 1^{er} août 2003 [http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_fr.pdf]

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS – CNIL (France), 25^e *Rapport d'Activité 2004*, France.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS – CNIL (France), « La cybersurveillance sur les lieux de travail » [en ligne] 2004 [<http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf>]

COMMUNAUTÉ EUROPÉENNE, « Déclaration sur la lutte contre le terrorisme », Bruxelles [en ligne] 25 mars 2004 [http://ue.eu.int/ueDocs/cms_Data/docs/pressdata/fr/ec/79639.pdf]

DANIELS, Ronald J., Patrick MARCLEM and Kent ROACH (Ed.), *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*, Canada, University of Toronto Press, 2001.

DAVID, Charles-Philippe, *La guerre et la paix : approches contemporaines de la sécurité et de la stratégie*, Paris, Presses de science po, 2000.

DELUMEAU, Jean, *La peur en Occident (XIV^e-XVIII^e siècle)*, Paris, Fayard 1978, Pluriel 1979.

DELUMEAU, Jean, *Rassurer et protéger. Le sentiment de sécurité dans l'Occident d'autrefois*, Paris, Fayard 1989.

DIONNE, Bernard, « La biométrie : Avantages, inconvénients et impacts sur la vie privée des citoyens », Conférence, Congrès 2003 de l'Association sur l'accès et la protection de l'information (AAPI) : L'Administration électronique et la mise en réseau de l'information : Enjeux et défis, 8 mai 2003.

DIONNE, Bernard et Èvelyne RACETTE, « La biométrie : présentation à la Commission de l'éthique de la science et de la technologie », mars 2004 (manuscrit).

DIXON, Thomas Homer, "The Rise of Complex Terrorism", *Foreign Policy*, January-February 2002.

DUMOUT, Estelle, « Passeports : visage et empreintes numériques imposés par le Conseil de l'UE », *ZDNet France* [en ligne] 27 octobre 2004 [<http://www.zdnet.fr/actualites/informatique/0.39040745.39179891.00.htm>]

DUPONT, Thierry, « À Angers, c'est biométrie tous les jours à la cantine des écoles cathos » [en ligne] 9 septembre 2003 [<http://www.transfert.net/a9255>]

GEIST, Michael A., "Computer and e-mail workplace surveillance in Canada: the shift from reasonable expectation of privacy to reasonable surveillance", *The Canadian Bar Review/La Revue du Barreau canadien*, vol. 82, no 2, août 2003.

GEREMEK, Bronislaw, « Le marginal », dans Jacques LE GOFF, *L'homme médiéval*, Paris, Seuil, Histoire, 1983.

GOSLINE, Anna, "Will DNA profiling fuel prejudice?", *NewScientist*, 19 April 2005.

GOUVERNEMENT DU CANADA, *Budget 2004*, Ministère des Finances, Canada, mars 2004.

GOUVERNEMENT DU CANADA, « Les amendements au projet de loi C-36 », Bureau du Conseil privé [en ligne] 20 novembre 2001 [http://canada.justice.gc.ca/fr/news/nr/2001/doc_27902.html].

GROSSMAN, David, *Le Temps*, Genève, repris dans *Le Courrier international*, no 570, [en ligne] 4 octobre 2001 [http://www.courrierinternational.com/article.asp?obj_id=12618&provenance=zop.archives] [page consultée le 17 mars 2004]

HEERS, Jacques, *La ville au Moyen-Âge*, Paris, Fayard 1990, Pluriel Histoire.

HOFFMAN, Bruce, *Inside Terrorism*, New York, Columbia University Press, 1998.

HUGGINS, Charnicia E., « States consider allowing cameras in nursing homes », *Elder Law Journal*, 23 August 2004, reproduit dans *MedicineNet.com* [en ligne] [<http://www.medicinenet.com/script/main/art.asp?articlekey=38589&pf=3&track=gpa385>]

IJJ@ L'ŒUVRE, Numéro spécial sur la biométrie, été 2004.

INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS), *Biometrics at the Frontiers : Assessing the Impact on Society*, For the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Technical Report Series, EUR21585EN, 2005.

INSTITUTE FOR PROSPECTIVE TECHNOLOGICAL STUDIES (IPTS), *Sécurité et respect de la vie privée du citoyen à l'ère du numérique après le 11 septembre : Vision prospective*, Document de synthèse, version française, Commission européenne, Directorate-General, Joint Research Centre, juillet 2003.

KANELLOS, Michael, "Human chips more than skin-deep", *Cnet New.com* [en ligne] 23 August 2004 [http://news.com.com/Human+chips+more+than+skin-deep/2009-7337_3-5318076.html]

LAQUEUR, Walter, *A History of Terrorism*, New Jersey, Transaction Publisher, 2002.

LAQUEUR, Walter, *The New Terrorism: Fanaticism and the Arms of Mass Destruction*, Oxford, Oxford University Press, 1999.

LE GOFF, Jacques, *L'homme médiéval*, Paris, Seuil, Histoire, 1983.

LE NOUVEL OBSERVATEUR, « Récidive : le Sénat rejette le bracelet » [en ligne] 10 février 2005 [<http://archquo.nouvelobs.com/cgi/articles?ad=politique/20050210.OBS8446.html&datebase=20050210>]

LE NOUVEL OBSERVATEUR, « Consensus à Bruxelles sur un 'Monsieur Terrorisme' », [en ligne] 19 mars 2004 [http://permanent.nouvelobs.com/cgi/edition/qobs_imprime?cle=20040319.OBS6161] [page consultée le 22 mars 2004]

LÉGARÉ, François, *Terrorisme : Peurs et réalités*, Outremont (Québec), Athéna, 2002.

LEGAULT, Albert, *La lutte antiterroriste ou la tentation démocratique autoritaire*, Québec, Les Presses de l'Université Laval, 2002.

LONDON SCHOOL OF ECONOMICS & POLITICAL SCIENCE, *The Identity Project. An assessment of the UK Identity Cards Bill & its implications*, Interim Report, Project Management by enterprise privacy group, Department of Information Systems, March 2005.

MACLEOD, Alex, Evelyne DUFAULT et F. Guillaume DUFOUR (dir.), *Relations internationales : théories et concepts*, Montréal, Athéna éditions, 2004.

MANONNI, Pierre, *Les logiques du terrorisme*, Paris, In Press, 2004.

MASSON, Isabelle, « Sécurité », dans MACLEOD, DUFAULT et DUFOUR (dir.), 2004.

MINISTÈRE DE LA SÉCURITÉ PUBLIQUE, *La sécurité privée partenaire de la sécurité intérieure*, Livre blanc, Gouvernement du Québec, décembre 2003.

MUMFORD, Lewis, *La cité à travers l'histoire*, Paris, Seuil, 1964 (1961).

NAUDIN, Christophe, *ALIAS. Le nouvel empire des crimes d'identité*, Paris, La Table Ronde, 2005.

NEWMAN, Cathy, "A Life Revealed", *National Geographic*, Special Report, April 2002.

NORRIS, Pipa, Montague KERN et Marion JUST (ed.), *Framing Terrorism: The News Media, the Government, and the Public*, New York, Routledge, 2003.

NORTON-TAYLOR, "Thinktank : invasion aided Al-Qaida", *The Guardian* [en ligne] 20 October 2004 [<http://www.guardian.co.uk/Iraq/Story/0,2763,1331362,00.html>]

OFFICE PARLEMENTAIRE D'ÉVALUATION DES CHOIX SCIENTIFIQUES ET TECHNOLOGIQUES (France), *Les méthodes scientifiques d'identification des personnes à partir de données biométriques et les techniques de mise en œuvre*, Rapport présenté au Sénat par Christian CABAL, député, Assemblée nationale, juin 2003.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT – OECD, *Biometric-Based Technologies*, Working Party on Information Security and Privacy, Directorate for Science,

Technology and Industry, Committee for Information, Computer and Communications Policy, Paris, 28 April 2004.

PAPINEAU, Jean-Marc, « Biométrie dernier cri », Dossier informatique, *Plan*, la revue de l'Ordre des Ingénieurs du Québec, octobre 2004.

RADIO-CANADA, « Biométrie : sécurité ou menace », journaliste et réalisateur Normand GRONDIN, Émission *Découverte* [en ligne] 14 septembre 2003 [http://www.radio-Canada.ca/actualite/decouverte/reportages/2003/09-2003/14_biometrie.html]

RICARD, Philippe, « L'Amérique dicte sa loi antiterroriste au trafic aérien avec l'Europe », *Le Monde.fr* [en ligne] 21 juin 2004 [<http://www.lemonde.fr/web/article/0,1-0@2-3222,36-369798,0.html>]

ROGER, Patrick, « Récidive : la gauche s'oppose au bracelet électronique », *Le Monde.fr* [en ligne] 15 décembre 2004 [http://www.lemonde.fr/web/imprimer_article/0,1-0@2-3224,36-390997,0.html] [page consultée le 15 décembre 2004]

RUFFIÉ, Jacques, *De la biologie à la culture*, Paris, Flammarion, Collection Champs, no 128, 1983.

SCHMID, Alex P., Albert J. JONGMAN ET AL, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories and Literature*, New Brunswick, Transaction Books, 1988.

SCHREIDER, Eugène, dans *Encyclopaedia Universalis*, article sur la biométrie.

SENDER, Eléna, « Biométrie. Des données physiques stockées sur une puce. Le corps pour tout passeport », *Sciences et avenir*, septembre 2004.

SOLLICITEUR GÉNÉRAL DU CANADA, *Avis public aux consommateurs : Rapport spécial sur le VOL d'identité* [en ligne] 21 mai 2003 [http://www.psepc-sppcc.gc.ca/publications/policing/pdf/identity_theft_consumers_f.pdf]

STODDART, Jennifer, « Des technologies de surveillance sous surveillance », discours [en ligne] septembre 2001 [http://www.cai.gouv.qc.ca/05_communiques_et_discours/discours_24_09_01.html]

THORAVAL, Armelle, « La prison GPS testée en Grande-Bretagne », *Libération.fr* [en ligne] 17 décembre 2004 [<http://www.liberation.fr/imprimer.php?Article=262328>]

WIKIPEDIA, « Pyramide des besoins » [en ligne] [http://fr.wikipedia.org/wiki/Pyramide_des_besoins]

WOODWARD, John D., "Biometrics: Privacy's Foe or Privacy's Friend", *Proceedings of the IEEE*, vol. 85, n° 9, September 1997 .

Autres textes consultés :

ACKLESON, Jason, "Securing Through Technology? 'Smart Borders' after September 11th", *Knowledge, Technology, & Policy*, Spring 2003, Vol. 16, No 1.

AGRE, Philip E., "Your Face Is Not a Bar Code : Arguments Against Automatic Face Recognition in Public Places", University of California [en ligne] 10 September 2003 [<http://polaris.gseis.ucla.edu/pagre/bar-code.html>]

ALIBECK Ken (avec la collaboration de Stephen Handelman), *La Guerre des Germes*, Paris, Libre Expression, 2000.

AMNESTY INTERNATIONAL, *Rapport 2004 d'Amnesty International* [en ligne] [<http://web.amnesty.org/web/web.nsf/print/2004-index-fra>]

ANDERSON, Alison, "Risk, Terrorism, and the Internet", *Knowledge, Technology, & Policy*, Summer 20, Vol. 16, No. 2, 2003.

ANÉ, Claire, « Passeport et liberté d'expression », *Le Monde* [en ligne] 30 août 2004 [http://www.lemonde.fr/web/imprimer_article/0,1-0@2-3266,36-377093,0.html] [page consultée le 30 août 2004]

ASSEMBLÉE NATIONALE (France), *Rapport d'information déposé par la délégation de l'Assemblée nationale pour l'Union Européenne sur L'Union européenne et la lutte contre le terrorisme*, présenté par Christian PHILIP, député, 2 mars 2005.

ASSEMBLÉE NATIONALE (France), *Rapport d'information déposé en application de l'article 145 du Règlement par la Commission des Affaires étrangères en conclusion des travaux d'une mission d'information sur la coopération internationale pour lutter contre le terrorisme*, présenté par Michel DELEBARRE, député, 6 juillet 2004.

BARCELO, Yan, « La biodéfense crée des occasions d'affaires alléchantes », *Les Affaires*, 17 avril 2004.

BIOMETRICS INSTITUTE, "Biometrics and Privacy", paper presented at the 1st Biometrics Institute Conference by Malcolm CROMPTON, Australia's third Federal Privacy Commissioner [en ligne] 2003 [<http://www.biomet.org/bi/cromptonspeech1.htm>]

BLANC, Gérard, « La biométrie, un outil qui fonctionne au doigt et à l'œil », *Gestion, Direction informatique*, mai 2004.

BOBBITT, Philip, "Being Clear About Present Dangers", *The New York Times* [en ligne] 11 August 2004 [<http://www.nytimes.com/2004/08/11/opinion/11bobbitt.html>]

BOILEAU, Josée, « L'œil fatal », *Le Devoir*, 14 octobre 2003.

BRONSKILL, Jim, « Le Bureau des passeports veut utiliser la reconnaissance faciale », *Le Devoir*, 30 août 2004.

BRZEZINSKI, Zbigniew, « L'hégémonie américaine face à la terreur », *Le Nouvel Observateur* [en ligne] semaine du jeudi 25 mars 2004, n° 2055 – Réflexions [<http://www.nouvelobs.com/articles/p2055/a235983.html>] [page consultée le 25 mars 2004]

CAMP, L. Jean, "Digital Identity", *IEEE Technology and Society Magazine*, Fall 2004.

CASONI, Dianne et Louis BRUNET (sous la direction de), *Comprendre l'acte terroriste*, Québec, Presses de l'Université du Québec, 2003.

CHANG, Kenneth, "Buy a Golf Club, Build a Bomb", *The New York Times* [en ligne] 14 March 2004 [<http://nytimes.com/2004/03/14/weekinreview/14chang.html>]

CHULOV, Martin and Rory CALLINAN, "Plot to bomb power grid", *The Australian* [en ligne] 23 April 2004 [<http://www.theaustralian.news.com.au/printpage/0,5942,9362265,00.html>] [page consultée le 26 avril 2004]

CITOYENNETÉ ET IMMIGRATION CANADA, *Biométrie : incidences et applications pour la citoyenneté et l'immigration*, « Au sujet de la biométrie. Questions et réponses sur la biométrie » [en ligne] non daté [http://www.ppt.gc.ca/faq/index_f.asp#700]

CITOYENNETÉ ET IMMIGRATION CANADA, « Lancement d'un débat au Canada sur des cartes d'identité plus sécuritaires et sur la biométrie », Opinion de l'honorable Denis Coderre, ministre de la Citoyenneté et de l'Immigration, gouvernement du Canada [en ligne] 7 octobre 2003 [<http://www.cic.gc.ca/francais/nouvelles/03/0338-f.html>]

CLARKE, Richard A., "The Wrong Debate on Terrorism", *The New York Times* [en ligne] 25 April 2004 [<http://www.nytimes.com/2004/04/25/opinion/25CLAR.html>]

CLARKE, Roger, "Biometrics' Inadequacies and Threats, and the Need for Regulation", Australian National University, [en ligne] 15 April 2002 [<http://www.anu.edu.au/people/Roger.Clarke/DV/BiomThreats.html>]

CODERRE, Denis, « L'amélioration de nos documents d'identité mérite un débat immédiat et sérieux », *Le Soleil*, 8 octobre 2003.

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics », juin 2004.

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Consultation publique. L'utilisation de caméras de surveillance par des organismes publics dans les lieux publics », Sommaire du bilan de la consultation publique, juin 2004.

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Consultation publique. L'utilisation de caméras de surveillance par des organismes publics dans les lieux publics », Résumés des mémoires, novembre 2003.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS – CNIL (France), « Le nouveau passeport européen avec biométries et puces sans contact : un enjeu de taille pour la protection des données personnelles » [en ligne] 29 novembre 2004 [<http://www.cnil.fr/index.php?id=1719>]

CONSEIL DE L'EUROPE, *Les droits de l'homme et la lutte contre le terrorisme. Les lignes directrices du Conseil de l'Europe*, Strasbourg, Éditions du Conseil de l'Europe, mars 2005.

COPELAND, Larry, "Domestic terrorism : New trouble at home", *USA Today* [en ligne] 14 November 2003 [http://www.usatoday.com/news/nation/2004-11-14-domestic-terrorism_x.htm]

CORDIS, "Resolving the identity question electronically", Commission européenne, [en ligne] 5 June 2003 [<http://istresults.cordis.lu/index.cfm/section/news/Tpl/article/BrowsingType/Long%20Feature/ID/941>]

COT, Bruno D., «La biométrie. L'antidote high-tech au terrorisme », *L'express.fr* [en ligne] 22 novembre 2001 [<http://www.lexpress.fr/express/formatimp/imprime.asp?idarticle=289129&ref>] [page consultée le 17 mars 2004]

COUGHLAN, Sean, "Security under the skin", *BBC News* [en ligne] 15 October 2004 [<http://news.bbc.co.uk/1/hi/magazine/3742684.stm>]

COURMONT, Barthélémy, *Terrorisme et contre-terrorisme*, Document, Paris, Le cherche midi, 2003.

COURTOIS, Stéphane (sous la direction de), *Enjeux philosophiques de la guerre, de la paix et du terrorisme*, Québec, Les Presses de l'Université Laval, 2003.

COWELL, Alan, "Citing Terror Issues, Britain Plans ID Cards", *The New York Times* [en ligne] 24 November 2004 [<http://www.nytimes.com/2004/11/24/international/europe/24britain.html>]

CROWLEY, Matthew, "Identification technology raises privacy concerns", *Las Vegas Review-Journal* [en ligne] 21 March 1999 [http://www.reviewjournal.com/lvj_home/1999/Mar-21-Sun-1999/business/10800971.html]

D'AMOURS, Liette, « Création d'un institut québécois de la sécurité de l'information », *La Presse*, 23 septembre 2003.

DALPHOND-GUIRAL, Madeleine, «Le droit à la vie privée n'est pas un privilège », *Le Soleil*, 8 octobre 2003.

DELIO, Michelle, "Who's Winning Privacy Tug of War?", *Wired News* [en ligne] 17 March 2003 [<http://www.wired.com/news/privacy/0,1848,58064,00.html>]

DE PIERREBOURG, Fabrice, «Fraudes avec les cartes de débit : la technologie actuelle tire à sa fin », *Journal de Montréal* dans *Canoë* [en ligne] 18 novembre 2004 [<http://www2.infinit.com/cgi-bin/imprimer.cgi?id=156712>]

DIRECTION INFORMATIQUE, « Ottawa questionne l'identification biométrique », *Presse canadienne*, février 2005.

DUPUY, Jean-Pierre, *Pour un catastrophisme éclairé. Quand l'impossible est certain*, Paris, Seuil, La couleur des idées, 2002.

ELSEVIER B.D., « La variole : une maladie du passé ou une arme de demain? – Ce tueur qu'on croyait éliminé pourrait-il revenir comme arme de destruction massive? » [en ligne] 29 octobre 2004 [http://www.guidesanteenligne.com/imprimer_nouvelle.asp?ID=28629]

FEDER, Barnaby J. and Tom ZELLER Jr., "Identity Badge Worn Under Skin Approved for Use in Health Care", *The New York Times* [en ligne] 14 October 2004 [<http://www.healthanddiets.com/article116.html>]

FOUCART, Stéphane, « Le fichage des empreintes de tous les Français est envisagé », *Le Monde.fr* [en ligne] 17 décembre 2003 [http://www.lemonde.fr/web/imprimer_article/0,1-0@2-3244,36-346327,0.html] [page consultée le 25 janvier 2004]

GOUVERNEMENT DU CANADA, *Protéger une société ouverte : la politique canadienne de sécurité nationale*, Bureau du Conseil privé [en ligne] avril 2004 [http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_f.pdf]

GOUVERNEMENT DU CANADA, *Sécurité accrue*, Rapport annuel 2002-2003, Bureau des passeports (non daté).

GRAHAM-ROWE, Duncan, "Secure signature means no one can steal your ID", *NewScientist*, 22 May 2004.

GRAHAM-ROWE, Duncan, "New biometric approach secures ID cards", *NewScientist.com* [en ligne] 19 May 2004 [<http://www.newscientist.com/news/news.jsp?id=ns99995010>]

HALL, Mimi, "Visitor screening program expands", *USA Today* [en ligne] 14 November 2004 [http://www.usatoday.com/news/washington/2004-11-14-visitor-screening_x.htm]

JACQUÉ, Philippe, « Big Brother, es-tu là ? », *Courrier international*, 13 janvier 2004 [en ligne] http://www.courrierinternational.com/numeros/688/13122004_multimedia.asp (page consultée le 19 janvier 2004).

JOHNSTON, David and David. E. SANGER, "New Generation of Leaders is Emerging for Al Qaeda", *The New York Times* [en ligne] 10 August 2004 [<http://www.nytimes.com/2004/08/10/politics/10terror.html?ex=1116993600&en=b4d7bf5ca5752beb&ei=5070>]

KINZER, Stephen, "Chicago Moving to 'Smart' Surveillance Cameras", *The New York Times* [en ligne] 21 September 2004 [<http://www.nytimes.com/2004/09/21/national/21cameras.html>]

KINZER, Stephen and Todd S. PURDUM, "An American Debate: How Severe the Threat?", *The New York Times* [en ligne] 5 August 2004 [<http://www.nytimes.com/2004/08/05/politics/05react.html?ex=1116993600&en=0a0783479b1aa4be&ei=5070&th>]

KORNBLUM, Janet, "Prying eyes are everywhere", *USAToday.com*, [en ligne] 13 April 2005 [http://www.usatoday.com/tech/news/2005-04-13-spyware_x.htm]

LABAN, James, "Privacy Issues Surrounding Personal Identification Systems" [en ligne] April 1996 [<http://www.dss.state.ct.us/pubs/diprivac.pdf>]

LACOMBE, Réjean, « Le bioterrorisme demeure une possibilité réelle », *Le Soleil*, 14 juillet 2004.

LANGELLIER, Jean-Pierre, « Les plus hauts magistrats britanniques condamnent la loi antiterroriste », *Le Monde.fr* [en ligne] 17 décembre 2004 [http://www.lemonde.fr/web/imprimer_article/0,1-0@2-3214,36-391283,0.html] [page consultée le 20 décembre 2004]

LA PRESSE, « La sécurité prime la vie privée », tiré de *The New YorkTimes*, 17 avril 2004.

LEDUC, Louise, « La carte d'identité nationale ouvre la porte aux abus », *La Presse*, 29 octobre 2003.

LE JOURNAL DE QUÉBEC, « Ottawa envisage de prendre les empreintes des visiteurs », *Presse canadienne*, 6 septembre 2004.

LE JOURNAL DE QUÉBEC, « Selon Manley, l'utilisation de données biométriques peut poser problème », *Presse canadienne*, 16 septembre 2003.

LE MONDE.FR, « 'Le danger existe' de voir la Grande-Bretagne devenir 'une société sous surveillance', avec l'Agence France Presse [en ligne] 16 août 2004 [http://www.bethel-fr.com/afficher_info.php?id=11026.9]

LE NOUVEL OBSERVATEUR, « Libertés : le cri d'alarme de la Cnil », propos recueillis par Stéphane Arteta [en ligne] 4 janvier 2005 [<http://archquo.nouvelobs.com/cgi/articles?ad=multimedia/20050104.OBS5314.html&host=>]

LE SOLEIL, « Le Manitoba abandonne un projet de permis de conduire 'biométrique' », La Presse canadienne, 12 janvier 2004.

LE SOLEIL, « Consignes pour les passeports. Des craintes de violation de la vie privée font surface », La Presse canadienne, 2 septembre 2003.

McNAMARA, Kate, "New privacy law a Pandora's box", *The National Post*, 7 April 2004.

MEISSNER, Dirk, « Les Canadiens ne sont pas à l'abri du Patriot Act », *Le Soleil*, Presse canadienne, 30 octobre 2004.

MINISTÈRE DE LA FONCTION PUBLIQUE (France), *Administration électronique et protection des données personnelles*, Livre blanc, Pierre TRUCHE, Jean-Paul FAUGÈRE et Patrice FLICHY [en ligne] février 2002 [<http://lesrapports.ladocumentationfrancaise.fr/BRP/024000100/0000.pdf>]

MOORE, Lynn, "You're just a number. New technology is tracking you in ways that may be a surprise", *The Gazette*, 20 June 2004.

NORMAND, François, « Les mesures de sécurité à la frontière se renforceront », *Les Affaires*, 13 novembre 2004.

NORTON, Amy, "DNA Databases : The New Dragnet", *The Scientist*, 11 April 2005.

O'BRIEN, Timothy L., "Identity Theft is Epidemic. Can It Be Stopped?", *The New York Times* [en ligne] 24 October 2004 [<http://www.nytimes.com/2004/10/24/business/yourmoney/24theft.html?ex=1116993600&en=f2619f32dca788cc&ei=5070>]

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUE (OCDE), *Inscrire la coopération pour le développement dans une optique de prévention du terrorisme. Principaux point d'ancrage pour l'action*, Les lignes directrices et ouvrages de référence du Comité d'aide au développement (CAD), Paris, 2003.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD), *Security System Reform and Governance: Police and Good Practice*, Paris, May 2004.

PACIENZA, Angela, « La surveillance des courriels des employés est de plus en plus courante », *Canoe* [en ligne] 17 mars 2005 [<http://www2.infinit.com/cgi-bin/imprimer.cgi?id=181911>]

PATENAUDE, Pierre, *L'expertise en preuve pénale, Les sciences et techniques modernes d'enquête, de surveillance et d'identification*, Québec, Les Éditions Yvon Blais, 2003.

PAYNE, Jenna, « L'UE a besoin de plus de temps pour émettre des passeports biométriques », *Associated Press* [en ligne] 20 mars 2005 [<http://www2.canoe.com/techno/nouvelles/archives/2005/03/20050331-082933.html>]

PELOW, Mark, "Biometric passports are a 'tall order'. Experts warn that security systems are too immature for a 2005 start", *News@nature.com* [en ligne] 16 December 2004 [<http://www.nature.com/news/2004/041213/full/041213-12.html>]

PLANTEVIN, Jérôme, « Le Canada n'échappera pas au passeport biométrique », *Les Affaires*, 27 septembre 2003.

PLANTEVIN, Jérôme, « Pas de place pour la biométrie à Montréal », *Les Affaires*, 27 septembre 2003.

PRIVACY INTERNATIONAL, "Privacy and Human Rights. An International Survey of Privacy Laws and Practice", Global Internet Liberty Campaign, [en ligne] non daté [<http://www.gilc.org/privacy/survey/>]

RICARD, Philippe, « Un code couleur pour cibler les passagers 'à risques' », *Le Monde.fr* [en ligne] 21 juin 2004 [http://www.lemonde.fr/web/imprimer_article/0,1-0@2-3222,36-369799,0.html]

ROGEL, Jean-Pierre, « Bioterrorisme : la fin de l'innocence », *L'Observatoire de la génétique* [en ligne] n° 1, février/mars 2002 [http://www.ircm.qc.ca/bioethique/obsngenetique/cadrages/cadr2002/c_no1_02/c_no1_02_1.html]

ROTENBERG, Marc, "Statement", Electronic Privacy Information Center, Before the Special Committee on Aging, United States Senate, 18 July 2002 [en ligne] [http://www.epic.org/privacy/biometrics/testimony_071802.html] (page consultée le 6 janvier 2004).

SCHNEIER, Bruce, *Beyond Fear. Thinking Sensibly About Security in an Uncertain World*, New York, Copernicus Books, 2003.

SCHWARTZ, John, "AOL to Add Spyware Detection to Service", *The New York Times* [en ligne] 6 January 2004 [<http://www.nytimes.com/2004/01/06/technology/06spy.html>] (page consultée le 9 janvier 2004).

SCHWARTZ, John and Micheline MAYNARD, "F.B.I. Got Records on Air Travelers", *The New York Times* [en ligne] 1 May 2004 [<http://www.nytimes.com/2004/05/01/politics/01AIRL.html>]

SCIOLINO, Elaine, "World Opinion Is Fragmented on Tighter Security for Visitors", *The New York Times* [en ligne] 7 January 2004 [<http://www.nytimes.com/2004/01/07/international/07TRAV.html>]

SECURITEINFO.COM, « La biométrie », [en ligne] non daté [<http://www.securiteinfo.com/conseils/biometrie.shtml>]

SHENK, David, "The world of High-tech surveillance", *National Geographic*, November 2003.

SMOLAR, Piotr, « Les passeports biométriques devraient être disponibles dans deux ans », *Le Monde.fr* [en ligne] 28 septembre 2004 [http://www.lemonde.fr/web/recherche_resumedoc/1,13-0,37-870217,0.html?message=redirection_article] [page consultée le 28 septembre 2004]

SMOLAR, Piotr, « La Commission de l'informatique et des libertés face aux exigences sécuritaires », *Le Monde.fr* [en ligne] 22 juin 2004 [http://www.lemonde.fr/web/imprimer_article/0,1-0@2-3226,36-369975,0.html] [page consultée le 22 juin 2004]

SMOLAR, Piotr, « Les convertis à l'islam radical, une minorité croissante d'activistes », *Le Monde.fr* [en ligne] 3 juin 2004 [<http://www.lemonde.fr/web/article/0,1-0@2-3226,36-367343,0.html>] [page consultée le 3 juin 2004]

STROOBANTS, Jean-Pierre, « Les polices occidentales découvrent les nouvelles formes d'Al-Qaida », *Le Monde.fr* [en ligne] 20 août 2004 [http://www.lemonde.fr/web/recherche_resumedoc/1,13-0,37-865130,0.html?message=redirection_article] [page consultée le 23 août 2004]

SWARNS, Rachel L., "U.N. Report Cites Harassment at American Airports of Asylum Seekers", *The New York Times* [en ligne] 13 August 2004 [<http://www.nytimes.com/2004/08/13/national/13immig.html>]

SWARNS, Rachel L., "Millions More Travelers to U.S. to Face Fingerprints and Photos", *The New York Times* [en ligne] 3 April 2004 [<http://www.nytimes.com/2004/04/03/politics/03TRAV.html?th>]

SWARTZ, Jon, "Terrorists' use of Internet spreads", *USA Today* [en ligne] 20 February 2005 [http://www.usatoday.com/money/industries/technology/2005-02-20-cyber-terror-usat_x.htm]

TALEB, Nassim Nicholas, "Learning to Expect the Unexpected", *The New York Times* [en ligne] 8 April 2004 [<http://nytimes.com/2004/04/08/opinion/08TALE.html>]

THE NEW YORK TIMES, "Paying the Price for Safety", Jim Hall [en ligne] 23 February 2005 [<http://www.nytimes.com/2005/02/23/opinion/23hall.html>]

THE NEW YORK TIMES, "Intelligence and Civil Rights", [en ligne] 11 December 2004 [<http://www.nytimes.com/2004/12/11/opinion/11sat1.html>]

THE NEW YORK TIMES, "A National ID" [en ligne] 31 May 2004 [<http://www.nytimes.com/2004/05/31/opinions/31MON1.html>]

TOMKO, George, "Biometrics as a Privacy-Enhancing Technology: Friend or Foe of Privacy?", Photonics Research Ontario, paper presented at the Privacy Laws & Business 9th Privacy Commissioners'/Data Protection Authorities Workshop, Spain [en ligne] 15 September 1998 [<http://www.dss.state.ct.us/digital/tomko.htm>]

UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE – GAO, *Aviation Security. Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed*, Report to Congressional Committees, GAO-05-356 [en ligne] March 2005 [<http://www.gao.gov/cgi-bin/getrpt?GAO-05-356>]

USA TODAY, "Police say cameras will help them monitor Dallas neighbourhood", Associated Press [en ligne] 30 December 2004 [http://www.usatoday.com/tech/news/surveillance/2004-12-30-surveilling-deep-ellum_x.htm]

WALD, Matthew L., "U.S. Wants All Air Traveler Files for Security Test", *The New York Times* [en ligne] 22 September 2004 [<http://www.nytimes.com/2004/09/22/politics/22secure.html>]

ZECCHINI, Laurent, « 35 données personnelles des passagers aériens seront transmises aux douanes américaines », *Le Monde.fr*, 18 décembre 2003 [en ligne] [http://www.lemonde.fr/web/recherchesumedoc/1,13-0,37-832394,0.html?message=redirection_article] [page consultée le 5 janvier 2004]

ANNEXE 1

PROFIL DES PRINCIPALES DONNÉES BIOMÉTRIQUES²¹⁹

Biométrie	Avantages	Inconvénients	Applications
Empreintes digitales	▪ technologie la plus éprouvée techniquement et la plus connue du grand public ▪ petite taille du lecteur facilitant son intégration dans la majorité des applications (téléphones cellulaires, PC) ▪ faible coût des lecteurs ▪ traitement rapide ▪ bon compromis entre les faux rejets et les fausses acceptations	▪ image « policière » ▪ difficulté de lecture avec des doigts sales ou abîmés ▪ besoin de la coopération de la personne concernée (pose correcte du doigt sur le lecteur) ▪ certains systèmes peuvent être trompés par un moulage de doigt ▪ environ 2 % de la population mondiale ont des empreintes difficilement exploitables	▪ en théorie, toutes les applications possibles, mais le capteur est exposé à une éventuelle dégradation dans les applications grand public (distributeur de billets, accès extérieur à des locaux, ...) ▪ contrôle d'accès physique (locaux, machines, équipements spécifiques, contrôle d'accès logique – système d'information) ▪ identification judiciaire ▪ gestion des titres délivrés (permis de conduire, passeport, carte d'identité nationale)
Reconnaissance faciale	▪ seule une opération chirurgicale intervenant sur le cartilage est en mesure de la tromper ▪ n'est pas intrusive et n'exige aucun contact physique avec le capteur	▪ sensible à la variation de l'éclairage et au changement de la position du visage lors de l'acquisition de l'image ▪ taux élevés de fausses acceptations ou faux refus ▪ se fait souvent à l'insu de la personne	▪ contrôle d'accès physique (locaux, machines, équipement spécifiques, contrôle d'accès logique – système d'information) ▪ identification judiciaire (aéroports, casinos, centres commerciaux, stades, etc.) ▪ gestion des titres délivrés (gestion des permis de conduire aux États-Unis)

²¹⁹ Information tirée de Bernard DIONNE et ÈVELYNE RACETTE, « La biométrie : présentation à la Commission de l'éthique de la science et de la technologie », Ministère des Relations avec les citoyens et de l'Immigration, Québec, mars 2004 – document d'information, p. 21-37.

Biométrie	Avantages	Inconvénients	Applications
Géométrie de la main	▪ très simple à utiliser ▪ technique moins capricieuse que la reconnaissance d'empreintes digitales : le taux d'humidité, la saleté et les petites coupures n'empêcheront pas le système de fonctionner ▪ pas de traces de la géométrie de la main laissées partout ▪ niveaux très raisonnables d'exactitude	▪ trop encombrant pour un usage sur le bureau, dans une voiture ou un téléphone ▪ sujet aux modifications de la forme de la main liées au vieillissement ▪ taux de fausses acceptations élevé pour des jumeaux ou d'autres membres de la même famille	▪ contrôle d'accès à des locaux ou à des sites (Disney World, J.O. d'Atlanta, Aéroports de San-Francisco et de Tel Aviv, Université de Georgia, etc.) ▪ Horodateur
Reconnaissance de l'iris	▪ très grande fiabilité ▪ grande quantité d'informations contenue dans l'iris ▪ vrais jumeaux non confondus ▪ caméra moins exposée qu'un capteur avec contact (empreintes) mais davantage qu'un micro (voix) ▪ faible taux d'erreur pour les produits haut de gamme (méthode très fiable) ▪ le fleuron de la biométrie	▪ aspect psychologiquement invasif de la méthode ▪ les contraintes sur l'éclairage demandent souvent que le capteur soit proche de l'œil. Les variations de l'éclairage ambiant et les reflets perturbent fortement la mesure ▪ les systèmes bas de gamme peuvent être trompés à partir d'une photo ou d'une lentille de contact ▪ la technologie n'est pas encore suffisamment simple d'utilisation pour permettre le contrôle d'accès sur les postes clients	▪ distributeurs de billets de banques ▪ contrôle d'accès physique (locaux, machines, équipement spécifiques, contrôle d'accès logique – systèmes d'information critiques)

Biométrie	Avantages	Inconvénients	Applications
Reconnaissance de la rétine	▪ réputé comme étant le plus fiable des moyens biométriques ▪ carte vasculaire, propre à chaque individu (diffère entre deux jumeaux) et évolue peu avec l'âge ▪ l'empreinte rétinienne est peu exposée aux blessures (coupure, brûlure) ▪ faibles taux de faux rejets et de fausses acceptations ▪ résistant à la fraude ▪ faible taille du fichier signature : 96 octets (512 pour l'iris)	▪ mauvaise acceptation du public (l'œil est un organe sensible). Réticence psychologique de l'utilisateur. On accepte difficilement l'idée d'un rayon lumineux, même inoffensif, dans l'œil ▪ nécessité de placer ses yeux à proximité d'une tête de lecture (à moins de 4 cm.) ▪ méthode qui requiert des sujets coopératifs et entraînés ▪ technologie pas encore suffisamment simple d'utilisation pour permettre le contrôle d'accès sur les poste clients ▪ coûteux	▪ contrôle d'accès à des locaux très sensibles ▪ distributeurs automatiques de billets ▪ identification judiciaire
Reconnaissance de la voix	▪ plus facile de protéger le capteur que dans les autres technologies ▪ technologie non intrusive qui n'exige aucun contact physique avec le capteur ▪ permet l'identification à distance au moyen d'une liaison téléphonique	▪ sensible à l'état physique de la personne. La fatigue, le stress ou un rhume peuvent provoquer des variations de la voix ▪ dégradation croissante des performances au fur et à mesure que le temps augmente entre la session d'enregistrement et la session de contrôle ▪ le comportement des locuteurs se modifie lorsque ceux-ci s'habituent au système ▪ fraude possible par enregistrement ▪ sensible aux bruits ambiants; nécessite une excellente qualité audio ▪ taux élevé de faux rejets et de fausses acceptations	▪ « sur site » : serrures vocales pour contrôle d'accès, cabines bancaires en libre service ▪ liées aux télécommunications : identification du locuteur à travers le réseau téléphonique pour accéder à un service ▪ judiciaires : pour la recherche de suspects, orientation d'enquêtes, preuves lors d'un procès.

Biométrie	Avantages	Inconvénients	Applications
Reconnaissance de la signature	▪ culturellement ergonomique car la signature est un geste commun de la vie courante ▪ produit une représentation visuelle de la signature ▪ apporte une certaine sécurité sans nécessairement imposer la vérification systématique de la signature actuellement la seule technologie classée comme comportementale qui a véritablement abouti	▪ signature instable (certaines personnes ont une signature très erratique) ▪ la signature peut aussi changer sensiblement dans le temps (au bout de quelques années) ▪ sensible à l'état physique de la personne : la fatigue et le stress peuvent provoquer des variations dans la signature ▪ peut être imitée avec de l'entraînement ▪ mesure d'identification très restrictive	▪ contrôle d'accès logique
Dynamique de la frappe au clavier	▪ très convivial	▪ vitesse de frappe instable (peut être très erratique chez certaines personnes) ▪ sensible à l'état physique de la personne : la fatigue et le stress peuvent provoquer des variations dans la vitesse ▪ mesure d'identification très restrictive	▪ contrôle d'accès logique ▪ commerce électronique
Le profil génétique (ADN)	▪ technologie très fiable	▪ les techniques d'analyse sont chimiques pour le moment ▪ tests actuels très intrusifs	▪ identification judiciaire
Thermographie	▪ pas intrusive	▪ très coûteuse	▪ expérimental

ANNEXE 2

QUESTIONS D'INTÉRÊT PUBLIC LIÉES À LA BIOMÉTRIE POUR ACCROÎTRE L'INTÉGRITÉ DES DOCUMENTS D'IDENTITÉ ET DE VOYAGE

- FORUM DES POLITIQUES PUBLIQUES²²⁰ -

❖ **Juste équilibre entre sécurité, protection de la vie privée et libertés fondamentales**

Sur quelles valeurs fondamentales devraient se fonder les décisions concernant l'utilisation de la biométrie dans les documents d'identité relatifs à la citoyenneté ou à l'immigration?

La relation entre ces valeurs équivaut-elle à un jeu à somme nulle? Par exemple, une protection accrue de la vie privée se fera-t-elle nécessairement au détriment de la sécurité (ou vice versa)?

❖ **Finalité et application**

Quels objectifs d'intérêt public l'utilisation de la biométrie dans les documents de citoyenneté et d'immigration permettra-t-elle d'atteindre?

Quelles applications (identification ou vérification) seraient utilisées?

❖ **Technologie au service de la protection de la vie privée et gestion de l'information**

Existe-t-il des technologies qui peuvent garantir une protection adéquate de la vie privée et des renseignements personnels?

Quelles bases de données gouvernementales seraient liées à des documents biométriques? Comment l'information serait-elle gérée?

❖ **La biométrie et la loi**

Le cadre juridique actuel est-il approprié? Quels ajustements faudrait-il apporter?

Est-il applicable?

❖ **La gestion publique**

Est-il possible d'adopter une approche nationale unique? Ou vaut-il mieux que chaque ordre de gouvernement ou chaque programme ait son approche particulière?

Les mécanismes politiques et juridiques de surveillance et de reddition de compte sont-ils appropriés? Ou faut-il en créer d'autres?

Dans quelle mesure est-ce qu'il importe d'harmoniser la conception et l'exécution à l'échelle internationale?

²²⁰ « Biométrie : incidences et applications pour la citoyenneté et l'immigration », Document d'information, Forum tenu par CITOYENNETÉ ET IMMIGRATION CANADA, 7 et 8 octobre 2003, Ottawa (Ontario), Forum des politiques publiques, Canada, p. 15-25.

❖ **La capacité financière et administrative**

Du point de vue financier et administratif, est-il faisable d'instaurer des documents de citoyenneté et d'immigration biométriques?

❖ **Les documents biométriques : un système cohérent**

À quoi ressemblerait un système biométrique efficace dans les domaines de la citoyenneté et de l'immigration?

Les documents que ce système comporterait seraient-ils obligatoires? Dans l'affirmative, leur mise en œuvre pourrait-elle reposer sur le principe du respect volontaire?

CONCLUSIONS DU FORUM - EXTRAITS²²¹
--

- ❖ **L'utilisation de la biométrie en vue de documenter l'identité pose de véritables problèmes qui doivent faire l'objet d'un débat public sérieux** – il y a actuellement un vide politique et législatif dans ce secteur de la politique publique.
- ❖ **Le statu quo n'est pas viable** – les Canadiens ne peuvent pas compter sur l'échec de la technologie pour protéger leur vie privée ; il faut s'assurer que les impératifs stratégiques dictent le développement de la technologie et non l'inverse.
- ❖ **La dichotomie perçue entre la sécurité et la protection de la vie privée est fausse** – la biométrie ne comporte en soi aucun élément qui améliore ou qui limite le respect de la vie privée.
- ❖ **Il faut procéder à une étude de rentabilisation pour les applications biométriques dans les documents d'identité, y compris pour la carte d'identité nationale** – il est nécessaire de déterminer quels problèmes seraient éliminés par les instruments biométriques afin de mieux cerner les fonctions, les buts, les utilisations et les garanties nécessaires dans l'utilisation de la biométrie.
- ❖ **La biométrie a été appliquée avec succès dans d'autres pays** – notamment en ce qui a trait à l'immigration ; il faut s'inspirer des leçons tirées de l'expérience étrangère, comme le fait que les garanties de protection de la vie privée, pour être efficaces, doivent être intégrées dans le système dès le début.
- ❖ **La résolution satisfaisante des questions de respect de la vie privée et de protection des renseignements personnels doit faire partie intégrante de la conception et de l'élaboration de tout document doté de caractéristiques biométriques** – notamment au regard de l'accès non autorisé à l'information, de l'utilisation de l'information à d'autres fins que celles prévues et au respect du principe de confidentialité.

²²¹ « La biométrie : Incidences et applications pour la citoyenneté et l'immigration », Actes d'un forum tenu par CITOYENNETÉ ET IMMIGRATION CANADA, le 7 et 8 octobre 2003, Ottawa (Ontario), Forum des politiques publiques (non daté)

ANNEXE 3

DONNÉES FOURNIES SUR LES PASSAGERS AÉRIENS

« Voici les trente-quatre données fournies aux Américains, en vertu de l'accord signé avec Bruxelles le 28 mai :

- Code repère du fichier Passenger Name Record (PNR) : pour identifier le fichier
- Date de réservation du voyage
- Date(s) prévue(s) du voyage
- Nom du passager
- Autres noms figurant dans le fichier, ceux des autres passagers, et de l'équipage
- Adresse : cette mention concerne en fait le vol (comme le code des aéroports de départ, de transit et d'arrivée)
- Mode de paiement, dont le numéro de carte de crédit
- Adresse de facturation
- Numéros de téléphone du passager
- Itinéraire complet du voyageur, en cas de changement, ou de pause dans le voyage
- Informations « grands voyageurs » : miles parcourus et coordonnées des vols
- Agence de voyages, où le billet a été vendu
- Agent de voyages
- Information sur le partage des codes, quand un vol est effectué en partenariat entre deux compagnies (par exemple entre Air France et Delta Airlines)
- Statut du voyageur
- PNR scindé/divisé : lorsque le fichier occupe plusieurs pages sur un écran d'ordinateur
- Adresse électronique du passager
- Informations sur l'établissement des billets
- Observations générales : celles-ci peuvent concerner les éventuels incidents survenus sur les vols précédents (altercations, alcoolisme, etc.)
- Numéro du billet
- Numéro du siège occupé
- Date d'émission du billet
- Passager répertorié comme défaillant : qui ne s'est pas présenté à l'embarquement, malgré une réservation
- Numéros d'étiquetage des bagages
- Passager de dernière minute sans réservation : pour les passagers embarqués au dernier moment
- Données OSI : mention des demandes diverses exprimées par un voyageur, comme la fourniture d'une chaise roulante à son arrivée
- Données SSI/SSR : « demande de services spéciaux », en fonction des préférences alimentaires, de l'état de santé ou de l'âge. La plupart de ces données sont codées au niveau international
- Informations sur la source
- Historique des changements apportés dans le fichier des voyageurs
- Nombre de voyageurs dans le fichier
- Informations relatives au siège occupé (à gauche, à droite, à l'avant, à l'arrière)
- Allers simples
- Informations APIS éventuellement recueillies : numéro de passeport, date de naissance, nationalité du passager
- Données ATFQ : prix du billet »

Philippe Ricard²²²

²²² Philippe RICARD, « L'Amérique dicte sa loi antiterroriste au trafic aérien avec l'Europe », *Le Monde.fr* [en ligne] 21 juin 2004 [http://www.lemonde.fr/web/imprimer_article/0,1-0@2-3222,36-369798,0.html]

ANNEXE 4

ARTICLES DE LOIS CITÉS DANS LE TEXTE (EXTRAITS)

❖ **CHARTRE DES DROITS ET LIBERTÉS DE LA PERSONNE (L.R.Q. C-12)**

Préambule.

CONSIDÉRANT que tout être humain possède des droits et libertés intrinsèques, destinés à assurer sa protection et son épanouissement;

Considérant que tous les êtres humains sont égaux en valeur et en dignité et ont droit à une égale protection de la loi;

Considérant que le respect de la dignité de l'être humain et la reconnaissance des droits et libertés dont il est titulaire constituent le fondement de la justice et de la paix;

Considérant que les droits et libertés de la personne humaine sont inséparables des droits et libertés d'autrui et du bien-être général;

Considérant qu'il y a lieu d'affirmer solennellement dans une Charte les libertés et droits fondamentaux de la personne afin que ceux-ci soient garantis par la volonté collective et mieux protégés contre toute violation;

À ces causes, Sa Majesté, de l'avis et du consentement de l'Assemblée nationale du Québec, décrète ce qui suit:

PARTIE I

LES DROITS ET LIBERTÉS DE LA PERSONNE

CHAPITRE I

LIBERTÉS ET DROITS FONDAMENTAUX

Droit à la vie.

1. Tout être humain a droit à la vie, ainsi qu'à la sûreté, à l'intégrité et à la liberté de sa personne.

Personnalité juridique.

Il possède également la personnalité juridique.

1975, c. 6, a. 1; 1982, c. 61, a. 1.

Droit au secours.

2. Tout être humain dont la vie est en péril a droit au secours.

Secours à une personne dont la vie est en péril.

Toute personne doit porter secours à celui dont la vie est en péril, personnellement ou en obtenant du secours, en lui apportant l'aide physique nécessaire et immédiate, à moins d'un risque pour elle ou pour les tiers ou d'un autre motif raisonnable.

1975, c. 6, a. 2.

Libertés fondamentales.

3. Toute personne est titulaire des libertés fondamentales telles la liberté de conscience, la liberté de religion, la liberté d'opinion, la liberté d'expression, la liberté de réunion pacifique et la liberté d'association.

1975, c. 6, a. 3.

Sauvegarde de la dignité.

4. Toute personne a droit à la sauvegarde de sa dignité, de son honneur et de sa réputation.

1975, c. 6, a. 4.

Respect de la vie privée.

5. Toute personne a droit au respect de sa vie privée.

1975, c. 6, a. 5.

❖ **LOI CONCERNANT LE CADRE JURIDIQUE DES TECHNOLOGIES DE L'INFORMATION
(L.R.Q. C-1.1)**

Respect de l'intégrité physique.

43. Nul ne peut exiger que l'identité d'une personne soit établie au moyen d'un procédé ou d'un dispositif qui porte atteinte à son intégrité physique.

Dispositif de localisation.

À moins que la loi le prévoie expressément en vue de protéger la santé des personnes ou la sécurité publique, nul ne peut exiger qu'une personne soit liée à un dispositif qui permet de savoir où elle se trouve.

2001, c. 32, a. 43.

Caractéristiques ou mesures biométriques.

44. Nul ne peut exiger, sans le consentement exprès de la personne, que la vérification ou la confirmation de son identité soit faite au moyen d'un procédé permettant de saisir des caractéristiques ou des mesures biométriques. L'identité de la personne ne peut alors être établie qu'en faisant appel au minimum de caractéristiques ou de mesures permettant de la relier à l'action qu'elle pose et que parmi celles qui ne peuvent être saisies sans qu'elle en ait connaissance.

Fin d'identification.

Tout autre renseignement concernant cette personne et qui pourrait être découvert à partir des caractéristiques ou mesures saisies ne peut servir à fonder une décision à son égard ni être utilisé à quelque autre fin que ce soit. Un tel renseignement ne peut être communiqué qu'à la personne concernée et seulement à sa demande.

Destruction des caractéristiques.

Ces caractéristiques ou mesures ainsi que toute note les concernant doivent être détruites lorsque l'objet qui fonde la vérification ou la confirmation d'identité est accompli ou lorsque le motif qui la justifie n'existe plus.

2001, c. 32, a. 44.

Banque de caractéristiques.

45. La création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la Commission d'accès à l'information. De même, doit être divulguée l'existence d'une telle banque qu'elle soit ou ne soit pas en service.

Ordonnance de la Commission d'accès à l'information.

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

Fin de la mise en service.

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

2001, c. 32, a. 45.

❖ **LOI SUR L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS**
(L.R.Q. CHAPITRE A-2.1)

Renseignements confidentiels.

53. Les renseignements nominatifs sont confidentiels sauf dans les cas suivants:

- 1° leur divulgation est autorisée par la personne qu'ils concernent; si cette personne est mineure, l'autorisation peut également être donnée par le titulaire de l'autorité parentale;
- 2° ils portent sur un renseignement obtenu dans l'exercice d'une fonction d'adjudication par un organisme public exerçant des fonctions quasi judiciaires; ils demeurent cependant confidentiels si l'organisme les a obtenus alors qu'il siégeait à huis-clos ou s'ils sont visés par une ordonnance de non-divulgation, de non-publication ou de non-diffusion.

1982, c. 30, a. 53; 1985, c. 30, a. 3; 1989, c. 54, a. 150; 1990, c. 57, a. 11.

Consentement.

59. Un organisme public ne peut communiquer un renseignement nominatif sans le consentement de la personne concernée.

Exception.

Toutefois, il peut communiquer un tel renseignement sans le consentement de cette personne, dans les cas et aux strictes conditions qui suivent:

- 1° au procureur de cet organisme si le renseignement est requis aux fins d'une poursuite pour infraction à une loi que cet organisme est chargé d'appliquer, ou au Procureur général si le

renseignement est requis aux fins d'une poursuite pour infraction à une loi applicable au Québec;

- 2° au procureur de cet organisme, ou au Procureur général lorsqu'il agit comme procureur de cet organisme, si le renseignement est requis aux fins d'une procédure judiciaire autre qu'une procédure visée dans le paragraphe 1°;
- 3° à une personne qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si le renseignement est requis aux fins d'une poursuite pour infraction à une loi applicable au Québec;
- 4° à une personne à qui cette communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée;
- 5° à une personne qui est autorisée par la Commission d'accès à l'information, conformément à l'article 125, à utiliser ce renseignement à des fins d'étude, de recherche ou de statistique;
- 6° (*paragraphe abrogé*);
- 7° (*paragraphe abrogé*);
- 8° à une personne ou à un organisme, conformément aux articles 61, 67, 67.1, 67.2, 68 et 68.1;
- 9° à une personne impliquée dans un événement ayant fait l'objet d'un rapport par un corps de police, lorsqu'il s'agit d'un renseignement sur l'identité de toute autre personne qui a été impliquée dans cet événement, sauf s'il s'agit d'un témoin, d'un dénonciateur ou d'une personne dont la santé ou la sécurité serait susceptible d'être mise en péril par la communication d'un tel renseignement.

1982, c. 30, a. 59; 1983, c. 38, a. 55; 1984, c. 27, a. 1; 1985, c. 30, a. 5; 1987, c. 68, a. 5; 1990, c. 57, a. 13.

Communication sans consentement.

59.1. Outre les cas prévus à l'article 59, un organisme public peut également communiquer un renseignement nominatif, sans le consentement des personnes concernées, en vue de prévenir un acte de violence, dont un suicide, lorsqu'il existe un motif raisonnable de croire qu'un danger imminent de mort ou de blessures graves menace une personne ou un groupe de personnes identifiable.

Communication.

Les renseignements peuvent alors être communiqués à la ou aux personnes exposées à ce danger, à leur représentant ou à toute personne susceptible de leur porter secours.

Conditions et modalités.

La personne ayant la plus haute autorité au sein de l'organisme public doit, par directive, établir les conditions et les modalités suivant lesquelles les renseignements peuvent être communiqués par le personnel de l'organisme. Le personnel est tenu de se conformer à cette directive.

2001, c. 78, a. 1.

Accessibilité des renseignements nominatifs.

62. Un renseignement nominatif est accessible, sans le consentement de la personne concernée, à toute personne qui a qualité pour le recevoir au sein d'un organisme public lorsque ce renseignement est nécessaire à l'exercice de ses fonctions.

Conditions.

En outre, cette personne doit appartenir à l'une des catégories de personnes visées au paragraphe 4° du deuxième alinéa de l'article 76 ou au paragraphe 5° du premier alinéa de l'article 81.

1982, c. 30, a. 62; 1990, c. 57, a. 14.

Demande prohibée.

64. Nul ne peut, au nom d'un organisme public, recueillir un renseignement nominatif si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en oeuvre d'un programme dont il a la gestion.

1982, c. 30, a. 64.

Identification préalable.

65. Quiconque, au nom d'un organisme public, recueille un renseignement nominatif auprès de la personne concernée ou d'un tiers doit au préalable s'identifier et l'informer:

- 1° du nom et de l'adresse de l'organisme public au nom de qui la collecte est faite;
- 2° de l'usage auquel ce renseignement est destiné;
- 3° des catégories de personnes qui auront accès à ce renseignement;
- 4° du caractère obligatoire ou facultatif de la demande;
- 5° des conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande;
- 6° des droits d'accès et de rectification prévus par la loi.

Dossiers d'adoption.

Toutefois, une personne dûment autorisée par un organisme public qui détient des dossiers ayant trait à l'adoption de personnes et qui recueille un renseignement relatif aux antécédents d'une personne visée dans l'un de ces dossiers ou permettant de retrouver un parent ou une personne adoptée n'est pas tenue d'informer la personne concernée ou le tiers de l'usage auquel est destiné le renseignement ni des catégories de personnes qui y auront accès.

Collecte de renseignements.

Les règles suivant lesquelles la collecte de renseignements nominatifs doit être faite sont prescrites par règlement du gouvernement.

Restrictions.

Le présent article ne s'applique pas à une enquête de nature judiciaire, ni à une enquête ou à un constat faits par une personne qui, en vertu de la loi, est chargée de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

1982, c. 30, a. 65; 1990, c. 57, a. 15.

Consentement non requis.

Conservation.

72. Un organisme public doit veiller à ce que les renseignements nominatifs qu'il conserve soient à jour, exacts et complets pour servir aux fins pour lesquelles ils sont recueillis.

1982, c. 30, a. 72.

Renseignements nominatifs.

§ 1. — *Droit d'accès*

Droit à l'information.

83. Toute personne a le droit d'être informée de l'existence, dans un fichier de renseignements personnels, d'un renseignement nominatif la concernant.

Communication.

Elle a le droit de recevoir communication de tout renseignement nominatif la concernant.

Mineur de moins de quatorze ans.

Toutefois, un mineur de moins de quatorze ans n'a pas le droit d'être informé de l'existence ni de recevoir communication d'un renseignement nominatif de nature médicale ou sociale le concernant, contenu dans le dossier constitué par l'établissement de santé ou de services sociaux visé au deuxième alinéa de l'article 7.

1982, c. 30, a. 83; 1987, c. 68, a. 6; 1990, c. 57, a. 21; 1992, c. 21, a. 74.

Communication d'un renseignement nominatif.

§ 3. — *Droit de rectification*

Rectification.

89. Toute personne qui reçoit confirmation de l'existence dans un fichier d'un renseignement nominatif la concernant peut, s'il est inexact, incomplet ou équivoque, ou si sa collecte, sa communication ou sa conservation ne sont pas autorisées par la loi, exiger que le fichier soit rectifié.

1982, c. 30, a. 89.

Rectification d'un renseignement.

89.1. Un organisme public doit refuser d'accéder à une demande de rectification d'un renseignement nominatif faite par l'administrateur de la succession, par le bénéficiaire d'une assurance-vie, par l'héritier ou le successeur de la personne concernée par ce renseignement, à moins que cette rectification ne mette en cause ses intérêts ou ses droits à titre d'administrateur, de bénéficiaire, d'héritier ou de successeur.

1986, c. 95, a. 6; 1993, c. 17, a. 100.

❖ **LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE SECTEUR PRIVÉ
(L.R.Q. CHAPITRE P-39.1)**

Constitution d'un dossier.

4. Toute personne qui exploite une entreprise et qui, en raison d'un intérêt sérieux et légitime, peut constituer un dossier sur autrui doit, lorsqu'elle constitue le dossier, inscrire son objet.

Inscription de l'objet.

Cette inscription fait partie du dossier.

1993, c. 17, a. 4; 1999, c. 40, a. 233.

Renseignements nécessaires.

5. La personne qui recueille des renseignements personnels afin de constituer un dossier sur autrui ou d'y consigner de tels renseignements ne doit recueillir que les renseignements nécessaires à l'objet du dossier.

Moyens.

Ces renseignements doivent être recueillis par des moyens licites.

1993, c. 17, a. 5.

Cueillette de renseignements.

Information.

8. La personne qui recueille des renseignements personnels auprès de la personne concernée doit, lorsqu'elle constitue un dossier sur cette dernière, l'informer:

1° de l'objet du dossier;

2° de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise;

3° de l'endroit où sera détenu son dossier ainsi que des droits d'accès ou de rectification.

1993, c. 17, a. 8.

Confidentialité.

10. Toute personne qui exploite une entreprise et recueille, détient, utilise ou communique des renseignements personnels sur autrui doit prendre et appliquer des mesures de sécurité propres à assurer le caractère confidentiel des renseignements.

1993, c. 17, a. 10.

Dossier en état.

11. Toute personne qui exploite une entreprise doit veiller à ce que les dossiers qu'elle détient sur autrui soient à jour et exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée.

1993, c. 17, a. 11.

Interdiction.

13. Nul ne peut communiquer à un tiers les renseignements personnels contenus dans un dossier qu'il détient sur autrui ni les utiliser à des fins non pertinentes à l'objet du dossier, à moins que la personne concernée n'y consente ou que la présente loi le prévoit.

1993, c. 17, a. 13.

Consentement non requis.

20. Dans l'exploitation d'une entreprise, un renseignement personnel n'est accessible, sans le consentement de la personne concernée, à tout préposé, mandataire ou agent de l'exploitant qui a qualité pour le connaître qu'à la condition que ce renseignement soit nécessaire à l'exercice de ses fonctions ou à l'exécution de son mandat.

1993, c. 17, a. 20.

Communication des renseignements.

27. Toute personne qui exploite une entreprise et détient un dossier sur autrui doit, à la demande de la personne concernée, lui en confirmer l'existence et lui donner communication des renseignements personnels la concernant.

1993, c. 17, a. 27.

Collecte non autorisée.

28. Outre les droits prévus au premier alinéa de l'article 40 du Code civil du Québec, la personne concernée peut faire supprimer un renseignement personnel la concernant si sa collecte n'est pas autorisée par la loi.

1993, c. 17, a. 28.



LES PUBLICATIONS DE LA COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE

La liste qui suit mentionne toutes les publications parues depuis 2002. Il est possible de les consulter et de les télécharger en accédant au site Web de la Commission de l'éthique de la science et de la technologie (www.ethique.gouv.qc.ca). Des résumés en français, en anglais et en espagnol accompagnent chacun des avis dans le site.

À moins d'indication contraire, les documents sont également disponibles en version imprimée et peuvent être obtenus en adressant une demande à :

Commission de l'éthique de la science et de la technologie
1200, route de l'Église, bureau 3.45
Sainte-Foy QC G1V 4Z2
Téléphone : (418) 528-0965
Télécopieur : (418) 646-0920
Courriel : ethique@ethique.gouv.qc.ca
ou lauraine.berard@cst.gouv.qc.ca

AVIS

Le don et la transplantation d'organes : dilemmes éthiques en contexte de pénurie
Novembre 2004, 142 p.; ISBN 2-550-43415-3

Organ Donation and Transplantation : Ethical Dilemmas Due to Shortage
November 2004, 145p.; ISBN 2-550-43415-3 (fichier pdf seulement)

Pour une gestion éthique des OGM
Décembre 2003, 144 p.; ISBN 2-550-41769-6

Les enjeux éthiques des banques d'information génétique : pour un encadrement démocratique et responsable
Février 2003, 97 p.; ISBN 2-550-40365-7

DOCUMENT DE RÉFLEXION

L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques
Juin 2005, 87p.; ISBN 2-550-44634-8

MÉMOIRE

Les nouveaux enjeux de la sécurité alimentaire au Québec
Janvier 2004, 40 p.

ÉTUDES ET RECHERCHES

Documents complémentaires à l'avis *Pour une gestion éthique des OGM*

Disponibles uniquement sur le site Web (www.ethique.gouv.qc.ca/fr/publications.html)

Rapport de recherche sur la couverture médiatique au Québec en matière d'alimentation et d'OGM

Juin 2003, 29 p.

Par Richard Lair et Alain Létourneau

Financement de la recherche dans le secteur des biotechnologies : le cas des OGM

Janvier 2003, 23 p.

Par Guillaume Lavallée

Les représentations véhiculées dans la culture amérindienne du Québec en ce qui a trait à l'alimentation, aux organismes génétiquement modifiés (OGM) et aux transformations que l'humain peut apporter à la nature

Décembre 2002, 49 p.

Par Jose Lopez Arellano

Est-il possible de faire... sans la transgénèse?

Novembre 2002, 13 p.

Par Jean-François Sénéchal

Le christianisme et les OGM

Novembre 2002, 13 p.

Par André Beauchamp

Cuisine de Dieu – Aliments profanes. Prohibitions alimentaires du judaïsme, organismes génétiquement modifiés et enjeux éthiques

Octobre 2002, 52 p.

Par Michaël Elbaz et Ruth Murbach

Le bouddhisme et les OGM

Septembre 2002, 33 p.

Par Charles-Anica Endo

L'Islam et les OGM

Septembre 2002, 35 p.

Par Ali Maarabouni

Les modifications génétiques chez les microorganismes

Août 2002, 17 p.

Par Isabelle Boucher

OGM végétaux

Août 2002, 40 p.

Par Éric Dion

Vue d'ensemble des techniques usuelles en transgénèse animale

Août 2002, 9 p.

Par Jean-François Sénéchal

Documents complémentaires à l'avis *Les enjeux éthiques des banques d'information génétique : pour un encadrement démocratique et responsable*

Disponibles uniquement sur le site Web (www.ethique.gouv.qc.ca/fr/publications.html)

Les banques d'information génétique dans le monde : aperçu de la situation

Janvier 2003, 32 p.

Par David Boucher et Emmanuelle Trottier

Le consentement libre et éclairé : un paradigme révolu en matière de recherche génétique sur les populations?

Décembre 2002, 18 p.

Par Dany Joncas

Les banques de données génétiques et le droit étranger

Octobre 2002, 30 p.

Par Dany Joncas

RAPPORT ANNUEL

Rapport d'activité 2001-2003 et perspectives d'avenir

Octobre 2003, 30 p.; ISBN 2-550-41684-8 et ISSN 1708-8534

BROCHURE

Les banques d'information génétique : «C'est BIG!»

Mars 2004, 27 p.; ISBN 2-550-42074-8

Par Luc Dupont

CONSULTATION

L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques

Document de consultation

Juin 2005, 18p.; ISBN 2-550-44626-7

Rapport de consultation sur les enjeux éthiques du don et de la transplantation d'organes. Résultats des entrevues de groupes et du mini-sondage réalisé dans le cadre de l'Enquête Stamédia printemps 2004

Novembre 2004, 94 p.; ISBN 2-550-43416-1

Les enjeux éthiques du don et de la transplantation d'organes

Document de consultation

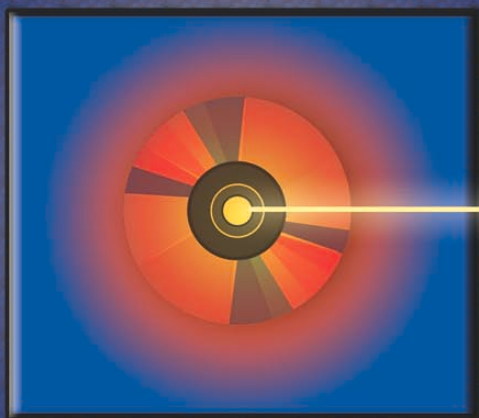
Mai 2004, 41 p.; ISBN 2-550-42564-2

L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques constitue un document de réflexion que la Commission de l'éthique de la science et de la technologie soumet au débat public. Considérant l'intensification des mesures de contrôle et la disponibilité croissante de moyens techniques fondés sur l'acquisition de données personnelles et l'utilisation de traits personnels – des données biométriques – pour établir ou contrôler l'identité d'une personne, la Commission estime urgent de s'interroger sur les enjeux éthiques que la question soulève et d'en débattre publiquement.

D'entrée de jeu, la Commission souligne l'importance de la sécurité pour l'être humain et pour les cités. Elle fait ensuite le point sur les aspects techniques de la biométrie, sur ses champs d'application – lutte au terrorisme et à la criminalité reliée au vol d'identité, contrôle de l'accès à des sites physiques ou virtuels – et sur les encadrements normatifs (lois, règlements ou autres) qui permettent de baliser le domaine, pour ensuite signaler les enjeux éthiques que soulève l'application de la technologie biométrique dans une société pluraliste et démocratique. Ces enjeux ne sont cependant abordés que succinctement dans le présent document de réflexion; la consultation que mènera la Commission sur le sujet, tant auprès d'experts qu'auprès de la population, lui permettra d'amorcer la préparation d'un avis sur ce thème à l'intention des décideurs politiques et institutionnels.

Ce document de réflexion de la Commission est disponible en fichier électronique à l'adresse suivante : www.ethique.gouv.qc.ca

La mission de la CEST consiste, d'une part, à informer, sensibiliser, recevoir des opinions, susciter la réflexion et organiser des débats sur les enjeux éthiques du développement de la science et de la technologie, et, d'autre part, à proposer des orientations susceptibles de guider les acteurs concernés dans leur prise de décision.



Commission
de l'éthique
de la science
et de la technologie

Québec

